Федеральное государственное бюджетное образовательное учреждение
высшего образования «Московский государственный технический университет
гражданской авиации» (МГТУ ГА)

---

На правах рукописи

**МАШОШИН**
**Антон Олегович**

# МЕТОДЫ И АЛГОРИТМЫ ВАЛИДАЦИИ СООБЩЕНИЙ СИСТЕМЫ АВТОМАТИЧЕСКОГО ЗАВИСИМОГО НАБЛЮДЕНИЯ В УСЛОВИЯХ НЕСАНКЦИОНИРОВАННОГО ВМЕШАТЕЛЬСТВА ПРИ УПРАВЛЕНИИ ВОЗДУШНЫМ ДВИЖЕНИЕМ

Специальность 05.22.13 «Навигация и управление воздушным движением»

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель:
к.т.н, доцент
Петров Виктор Иванович

Москва — 2022

## Оглавление

Стр.

**Введение** . . . . . 4

**Глава 1. Анализ состояния вопроса и постановка задачи исследования** . . . . . 12

1.1 Анализ системы управления воздушным движением с использованием системы автоматического зависимого наблюдения 12

1.2 Анализ несанкционированного вмешательства в систему автоматического зависимого наблюдения . . . . . 21

1.3 Постановка задачи исследования . . . . . 31

**Глава 2. Разработка методов и алгоритмов валидации сообщений системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства** . . . . . 33

2.1 Методы противодействия несанкционированному вмешательству на компоненты системы автоматического зависимого наблюдения 33

2.2 Методы вычисления временных характеристик и синхронизации сигналов системы автоматического зависимого наблюдения . . . . 51

2.3 Методы и алгоритмы машинного обучения в задаче определения события несанкционированного вмешательства . . . . . 61

2.4 Разработка математической модели каналов информационного обмена в условиях несанкционированного вмешательства . . . . . 70

2.5 Разработка математической модели мультилатерационного метода определения местоположения воздушного судна в условиях несанкционированного вмешательства . . . . . 77

2.5.1 Разработка критериев достоверности данных системы автоматического зависимого наблюдения . . . . . 77

2.5.2 Исследование математических моделей при работе с избыточными данными . . . . . 78

2.6 Разработка алгоритмов системы анализа и фильтрации сообщений АЗН-В . . . . . 87

**Глава 3. Практическое применение методов и алгоритмов валидации сообщений системы автоматического зависимого наблюдения** . . . . . 97

3.1 Определение местоположения ВС в условиях несанкционированного вмешательства на систему автоматического зависимого наблюдения . . . . . 98

3.2 Разработка архитектуры системы анализа и фильтрации сообщений автоматического зависимого наблюдения . . . . . 106

3.3 Исследование мер по резервированию системы анализа и фильтрации сообщений АЗН-В . . . . . 110

**Глава 4. Апробация системы анализа и фильтрации сообщений автоматического зависимого наблюдения** . . . . . 112

4.1 Моделирование угроз несанкционированного вмешательства на систему автоматического зависимого наблюдения . . . . . 114

4.2 Результаты работы системы анализа и фильтрации сообщений системы автоматического зависимого наблюдения . . . . . 122

**Заключение** . . . . . 130

**Список сокращений и условных обозначений** . . . . . 133

**Список рисунков** . . . . . 144

**Список таблиц** . . . . . 147

**Приложение А. Примеры кода имитационного моделировнаия** . 148

**Приложение Б. Примеры кода определения точного времени прихода сигнала** . . . . . 166

# Введение

Увеличение интенсивности воздушного движения, необходимость в повышении безопасности при одновременном сокращении затрат на осуществление полетов, а также гармонизация с международными стандартами и необходимость в поддержании конкурентоспособности на внешнем рынке аэронавигационных провайдеров послужило необходимым импульсом для модернизации Единой системы организации воздушного движения (ЕС ОрВД). На данный момент Правительством Российской Федерации одобрена концепция и план создания и развития аэронавигационной системы (АНС) России[50], в рамках которой происходит внедрение новейших технологий, нацеленных на повышение качества предоставляемых аэронавигационных услуг.

По всей России на данный момент уже используется новая система вертикального эшелонирования с сокращенными интервалами (RVSM), воздушные суда оборудуются ответчиками RBS (Remote Beacon System), производится идентификация судна по каналу Mode S, осуществлен переход на футовую систему эшелонирования. Данные этапы модернизации – уже давно пройденные этапы европейских и американских программ: Single European Sky (Евроконтроль) и NextGen (Федеральное Авиационное Агентство (США)). Однако, применение их в воздушном пространстве РФ обосновано, в первую очередь, ориентированностью рынка на транзитные и зарубежные полеты. Интеграция используемых технологий позволит повысить удобство, а вместе с ним и привлекательность использования ВП РФ, как для ведущих отечественных операторов, так и для зарубежных партнеров.

Одним из последних трендов развития АНС является использование систем АЗН (Автоматически Зависимое Наблюдение). АЗН-В (АЗН-вещание) и многопозиционные системы наблюдения рассматриваются как наиболее перспективные в будущей системе ОрВД России[49; 50], обеспечивающие реализацию разрабатываемых в ИКАО новых концепций организации воздушного движения. «Долгосрочная цель концепции, в части наблюдения, заключается в том, чтобы ... АЗН-В стали, наряду с традиционными, основными методами наблюдения, используемыми в целях организации воздушного движения в РФ». Однако, последние эксперименты и опыты, проведенные специалистами в обла-

сти информационной безопасности, указывают на то, что использование данной системы без каких либо дополнительных проверок определения достоверности данных, может являться непредусмотрительным решением. Исследования[7; 15; 24; 30] показали, что благодаря открытости используемого формата передачи данных по радиоканалу, отсутствию аутентификации и алгоритмов шифрования данных, может быть произведен ряд атак, целью которых может быть как полный отказ системы АЗН, так и внесение изменений в информационное пространство пользователей данной технологии. Учитывая тот факт, что в будущем текущие системы ОрВД (первичные радиолокаторы) будут вытеснены или же будут использоваться с меньшим приоритетом, чем более точные АЗН, описанная выше атака сможет привести к нарушению функционирования центров ОрВД, вплоть до полного отказа работы сектора диспетчерского наблюдения (в районах, где первичная радиолокация не предусмотрена). Теме кибербезопасности гражданской авиации были полностью посвящены 39-я и 40-я сессии Ассамблеи ИКАО, в рамках которых была подтверждена важность и безотлагательность защиты критических систем инфраструктуры гражданской авиации от кибератак, а также необходимость в осуществлении стратегии кибербезопасности странами-участниками ИКАО. Так, согласно плану действий по обеспечению кибербезопасности, сказано, что к 2022-2023 году необходимо помимо прочего "разработать платформы и механизмы обмена информацией, ... , для предотвращения ... последствий соответствующих киберсобытий". В документе ICAO Doc 9924 [16] указано, что использование технологии АЗН-В возможно только при проверке сообщений дополнительными системами наблюдения, такими как ВРЛ (вторичная радиолокация) или МПСН (мультипозиционная система наблюдения). Поскольку одной из целей внедрения технологии АЗН-В является снижение расходов на средства наблюдения, требования ИКАО по дополнительной проверке сообщений указанными средствами являются трудновыполнимыми - в случае использования ВРЛ, необходимо поддерживать две системы наблюдения, а в случае использования МПСН, существует необходимость в многократном перекрытии воздушного пространства станциями приема, что в свою очередь также требует дополнительных затрат. Вышесказанное определяет **противоречие практического характера**. Отсутствие единой методики, комплексного алгоритма по определению достоверности сообщений АЗН-В и необходимость применения информации из системы АЗН-В в свою

очередь определяет **противоречие научного характера**. Научный интерес представляет вопрос о возможности противодействия киберугрозе на АЗН-В в различных конфигурациях - вплоть до конфигурации с одной станцией приема. Задачу определения истинности сообщения в таком случае невозможно решить методом мультилатерации, а в случае приема сообщений более чем тремя станциями необходимо использовать избыточность данных для получения точного местоположения ВС с использованием различных математических моделей. Сказанное определяет **актуальность работы**, посвященной разработке эффективных и не требующих значительных финансовых вложений методов по проверке достоверности информации поступающей от системы АЗН-В. Для разрешения сформулированных противоречий практического и научного характера в диссертации решается актуальная научно-техническая задача противодействия несанкционированному вмешательству при управлении воздушным движением, требующей разработки на основе единого научно-методического аппарата методов и алгоритмов валидации сообщений системы автоматического наблюдения.

**Степень разработанности темы исследования**

Большой вклад в решение широкого круга теоретических и прикладных вопросов авиационной кибербезопасности внесли Э.Я. Фальков, С.С. Бybин, Никитин А.В., Аршинов А.М., Дружинин Е.Л., Булатов Д.Г., Петров В.И., Педанов В.А., Минин В.В., Зыбин Е.Ю., Савельев М.С., Бybин С.С., Лаврентьев О.Ю., Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С., Овсянникова А.С., Хобта Д.О., Газизулин М.Р.

Теоретические и прикладные вопросы анализа сообщений АЗН-В излагаются в трудах Рубцова Е.А., Калинцева А.С., Григорьевой Е.А., Кузнецова А.М., Трусова С.В., Бобровского С.А., Барабошкина О.И., Алипов И.В., Ещенко А.А., Далецкого С.В., Косьянчука В.В., Сельвесюка Н.И., Хамматова Р.Р., Тараканова А.А., Лебедева Б.В., Соломенцева В.В., Стратиенко А.Н.

Возможности применения методов машинного обучения, в частности использование нейросетей для идентификации сигналов АЗН-В, освещались в работе Зинкевича А.В "Исследование возможности идентификации АЗН-В сигналов с помощью нейросетей" [47]. Также в работе Калинцева А. С. и Рубцова Е. А. "Методика выявления ложных преднамеренно формируемых сигналов АЗН-В" [48] описывается способ выявления аномалий АЗН-В, где ключевой

метрикой является отношение уровня мощности сигнала к расстоянию от наземной станции до воздушного судна. В данной диссертационной работе параметр уровня мощности сигнала наравне с другими метриками применялся для решения классификационной задачи определения истинности сообщения АЗН-В методом монолатерации.

Вместе с тем, задача валидации сообщений АЗН-В в условиях несанкционированного вмешательства до сих пор не решена в полной мере - не разработан метод валидации сообщений в условиях недостаточного количества станций приема для функционирования МПСН, нет единого алгоритма использования информации об аномалиях в сообщениях АЗН-В и информации от МПСН для оценки достоверности данных от АЗН-В, отсутствует технический облик системы валидации сообщений АЗН-В. В отличии от широко применяемого и хорошо изученного метода мультилатерации, разработка и использование алгоритмов машинного обучения, а также оценка эффективности такого подхода практически не производилась.

**Целью диссертационной работы** является разработка методов и алгоритмов валидации сообщений автоматического зависимого наблюдения в условиях несанкционированного вмешательства при управлении воздушным движением.

**Для достижения поставленной цели в диссертационной работе необходимо решить следующие задачи:**

1. Исследовать потенциальные угрозы функционирования технологии автоматического зависимого наблюдения при управлении воздушным движением.
2. Разработать модель угроз системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства при управлении воздушным движением.
3. Определить критерии достоверности данных системы АЗН-В.
4. Разработать алгоритм выбора математической модели метода мультилатерации для обеспечения наилучшего определения местоположения ВС.
5. Разработать метод валидации сообщений автоматического зависимого наблюдения, позволяющий производить оценку достоверности в условиях недостаточного количества станций приема (1 - 3 станции).

6. Разработать алгоритм выбора методов валидации сообщений автоматического зависимого наблюдения при различном количестве станций приема.
7. Разработать систему анализа и фильтрации данных автоматического зависимого наблюдения.
8. Произвести апробацию и оценить эффективность методов валидации сообщений автоматического зависимого наблюдения.

**Объект исследования:** Система автоматического зависимого наблюдения - вещания.

**Предмет исследования:** Методы и алгоритмы валидации сообщений АЗН-В в условиях несанкционированного вмешательства при управлении воздушным движением.

**Методология и методы исследования:** Системный анализ, математическое, имитационное и полунатурное моделирование.

**Научная новизна:**

1. Разработан алгоритм выбора методов валидации сообщений.
2. Предложен метод монолатерации для валидации сообщений автоматического зависимого наблюдения при различных типах несанкционированного вмешательства при управлении воздушным движением.
3. Разработана и апробирована система анализа и фильтрации сообщений автоматического зависимого наблюдения.

**Теоретическая значимость работы состоит в том, что в ней проведено и представлено решение задач, направленных на:**

- развитие и разработку новых алгоритмов валидации сообщений системы автоматического зависимого наблюдения;
- развитие и разработку новых методов валидации сообщений системы автоматического зависимого наблюдения;
- разработку информационных систем, обеспечивающих валидность сообщений системы автоматического зависимого наблюдения;
- применение методов машинного обучения для анализа сообщений системы автоматического зависимого наблюдения.

**Практическая значимость работы состоит в том, что в ней:**

- показана возможность несанкционированного вмешательства в систему АЗН-В посредством генерации ложных сообщений АЗН-В;

– определены алгоритмы обработки и фильтрации данных АЗН-В;
– найдены оптимальные математические методы определения местоположения ВС в условиях несанкционированного вмешательства при управлении воздушным движением;
– выбраны оптимальные алгоритмы машинного обучения для валидации данных АЗН-В;
– задача валидации сообщений автоматического зависимого наблюдения в условиях несанкционированного вмешательства при управлении воздушным движением может быть решена с помощью одной наземной станции.

**Положения, выносимые на защиту:**

1. Результаты анализа мер противодействия несанкционированному вмешательству в работу системы автоматического зависимого наблюдения.
2. Алгоритм выбора математической модели метода мультилатерации, обеспечивающий наилучшее определение местоположения ВС при заданном количестве станций приема.
3. Метод монолатерации на основе методов машинного обучения.
4. Гибридный алгоритм основанный на использовании методов моно- и мультилатерации.
5. Оценка эффективности методов валидации сообщений автоматического зависимого наблюдения при различных условиях функционирования системы и разных типах несанкционированного воздействия при управлении воздушным движением.
6. Архитектура системы анализа и фильтрации сообщений автоматического зависимого наблюдения.

**Апробация результатов.** Основные результаты работы докладывались на:

– международных НТК;
– всероссийских совещаниях-семинарах.

**Личный вклад.** Автором была сформулирована актуальная научно-техническая задача, проведена ее декомпозиция и определен определен комплекс частных задач, требующих решения. Автором лично:

– разработана модель угроз АЗН-В в соответствии со стратегией ИКАО на основе модели угроз ФСТЭК;

- проведено исследование метода мультилатерации с использованием необходимого и избыточного количества приемных станций;
- предложен и разработан метод монолатерации, основанный на методах машинного обучения, обеспечивающий решение задачи валидации сообщений АЗН-В при наличии только одной наземной станции;
- разработан гибридный алгоритм, основанный на использовании мульти- и монолатерации;
- разработана и апробирована система анализа и фильтрации сообщений АЗН-В;
- проведен натурный эксперимент несанкционированного вмешательства в систему АЗН-В;
- исследована эффективность методов мультилатерации и монолатерации при наличии несанкционированного вмешательства при управлении воздушным движением.

**Публикации.** По теме диссертационной работы опубликованы 4 (25 с.), 2 (21 с.) из которых были опубликованы в изданиях (по транспорту), рекомендованных ВАК при Минобрнауки РФ.

Также имеются тезисы участия в Международной научно-технической конференции в МГТУ ГА:

- «Актуальные угрозы АЗН-В и методы противодействия», «Гражданская авиация на современном этапе развития науки, техники и общества», Сборник тезисов докладов участников Международной научно-технической конференции, посвященной 45-летию Университета. 2016.
- «Практическое применение методов машинного обучения в задаче определения истинности сообщений системы автоматического зависимого наблюдения», «Гражданская авиация на современном этапе развития науки, техники и общества», Сборник тезисов докладов участников Международной научно-технической конференции, посвященной 50-летию Университета. 2021.

**Реализация результатов** работы проводилась при выполнении инициативных НИР в МГТУ ГА:

- НИР «Вопросы избыточности в задаче анализа аэронавигационных данных», Грант ученого совета МГТУ ГА:
  506-15/гр., МГТУ ГА, 2015-2016 г.

**Объем и структура работы.** Диссертация состоит из введения, четырёх глав, заключения и двух приложений. Полный объём диссертации составляет 171 страницу с 55 рисунками и 5 таблицами. Список литературы содержит 67 наименований.

# Глава 1. Анализ состояния вопроса и постановка задачи исследования

Система управления воздушным движением выполняет решающую роль в обеспечении безопасности полетов ВС, решая задачи проведения судов над зонами ответственности без опасного сближения по вертикали и горизонтали, донесения сведений до судна, и информирования его об окружающей обстановке, включая данные о погоде, а также местоположении других участников воздушного движения (ВД). В данном разделе будут рассмотрена современная система АС УВД, ее роль в единой системе организации воздушного движения, наиболее критичные элементы инфраструктуры управления полетами с точки зрения безопасности полетов и перечень угроз несанкционированного вмешательства, влияющих на нормальное функционирование АС УВД.

## 1.1 Анализ системы управления воздушным движением с использованием системы автоматического зависимого наблюдения

Управлением воздушным движением на территории Российской Федерации занимается Единая Система организации воздушного движения (ЕС ОрВД) [57]. Данная система является стратегически значимой для безопасности государства и безопасности использования воздушного пространства. С точки зрения структуры, Единая система состоит из руководящего органа в лице Федерального агентства воздушного транспорта (ФАВТ) и ряда оперативных органов – органов обслуживания воздушного движения (ОВД), которые являются подразделениями ФГУП “ГК по ОрВД”:

1. Главный центр (ГЦ) Единой Системы.
2. Зональные центры (ЗЦ) Единой Системы.
3. Региональные центры Единой Системы.
4. Районные центры Единой Системы.
5. Вспомогательные районные центры Единой Системы.

Рассмотрим более подробно Главный Центр Единой Системы ОрВД. ГЦ предназначен для планирования и координирования использования воздушного пространства, организации воздушного движения, обеспечения разрешительного порядка использования воздушного пространства, контроля за соблюдением Федеральных правил использования воздушного пространства Российской Федерации в пределах воздушного пространства Российской Федерации и районов, где ответственность за организацию воздушного движения возложена на Российскую Федерацию[58]. Зональные, региональные, районные центры выполняют те же функции, что и Главный центр но в своей зоне, своем регионе, своем районе ЕС ОрВД. Согласно Приказу Росавиации[60], перечень оперативных органов ЕС ОрВД состоит из 151 центра, выполняющих необходимые функции в рамках задач Единой системы. Для осуществления безопасности полетов, каждый из центров ОВД должен выполнять задачи по диспетчеркому, полетно-информационному обслуживанию, а также аварийному оповещению. В рамках данной работы наибольший интерес представляет диспетчерское обслуживание, поскольку именно данная задача непосредственно связана с получением анализом аэронавигационных данных, именно данная задача является наиболее критичной с точки зрения безопасности воздушного движения.

Обслуживание воздушного движения осуществляется путем передачи органами ОВД диспетчерских указаний, разрешений, рекомендаций и дополнительной информации. Диспетчерским обслуживанием обеспечиваются как полеты по приборам (ППП) в ВП классов А и С, по правилам визуальных полетов (ПВП) в ВП класса С, так и все виды аэродромного движения на контролируемых аэродромах. Таким образом процент покрытия полетов почти полностью покрывает все возможные на территории РФ.

Для выполнения задач по обслуживанию воздушного движения, применяются следующие системы наблюдения:

- первичный обзорный радиолокатор (ПРЛ);
- вторичный обзорный радиолокатор (ВРЛ) с использованием моноимпульсного метода или режима S;
- АЗН-В.

Данные системы могут применяться как самостоятельно, так и в сочетании с другими. Выбор тех или иных систем основывается на выполнении надежного перекрытия в пределах района, удовлетворительной вероятности об-

наружения, точности и целостности, а также приемлемой доступности данных от участвующих воздушных судов, в случае применения технологии АЗН-В.

Рассмотрим и проанализируем различия в способах опознавания ВС при использовании первичной радиолокации (ПРЛ), вторничной радиолокации (ВРЛ), а также АЗН-В. Исходя из принципов заложенных в те или иные системы опознавания, можно выделить следующие ключевые особенности:

- в ПРЛ опознавание судна определяется через установление взаимосвязи между радиолокационным отображением и воздушным судном с обязательным осуществлением сеанса радиосвязи между диспетчером и ВС и получением необходимой информации;
- в случае с ВРЛ происходит распознавание позывного ВС или дискретного кода ВРЛ, включая режим S. Для распознавания производится запрос на борт ВС;
- в случае с АЗН-В распознавание осуществляется напрямую исходя из индекса ВС в сообщении АЗН-В.

С точки зрения несанкционированного вмешательства наибольший интерес представляет информация, полученная через систему АЗН-В, поскольку её приём осуществляется наземными службами без установления дополнительных сеансов радиосвязи и без осуществления запроса в сторону ВС. Для определения критической важности аэронавигационной информации, рассмотрим основные операции, производимые наземными службами для обеспечения безопасности воздушного движения и эффективного использования воздушного пространства.

Основную работу по обслуживанию воздушного движения выполняет диспетчер. Согласно приказу Министерства транспорта РФ[59], утвердившему типовые технологии работы, диспетчера ОВД должны:

- ознакомиться с погодой на аэродроме (включая запасные), его состоянием, ограничениями и запретами на полеты, номером ВПП, наличием запасных аэродромов и суточным планом воздушного движения;
- уточнить выполнение и изменения в суточном плане, местоположение ВС, с которыми установлена связь;
- проверить корректность установки посадочных знаков, магнитного путевого угла (МПУ) ВПП, работу технических средств связи и прочей аппаратуры;

- контролировать прибытие экипажей ВС, информировать экипаж ВС об условиях полета;
- обеспечивать вылеты, включая вылеты задержанных рейсов и рейсов вне расписания;
- информировать об изменении в суточном плане всех участников воздушного движения;
- следить и контролировать заходы на посадку и вылеты ВС в подконтрольной зоне;
- контролировать движение ВС по маршруту руления.

В виду возросшей интенсивности воздушного движения и ограничения в возможностях человека, многие операции, такие как обеспечение и контролирование прибытия/вылетов ВС, руления по аэродрому, а также информирование всех участниках об изменениях диспетчер не в состоянии выполнить за необходимое время без потери качества работы [46; 56]. Для решения этой задачи для диспетчерского обслуживания воздушного движения используются автоматизированные системы управления воздушным движением (АС УВД). На данный момент в РФ системы АС УВД представлены двумя поставщиками: АО "ВНИИРА" и ООО "НИТА" . Поскольку логическая структура АС УВД у данных производителей не отличается, при исследовании вопроса защищенности АС УВД отправной точкой является типовая схема информационного взаимодействия. Рассмотрим более детально ключевые модули современных АС УВД, возможности по защите информационных потоков и противодействию возможным атакам, а в случае недостаточного функционала - предполагаемых мер по устранению недостатков с точки зрения защиты информации.

В общем случае АС УВД представляет собой архитектуру следующего вида:

Рисунок 1.1 — Структурная схема АС УВД

АС УВД состоит из ряда взаимосвязанных комплексов и систем (Рис. 1.1):

– подсистема сбора информации (ПСИ);
– подсистема связи и передачи информации (ПСПИ);
– вычислительный комплекс (ВК);
– подсистема отображения информации;
– подсистема связи с ВС (ПСВС).

Подсистема сбора информации получает данные от датчиков различных типов, включая ПРЛ, ВРЛ, АЗН-В, а также метеоинформацию и данные из соседних центров УВД. Информация, поступающая в данную подсистему, подразделяется на статическую и динамическую. К статической относятся параметры трасс и воздушных судов, но в рамках исследования наибольший интерес представляет именно динамическая информация, поскольку к ней относятся такие критично важные данные как: координаты ВС, высота полета, бортовой номер или номер рейса, остаток топлива, аварийные сообщения и метеорологические данные.

В качестве датчиков используются системы наблюдения, использование тех или иных типов (ПРЛ, ВРЛ, АЗН-В) определяется рядом условий по перекрытию, вероятности обнаружения, точности и целостности.

Согласно Федеральному закону о безопасности критической инфраструктуры РФ[66], системы АС УВД можно отнести к объектам критической информационной инфраструктуры и категоризировать их как социально, оборонно и экономически значимыми, поскольку отказ или сбой систем АС УВД повлечет за собой:

- ущерб жизни и здоровью людей;
- нарушение транспортной инфраструктуры;
- отсутствие доступа к государственной услуге;
- прямой ущерб бюджету РФ.

Таким образом необходимо определить наиболее уязвимые с информационной точки зрения подсистемы АС УВД, минимизировать риски от возможного несанкционированного вмешательства и предложить меры по оптимизации ключевых показателей.

Требования к обеспечению информационной безопасности в автоматизированных системах управления описаны в приказе №31 от 14.03.2014 (ред. от 23.03.2017) Федеральной службой по техническому и экспортному контролю (ФСТЭК)[61]. Согласно данному документу объектом защиты является информация о параметрах управляемого объекта (входная информация), командная (выходная) информация, благодаря которой осуществляется управление объектом, командная информация, а также контрольно-измерительная и иная информация необходимая для функционирования системы. Вторым объектом защиты является программно-технический комплекс, включающий технические средства и программное обеспечение. Для определения необходимых объектов защиты АС УВД, рассмотрим соответствие её элементов составляющим автоматизированной системы управления в соответствии с рассматриваемым приказом. Основываясь на используемых в данный момент современных АС УВД "Синтез"(производитель - АО "ВНИИРА") и АС УВД "Альфа"(производитель - ООО "НИТА") приведем схему информационного взаимодействия [64] между техническими и программными элементами системы.

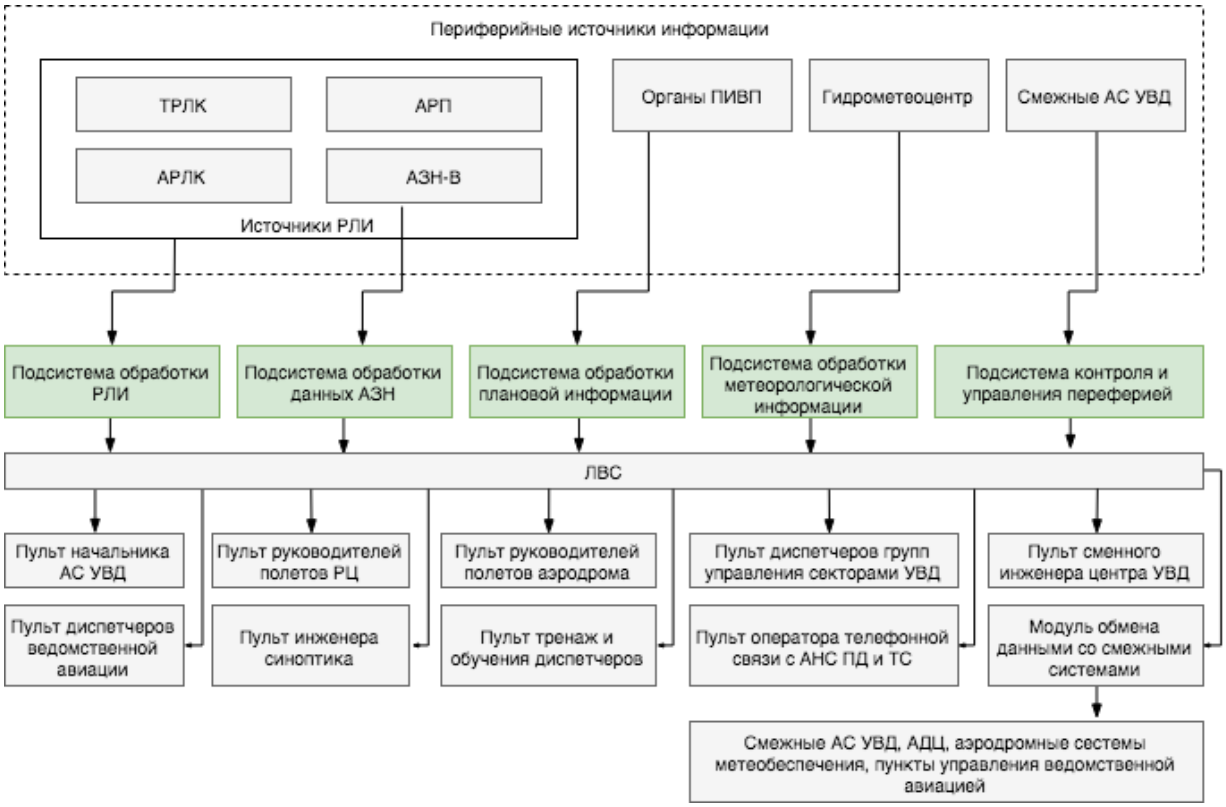



Рисунок 1.2 — Схема информационного взаимодействия ПО АС УВД с периферийными источниками полетных данных и смежными системами

Исходя из схемы на Рис. 1.2 становится понятно, что входной информацией является РЛИ (радиолокационная информация), ПИ (плановая информация), МЕТЕО (метеоинформация), и информация, полученная от смежных АС УВД, а выходной - данные от подсистем обработки, которые используются сотрудниками наземных служб и могут быть переданы как смежным подсистемам АС УВД, так и непосредственно через подсистемы связи на борт воздушного судна. Программно-технический комплекс в свою очередь отвечает за прием и обработку входной информации и предоставление выходной информации на ЧМИ (человеко-машинный интерфейс). К таким интерфейсам относятся пульты начальников, руководителей и диспетчеров наземных служб, а также различные модули по взаимодействию со смежными системами.

Рассмотрим применяемые средства по защите информации в современных АС УВД. В аппартано-программном комплексе СЗИ "Сфера"(производитель ООО "НИТА"), используемом в АС УВД "Альфа" , информационная безопасность автоматизированной системы достигается следующими мерами [55]:

- контроль доступа к файлам;
- контроль целостности сети;
- контроль целостности файлов;
- управление и настройка подсистемы доступа к конфиденциальной информации (ПДКИ);
- работа с защищаемой информацией.

Данный комплекс используется для исключения несанкционированного доступа к информации, хранимой и обрабатываемой в автоматизированных системах. Благодаря данной системе обеспечивается целостность и достоверность информации внутри программно-вычислительного комплекса АС УВД. Аналогичной системы для АС УВД "Синтез"на момент написания работы не было представлено в официальных документах компании.

Однако, даже рассматривая систему АС УВД "Альфа" и СЗИ "Сфера" нельзя говорить о полной защите, поскольку помимо атак на целостность и достоверность внутри системы, необходимо учитывать возможность несанкционированного вмешательства на входную информацию, в первую очередь на радиолокационную. Так, согласно документу ИКАО 9924 «Руководство по авиационному наблюдению» [16], для использования АЗН в режиме вещания (АЗН-В) наземными службами необходима проверка информации, поступающей от воздушных судов (ВС) с помощью вторичной радиолокации (ВРЛ) или мультипозиционных систем наблюдения (МПСН). Данные проверки необходимы для реализации работы технологии АЗН-В по линии связи 1090ES. Учитывая, что достоверность и целостность информации в классическом варианте ведения наблюдения обеспечивается физическими принципами - освещением электромагнитной волной цели (в случае гражданской авиации - воздушного судна) и приемом эха этой волны с подсчетом параметров, то в современных системах наблюдения, таких как АЗН-В используется принципиально новый подход определения местоположения цели, где знание о координатах ВС извлекается из сообщения по незащищенному каналу связи, переданного непосредственно самим судном. В условиях новой парадигмы наблюдения, наибольший упор

необходимо делать на исследование возможностей несанкционированного вмешательства и методов противодействия.

## 1.2 Анализ несанкционированного вмешательства в систему автоматического зависимого наблюдения

На данный момент не существует подходящей модели угроз ни для инфраструктуры АС УВД, ни для отдельных ее компонентов, однако ее разработка является необходимым шагом для классификации и регламентации угроз, направленных на функционирование критически важной системы, обеспечивающей безопасность полетов. Для анализа угроз АЗН-В рассмотрим и адаптируем под реалии пассивного радионаблюдения средствами АЗН-В модель угроз ФСТЭК [44]. Согласно базовой модели угроз безопасности персональных данных (УБПДн) при их обработке в информационных системах персональных данных (ИСПДн) , наибольший интерес представляет вид угрозы, связанный с "преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель)" - поскольку АЗН-В является открытой системой, то и атаки на неё будут производиться изнутри этой открытой системы. По типу информационной системы наиболее подходящей является - "угроза безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена)" - поскольку система АЗН-В представляет собой сеть, состоящую из множества участников - воздушных судов и наземных станций, действующих в одном информационном поле. По способу реализации - "угрозы специальных воздействий на ИСПДн" - под специальными воздействиями здесь, применимо к АЗН-В, являются попытки блокировать либо видоизменять сообщения АЗН-В, тем самым вводя в заблуждение легитимных пользователей ИСПДн. Очевидно, что в условиях электромагнитной среды передачи для осуществления данной атаки необходимо применять радиотехнические средства, позволяющие влиять на информационный радиообмен внутри системы. По виду несанкционированных действий - "угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение" - по сути данный вид несанкционированных действий частично перекрывает возможные угрозы на систему. По используемой уязвимости -

"угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных" - ввиду открытости протокола АЗН-В и особенностей условий передачи сообщений. По объекту воздействия - "угрозы безопасности ПДн, передаваемых по сетям связи" - объектом воздействия является непосредственно само сообщение АЗН-В, поскольку именно оно содержит критически важную информацию для участников воздушного движения.

Примем за персональные данные сообщения АЗН-В и приведем суммарную характеристику модели угроз АЗН-В.

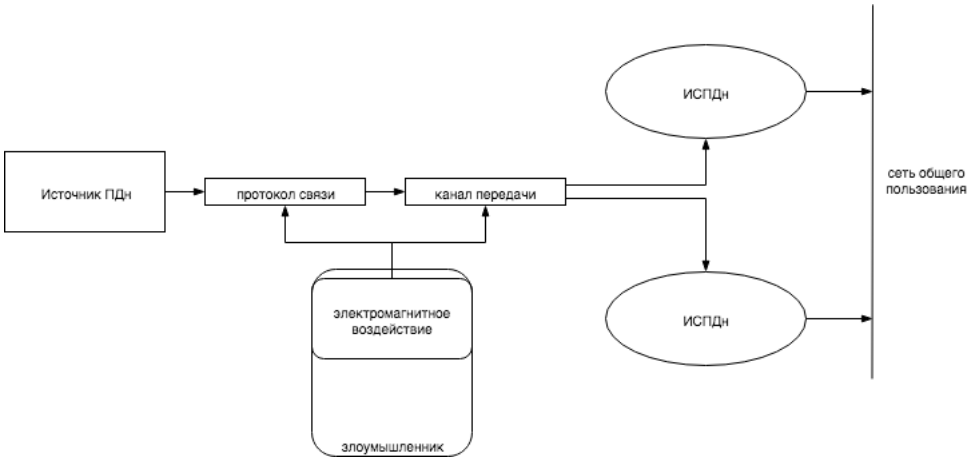



Рисунок 1.3 — Общая схема модели угроз АЗН-В

Для более детального определения угроз, рассмотрим архитектуру современной системы наблюдения (Рис. 1.4), выделив её наиболее уязвимые стороны и проанализировав влияние атак на безопасность воздушного движения.

На схеме показано взаимодействие участников воздушного движения в ключе применения тех или иных систем наблюдения – как традиционных (помечены серым цветом), так и современных (отображены как блоки синего цвета). В верхней части схемы располагаются ВС, оборудованные средствами для возможности собственного наблюдения со стороны наземных служб, а также со стороны других ВС, оборудованных оборудованием АЗН-В. В качестве классических средств на данной диаграмме представлены средства посадочных радиолокаторов (ПРЛ), вторичных обзорных радиолокаторов (ВОРЛ) в различных режимах взаимодействия (Mode A, C, S), мультипозиционных систем наблюдения (МПСН), аэродромных и трассовых обзорных радиолокаторов (ОРЛ-А/Т), автоматических радиопеленгаторов (АРП), радиолокационных станций обзора летного поля (РЛС ОЛП). В качестве современных средств на диаграмме

представлены наземные станции АЗН-В, работающих по протоколам 1090 ES и VDL-4:

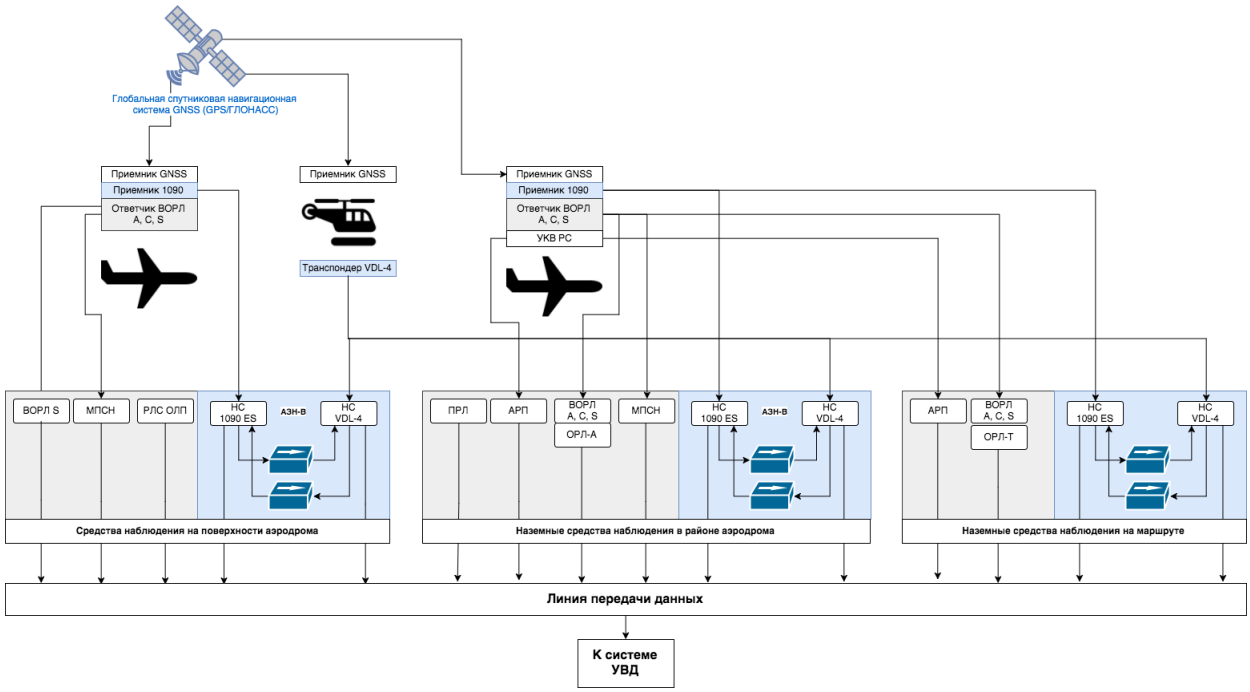



Рисунок 1.4 — Схема архитектуры современных систем наблюдения.

Такие организации как FAA, так и EUROCONTROL называют технологию АЗН-В приемником традиционных радарных систем наблюдения. В связи со своей быстрой окупаемостью при внедрении, низким эксплуатационным затратам, возможностям масштабирования и соответствию современным концепциям АС УВД (NextGen, Single European Sky), приемопередатчиками АЗН-В оснащают все большее количество воздушных судов, с перспективой дальнейшего отказа от еще используемых сейчас методов первичной радиолокации. Так на март 2021 года в США системами с поддержкой технологии АЗН-В оборудовано свыше 150000[3] воздушных судов, причем все современные суда изначально экипируются передатчиками АЗН-В.

Рассмотрим принципы АЗН-В и место в иерархии современных систем наблюдения. С точки зрения развития систем наблюдения, АЗН-В является самой передовой технологией, принципиально отличающейся от технологий наблюдения своих предшественников. Традиционное радионаблюдение использует технологии первичной радиолокации (ПРЛ), либо вторичной радиолокации (ВРЛ) с необходимостью периодического опроса всех судов в пределах действия локатора. В случае с ПРЛ используется зондирующий сигнал, который не несет никакой информации, а выступает как средство определения расстояния до цели,

от которой был отражен сигнал. В случае с ВРЛ имеет место быть архитектура типа «запрос-ответ», в которой воздушное судно отвечает не «эхом», а пакетом данных с конкретной информацией об идентификации ВС (ID воздушного судна) в случае использования транспондера режима «A» (Mode A) или информацией об идентификации и высоте ВС в случае использования транспондера режима «C» (Mode C). Местоположение ВС в данном случае высчитывается также, как и для Первичной радиолокации. Продолжением ВРЛ в режимах A и C стала технология передачи режима «S» (Mode S). Принципиальное отличие этого режима – передача позывного и высоты с заданной периодичностью, без необходимости запроса со стороны наземных станций. Следующей, и на данный момент последней утвержденной технологией, является АЗН-В. По факту эта технология является надстройкой над Mode S в режиме расширенного пакета данных в 112 бит, основной особенностью которой является передача местоположения непосредственно в пакете данных, на ряду с идентификатором и высотой, как в режимах Mode A/C/S. АЗН-В это полностью новая парадигма управления воздушным движением. Каждый участник воздушного движения, оборудованный системой АЗН-В (OUT) передает свое местоположение и скорость другим участникам, чье оборудование имеет возможность принимать данные сообщения АЗН-В (IN). Местоположение определяется исходя из данных полученных расположенным на борту GPS/ГЛОНАСС приемника. Сообщения также содержат такую информацию как ID, степень срочности, уровень неопределенности.

Всего существует 3 глобальных стандарта принятых организацией ИКАО для возможности осуществления работы АЗН-В: 1090 ES (1090 Extended Squitter), UAT (Universal Access Transceiver), VDL mode 4 (VHF Data Link mode 4). Использование того или иного стандарта определяется тем, к какому виду гражданской авиации относится воздушное судно. Так, в Российской Федерации в соответствии с утвержденной Минтрансом России программой для коммерческой авиации предполагается использование 1090 ES, а для авиации общего назначения (АОН), вертолетов и беспилотной авиации – VDL-4. В США и странах Европы вместо VDL-4 используется UAT. Стоит отметить, что стандарт VDL-4 гораздо более защищен от киберугроз нежели 1090ES, однако использование данного стандарта все еще под вопросом, поскольку поручение Президента РФ от 29.04.2016 № Пр-800 требует «разработать и утвердить комплекс

мероприятий по скоординированному внедрению единого стандарта системы автоматического зависимого наблюдения за магистральными воздушными судами и воздушными судами авиации общего назначения», где именно протокол 1090ES был утвержден как единый стандарт для использования в воздушном пространстве (ВП) России [63].

В коммерческой авиации, в отличии от авиации общего назначения, АЗН-В реализовано посредством использования транпондеров Mode S, которые являются обязательными при выполнении полетов. Схема использования АЗН-В на основе Mode S приведена ниже:

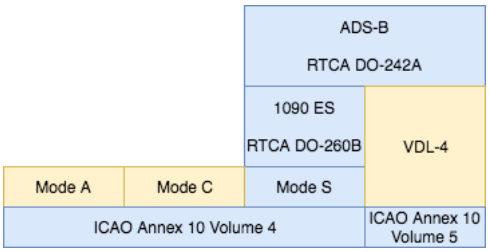



Рисунок 1.5 — Стек протоколов Mode S.

Рассмотрим протокол 1090 ES. В соответствии с названием, протокол передачи данных использует частоту 1090 МГц в полосе шириной ± 1,3 МГц для передачи информации как на наземные станции, так и другим ВС участникам ВД (для передачи данных с наземных станций используется частот 1030 МГц). Для передачи сообщений АЗН-В используется фазово-импульсная модуляция (ФИМ). При каждом временном интервале, равном 1 мкс, бит указывается либо отправкой импульса 0,5 мкс в первой половине интервала («1»), либо во второй половине («0»). Важно отметить, что данный тип модуляции очень чувствителен к отраженным сигналам и многолучевой дисперсии, что может играть важную роль в соображениях безопасности протокола.

В режиме передачи Mode S существуют 2 различные длины сообщения – 56 бит и 112 бит, в свою очередь для АЗН-В использует только длинный формат сообщения:

В каждом сообщении согласно протоколу передачи 1090ES присутствуют поле DF (downlink format), описывающее тип сообщения – так при выставленном значении DF=17, сообщение определяется как сообщение расширенного сквиттера, благодаря чему будет производиться учет дополнительных 56 бит информации в поле ME. В поле CA размещается информация о возможностях транспондера, а в поле AA – содержится ICAO код ВС, что обеспечивает иден-

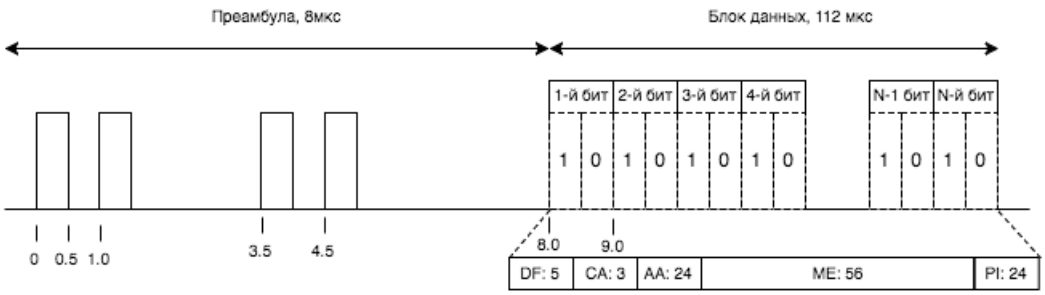



Рисунок 1.6 — Общая схема состава сообщения АЗН-В.

тификацию ВС в воздушном пространстве. Наконец последнее поле PI длиной 24 бита используется в качестве контрольной суммы и служит механизмом для коррекции возможных ошибок. Исходя из того, что непосредственно под данные АЗН-В в одном сообщении отведено только 56 бит, формат передачи 1090ES накладывает существенные ограничения на применение возможных средств по верификации сообщений, о которых будет сказано чуть позже.

Исследования в области безопасности современных систем наблюдения [7; 15; 24; 30] указывают на множество потенциальных уязвимостей, используя которые становится возможным повлиять на работу систем управления воздушным движением. Большинство данных уязвимостей относятся к системе АЗН-В. Рассмотрим их подробнее, и основываясь на исследованиях [25], произведем их классификацию исходя из их особенностей и типов воздействия на ключевые компоненты АС УВД.

Наиболее простой формой атаки среди многих уязвимостей является анализ радиотрафика. В работе [25] эта пассивная атака определяется как “разведка воздушных судов”. Поскольку в АЗН-В используются незашифрованные сообщения в среде, где каждый имеет к ней непосредственный доступ, возможность прослушивания не является неожиданной, более того данная возможность изначально заложена в архитектуру АЗН-В. Прослушивание, не является прямой угрозой для безопасности, однако информация полученная от участников воздушного движения, наземных станций может послужить основой для более сложных активных атак.

Аналогичная по простоте пассивной атака подслушивания, атака зашумления канала позволяет вывести из состояния работоспособности как оборудование АЗН-В воздушных судов, так и (в большей мере) наземных станций. Согласно банку данных угроз безопасности информации ФСТЭК, данная атака определяется как "Угроза приведения системы в состояние отказ в обслужива-

нии УБИ.140. Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов. В случае зашумления канала связи, несанкционированное вмешательство заключается в недостатке сетевого протокола системы АЗН-В - как и все сетевые протоколы, использующие радиоканал связи, 1090ES подвержен атаке посредством электромагнитного вмешательства при передаче данных. Также, согласно перечню угроз ФСТЭК, данная атака также может быть классифицирована как "Угроза неправомерных действий в каналах связи УБИ.069. Последствиями реализации такой угрозы будут:

– нарушение доступности;
– нарушение целостности.

Для осуществления атаки необходимо сгенерировать сигнал большой мощности на частоте 1090 МГц и находиться в районе приемопередающих устройств АЗН. В отличие от АЗН-В, наблюдение первичными радиолокаторами гораздо менее подвержено данному типу атаки чем наблюдение АЗН-В. Этому способствует ряд факторов: высокая испускаемая мощность сигнала радара, вращение локатора, узконаправленный сигнал. Возможность осуществления такого типа атаки на систему АЗН-В была продемонстрирована в лабораторных условиях в исследовании [36]. Примерами [25] реализации данного воздействия в реальной жизни являются:

– DOS АЗН на стороне ВС;
– DOS АЗН на стороне наземных служб.

Следующей по сложности атакой является атака ложной цели (спуфинг). Спуфинг – это термин применяемый в сетевой безопасности, который характеризует практику злонамеренного внедрения сообщения в канал связи. При этом злоумышленник маскируется под легитимного пользователя и может отправлять данные, которые будут приниматься и обрабатываться пользователями атакуемой системы. Согласно банку данных угроз безопасности информации ФСТЭК, данная атака определяется как "Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027, а также как "Угроза использования слабостей кодирования входных данных УБИ.033. Угроза заключается в возможности дезинформирования пользователей или автоматиче-

ских систем управления путём подмены или искажения исходных данных, а также в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).

В рамках АЗН-В сообщением является пакет данных отправленных по протоколу 1090ES, который при необходимой мощности передачи будет обработан участниками ВС с приемными устройствами АЗН-В: наземными станциями и воздушными судами. Производится спуфинг для введения в заблуждение как сотрудников наземных служб, так и пилотов ВС. В ряде работ было показано воспроизведение данного типа атаки, а учитывая открытый протокол взаимодействия, доступность и невысокую стоимость оборудования, для ее осуществления достаточно базовых знаний в области использования программно определяемых радиосистем (SDR) [34]. Примерами [25] реализации данного воздействия в реальной жизни являются:

– ложное информирование наземной службы обеспечения полетов;
– ложное информирование экипажа ВС.

Обладая знаниями о частоте испускаемого сигнала воздушным судном, легитимные сообщения могут быть «удалены» из среды передачи данных благодаря использованию конструктивной и деструктивной интерференции. Атака данного типа является труднореализуемой, поскольку для деструктивной интерференции необходимо сгенерировать и передать сигнал обратный легитимному в точное время, и наиболее близко к приемному устройству. Результатом атаки будет полное либо частичное затухание легитимного сигнала. Также атака может быть реализована посредством конструктивной интерференции. В результате данного типа воздействия на приемной стороне возникает достаточно большое количество ошибок, коррекция которых ограничена лишь 5-ю битами. Данная атака является более сложной чем простое зашумление канала поскольку может воздействовать на конкретные цели, а не на весь радиоэфир в целом. Примерами [25] реализации данного воздействия в реальной жизни являются [25]:

– скрытие ВС.

Еще более сложной атакой с точки зрения реализации, основанной на принципе предыдущей, является атака модификации сообщения АЗН-В. Из-

менение данных на физическом уровне выполняется с помощью двух разных подходов: деструктивное воздействие помехой и атака с манипуляцией битами. Под деструктивным воздействием в данном случае означает то, что злоумышленник посылает мощный сигнал для замены части или всего целевого сообщения. Манипуляция битов в свою очередь подразумевает преобразование битов в пакете данных на обратное значение (из значения “1” в “0” и наоборот). В обоих случаях данные вводятся незаметно для участников обмена сообщениями АЗН. Также эта атака может быть осуществлена путем удаления и последующего внедрения сообщения, однако именно модификация сообщения является наиболее опасной угрозой, поскольку в этом случае происходит объединение легитимного и нелегитимного сообщения и идентифицировать такое воздействие становится еще более сложным. Практическая реализация такого вида атаки была показана в работах [22] и [42]. Примерами [34] реализации такого воздействия в реальной жизни являются:

– виртуальный угон ВС;

– виртуальное изменение траектории движения ВС.

Описанные выше атаки можно классифицировать исходя из уровня воздействия, осуществляемого метода, силы влияния и сложности осуществления. Сравнительный анализ данных угроз приведен в таблице 1.1

Таблица 1.1

Сравнительная таблица атак на систему АЗН-В

| Тип атаки | Уровень | Метод | Воздействие | Сложность | Ссылки |
|---|---|---|---|---|---|
| Разведка | Физический, приложения | Анализ радиотрафика | Слабое | Низкая | [7; 25; 34] |
| DOS АЗН на стороне ВС | Физический | Зашумление канала | Среднее | Низкая | [7; 25; 34] |
| DOS АЗН на стороне НС | Физический | Зашумление канала | Среднее | Средняя | [7; 25; 34] |
| Ложное информирование ВС | Приложения | Спуфинг | Сильное | Низкая | [7; 25; 34] |
| Ложное информирование НС | Приложения | Спуфинг | Среднее | Средняя | [7; 25; 34] |
| Скрытие ВС | Физический | Удаление сообщения АЗН-В | Сильное | Низкая | [7; 25; 34] |
| Виртуалный угон ВС | Физический, приложения | Модификация сообщения АЗН-В | Сильное | Средняя | [7; 25; 34] |
| Виртуальное изменение траектории движения ВС | Физический, приложения | Модификация сообщения АЗН-В | Сильное | Средняя | [7; 25; 34] |

## 1.3 Постановка задачи исследования

Несанкционированное вмешательство в результате применения атаки ложной цели, модификации и блокирования сообщений АЗН-В может быть критичным для работы АС УВД и может влиять напрямую на безопасность полетов в том случае, когда рассматривается наихудший сценарий: отсутствуют ПРЛ и ВРЛ, нет иных средств ведения наблюдения, помимо системы АЗН. Данный сценарий может быть рассмотрен для отдаленных и труднодоступных регионов, где либо наличествует недостаточное радарное перекрытие, либо оно отсутствует полностью. Помимо этого, данный сценарий может быть рассмотрен при возникновении ЧС на основных радиолокационных станциях, например остановкой электроснабжения. Ввиду того, что приемники АЗН могут быть оснащены альтернативными источниками питания, данная система может являться по факту единственной действующей. Наконец, предлагаемый сценарий может рассматриваться в рамках перспективы развития АС УВД, как в России, так и в мире, ведь, согласно планам развития навигационных систем, значению системе АЗН будет уделяться все большее значение.

На данный момент, по данным Евроконтроля, основным подтипом АЗН является технология АЗН-В, в то время как АЗН-К используется не так широко. В то же время АЗН-В является наиболее уязвимым типом данной технологоии, поскольку он использует общедоступные частоты. Наиболее важным условием для противодействия несанкционированному вмешательству на АЗН является сохранение текущей инфраструктуры АС УВД. Таким образом, метод благодаря которому будет осуществляться противодействие данным угрозам, должен иметь возможность интеграции с современными АС УВД, причем затраты на его внедрение должны сводиться к минимуму. По большей части, методы и алгоритмы противодействия несанкционированному вмешательству должны нести дополняющий характер, и входить состав прикладной системы, направленной на обеспечение безопасности АС УВД. Внесение изменений в протоколы передачи данных, оборудование ВС, принимающих станций, использование другого типа манипуляции приведет к высоким затратам на создание соответствующих стандартов, переоборудование ВС и функциональных блоков

АС УВД, и, самое главное, приведет к проблеме гармонизации предлагаемого метода с уже существующими технологиями УВД.

Требования по противодействию угрозам несанкционированного вмешательства в систему АЗН-В должны соответствовать существующим авиационным правилам и иным действующим нормативным документам по обеспечению безопасности полетов. Для обеспечения информационной безопасности системы АЗН в части противодействия несанкционированному вмешательству, предлагается использовать методы, внедрение которых, по стоимости не будет превосходить использование вторичных активных РЛС с многократным перекрытием зоны наблюдения.

# Глава 2. Разработка методов и алгоритмов валидации сообщений системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства

## 2.1 Методы противодействия несанкционированному вмешательству на компоненты системы автоматического зависимого наблюдения

Исходя из проведенного анализа угроз, спуфинг-атака, как вид несанкционированного воздействия, направленного на снижение безопасность полетов, является критичной для работы АС УВД при отсутствии покрытия ПРЛ и ВРЛ. Вышеуказанные угрозы АЗН-В определяют необходимость разработки методов и алгоритмов валидации сообщений и создания системы по анализу и фильтрации сообщений АЗН-В поступающих в АС УВД. Поскольку наибольшую угрозу представляют данные АЗН-В, основной упор будет сделан на информацию, поступающую из данной системы. Для определения необходимых мер по обеспечению безопасности АЗН-В и, как следствие, АС УВД, определим требования к методам и алгоритмам валидации сообщений и к системе анализа и фильтрации сообщений АЗН-В.

Существует ряд требований к безопасности АЗН-В, связанных с тем, что данная система необходима для работы в реальных условиях воздушного движения и должна по-прежнему обладать характеристиками широковещательного вещания с условием открытого доступа к информации системы. Для составления требований определим сетевую модель системы АЗН-В, на основании которой будет произведен анализ того, какие именно характеристики необходимы для обеспечения безопасного функционирования АЗН-В и АС УВД в целом.

Примем сетевую модель АЗН-В, как систему взаимодействий, состоящую исключительно из однонаправленных сеансов широковещательной передачи информации. Воздушное судно передает свои координаты, скорость и направление открытым текстом с периодичностью в каждые несколько сотен миллисекунд, что соответствует сетевой концепции "beaconing"(буквально, испускать сигнал), то есть постоянной передачи сигнала, и оповещением всех устройств в среде передаче данных. Таким образом, в данной работе наибольшее внимание

будет уделено так называемой "baecon-based"сетевой безопасности. Для обеспечения работы системы анализа и фильтрации данных, примем, что не имеется каких либо ограничений с точки зрения затухания сигнала, отсутствуют значительные вычислительные ограничения. Также примем, что надежность является не самой главной проблемой, поскольку исходя из проведенных исследований [34] на физическом уровне существует значительная потеря пакетов, равная в среднем значении 33%. Данный показатель будет постоянно увеличиваться из-за возрастающей интенсивности полетов и, как следствие, возрастающей интерференции сигналов. Тип сети АЗН-В - ad-hoc, то есть беспроводная динамическая сеть, с движением узлов сети до 1000 км/ч . Сеанс связи между узлами очень короток и может длиться всего несколько секунд. Также примем, что движение и траектории ВС принципиально и физически никак не ограничены, несмотря на наличие регламентированных воздушных коридоров, трасс и запретных зон. Беспроводная сеть имеет большой диапазон действия и в случае АЗН-В информационное взаимодействие считается выполнимым на расстоянии 100 морских миль.

В работе по безопасности в широковещательных сетях связи авторы Адриан Перриг и Дулиш Тигар [29] определяют два условия обеспечения информационной безопасности (ИБ) в сетях такого типа: получатели знают, что любая полученная информация поступает от соответствующего отправителя, а во-вторых, отправители могут свободно ограничивать получателей широковещательной информации. Конфиденциальность, например, защита сообщений о местоположении для предотвращения атак в воздухе или потери коммерческой тайны не рассматривалась при разработке системы, поскольку это идет в разрез с основными принципами функционирования АЗН-В. В связи с тем, что для осуществления атак на АЗН-В может быть использовано сравнительно недорогое бытовое оборудование [7; 34], обеспечение безопасности сразу становится наиважнейшей областью в исследовании данного типа наблюдения. Основываясь на сетевой модели АЗН-В, определенной выше, приведем необходимые условия обеспечения сетевой безопасности:

– целостность данных: необходимость в неизменности отправляемых данных, без изменения их третий стороной;

- целостность источника: гарантия того, что сообщение отправляется от участника, который утверждает, что именно он произвел отправку сообщения;
- проверка подлинности источника данных: гарантия того, что пакет данных АЗН-В был отправлен из местоположения, заявленного в переданном сообщении;
- обнаружение инцидентов ИБ в течении времени, необходимого для нормального функционирования защищаемой системы;
- защита от DOS-атак на систему защиты;
- масштабируемость системы, обеспечивающей ИБ - этому способствует увеличивающаяся ИВД. Также система не должна увеличивать сетевой трафик на канала 1030/1090 МГц;
- устойчивость к потере пакетов. Зашумленный беспроводной канал не должен уменьшать безопасность и надежность схемы.

Таким образом, рассмотренные особенности системы и условия обеспечения ИБ указывают на необходимость анализа существующих методов защиты АЗН-В в соответствии с требованиями штатного функционирования системы.

На данный момент предложен значительный ряд мер и наработок по противодействию атакам на систему АЗН-В. Кроме того, большое количество исследований было проведено в смежных областях, таких как автомобильные сети и беспроводные сенсорные сети, где важную роль играет широковещательная аутентификация и безопасность. Произведем классификацию существующих методов противодействия угрозам на систему АЗН-В

Как показано на схеме, существует два подхода к обеспечению безопасности АЗН-В: шировоковещательная аутентификация и верификация местоположения. В следующей главе будут подробно изучены все разновидности схем защиты с использованием ассиметричной криптографии для непосредственной аутентификации широковещательной передачи и несколько различных методов, направленных на подтверждение достоверности информации АЗН-В в сообщении.

Среди предложенных, наибольший интерес представляют следующие: применение асимметричных криптографических алгоритмов для создания ЭЦП воздушного судна, использование плановой информации, применение группировки спутниковых космических аппаратов (СКА) для пеленгации ВС,

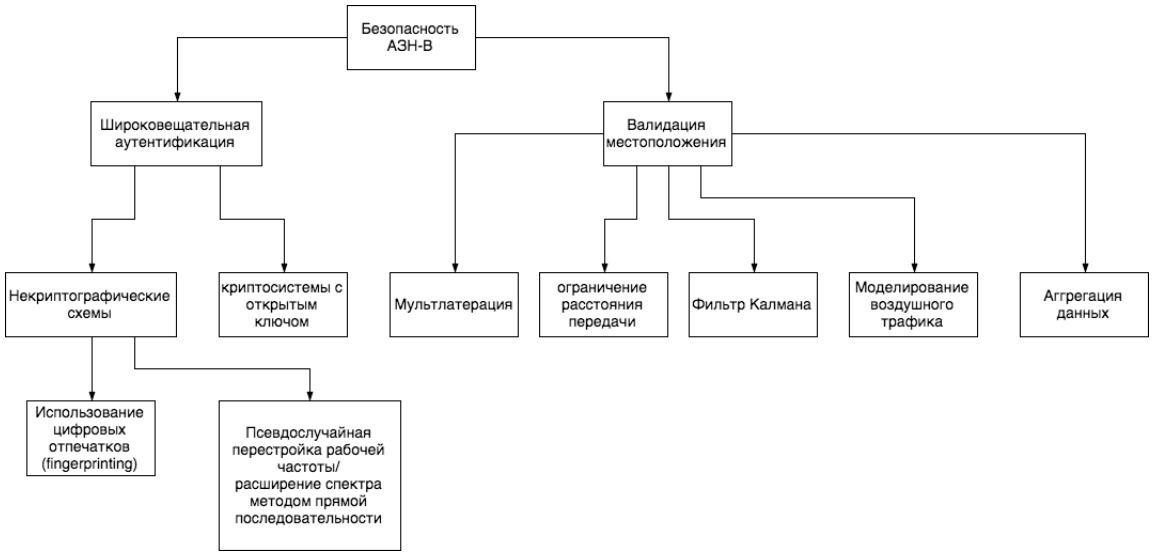



Рисунок 2.1 — Структурная схема методов защиты системы АЗН-В от потенциальных угроз

использование мультилатерационных систем на основе действующих ВРЛ, использование широкозонных мультилатерационных систем, использование узконаправленных пеленгационных антенн, применение алгоритмов машинного обучения.

Применение ЭЦП является наиболее популярным и очевидным методом для отражения данного вида атаки. Применяемые в современных информационных системах асимметричные алгоритмы доказали свое превосходство над симметричными. Сложность решения обратной задачи логарифмирования, лежащая в основе использования односторонних функций в асимметричных алгоритмах, совместно с использованием длинных ключей обеспечивает высокую степень защищенности, не позволяющую злоумышленнику подделать подпись. В ходе исследования методов защиты от несанкционированного воздействия спуфингового типа, была рассмотрена статья [40], в которой предлагалось использование ЭЦП на эллиптических кривых. Данный подход позволяет использовать ключи меньшей длины, чем в RSA (128 бит вместо 1024). Однако данный метод подходит для UAT протокола передачи данных, поскольку он использует кадры длиной в 274 бит. Благодаря такому размеру, в данный пакет, помимо непосредственных данных АЗН, есть возможность поместить данные ЭЦП (авторы статьи предлагают использовать подпись длиной 112 бит). Однако, на территории Российской Федерации используются только протокол 1090 ES, который не позволяет передавать одним кадром сообщение с инкапсулированной в него ЭЦП. В рассматриваемой работе авторы касаются этой проблемы и

приходят к выводу, что при использовании ЭЦП для протокола 1090 ES (наиболее широко используемого), объем передаваемых данных возрастет в 5 раз (путем разбиения ЭЦП на 5 пакетов данных). Возрастание объема передаваемого трафика может негативно сказаться на приеме сообщений АЗН, вызовет повышенную нагрузку на наземные станции и ВС, оборудованные соответствующими приемниками, повысит вероятность блокирования передачи сообщений. Так же, на частоте 1090 МГц, помимо системы АЗН-В работает система предупреждения столкновений (TCAS) [31]. Повышение нагрузки на данную полосу частот может негативно сказаться на безопасности полетов. Более того, использование протоколов ЭЦП для аутентификации ВС может быть невозможно ввиду ограничений на использование криптографических протоколов в некоторых странах, что создаст помехи международному использованию системы АЗН.

Рассмотрим подробнее два наиболее распространенных метода в обеспечении безопасности АЗН-В, а именно широковещательную аутентификацию и различные варианты валидации местоположения судна.

Широковещательная аутентификация, согласно схеме подразделяется на несколько типов.

Рассмотрим возможность использования криптосистем с открытым ключом для определения достоверности передающего устройства, а также определения достоверности самой информации, содержащейся в сообщении АЗН-В. Криптографические средства являются хорошо зарекомендовавшими себя мерами обеспечения защищенной связи в беспроводных сетях и возможность их применения должна учитываться при создании систем наблюдения с использованием технологии АЗН-В. Для дальнейшего анализа пригодности данного метода, определим степень готовности текущей реализации АЗН-В к применению таких средств ЗИ и варианты применения в текущих реалиях работы АС УВД.

Первый вариант заключается в распространении одних и тех же ключей шифрования для всех участников ВД по всему миру, или, по крайней мере, для воздушных судов и наземных станций в заданной зоне выполнения полетов, по сути данный вариант основан на принципах симметричного шифрования. При таком подходе возникает проблема передачи секретных ключей для всех участников. Такая обширная групповая схема шифрования, включая даже общую авиацию, будет считаться крайне небезопасной как для внутренних, так и

для внешних атак - публичная передача ключа является очевидным недостатком симметричного шифрования. Данный недостаток в варианте с симметричным шифрованием не может быть улучшен даже частыми обновлениями ключей (что в свою очередь усложнило бы процесс развертывания шифрования). Ряд авторов изучают различные схемы шифрования, в том числе возможность управления ключами для симметричного шифрования, например, через коммуникационную связь канала управления CPDLC, которую, по их мнению, стоит изучить более подробно. Авторы также дают анализ безопасности и практичности асимметричного, симметричного и сохраняющего формат шифрования. В своем заключении они поддерживают симметричный шифр с использованием алгоритма FFX (сохранение формата, шифрование на основе сети Фейстеля с множественными вариантами реализации), которое может зашифровать нестандартные размеры блоков (то есть 112-битные сообщения ADS-B) с достаточной энтропией. Однако понять трудности внедрения, связанные с ключевым управлением и распределением, достаточно сложно, поскольку на данный момент для ее реализации не предусмотрена соответствующая инфраструктура.

Совсем недавно рядом исследователей был рассмотрен более широкий вопрос о том, как использовать шифрование для защиты АЗН-В, в результате чего был сделан вывод, что проблемы с симметричной криптографией слишком велики для преодоления. Утверждается, что инфраструктура открытых ключей (PKI) является единственным возможным криптографическим подходом и может быть реализована через механизм подписи на эллиптических кривых (ECDSA). Помимо проблемы управления ключами в случае с симметричным шифрованием, была дополнительно проанализирована проблема интерференции сигнала на канале ADS-B, где был приведен ряд доказательств того, что даже без значительного дополнительного трафика, который в настоящее время передается на частоте 1090 МГц, снижение эксплуатационной емкости потенциально может привести к падению системы в целом. Как упоминалось ранее, если требуется широковещательная аутентификация, то требуется асимметричное свойство, характеристика, выполняемая криптографией с открытым ключом. На текущий момент уже существует ряд патентов под именами "Secure ADS-B Authentication System and Method"и "Automatic Dependent Surveillance System Secure ADS-S в которых используется принцип аутентификации с использованием ассиметричного шифрования. Рассмотрим подробнее предложенные вари-

анты аутентификации ВС и произведем анализ эффективности данного метода криптографии в АЗН-В. Основная идея ADS-S состоит в том, чтобы использовать формат запроса/ответа с наземной станцией-аутентификатором, который аутентифицирует каждого участника в своей зоне действия и уведомляет вышестоящий орган и/или всех других участников о попытке любой неудачной аутентификации. Эта концепция требует, чтобы станция имела доступ к всемирной базе данных с защищенными ключами. Исходя из этого возникает ряд вопросов по обеспечению безопасного доступа на чтение и запись ключей в данную БД. Кроме того, ADS-S включает в себя измененную модуляцию и полную перестройку системы обмена сообщениями, что делает ее несовместимой с ADS-B и столь дорогостоящей и крайне сомнительной для широкого распространения в будущем. Другой подход использования асимметричной криптографии состоит в использовании "облегченного"решения инфраструктуры открытых ключей, которое сводится к публикации ретроактивной части ключа: воздушное судно "А"передает подпись, распределенную по нескольким (N) сообщений АЗН-В, так что после каждого N сообщения участники аутентификационного радиообмена получили подпись А. Получатели сохраняют сообщения до тех пор, пока не будет передана полная подпись, после чего они смогут аутентифицировать буферизованные сообщения. Необходимое для этой схемы распределение ключей может быть произведено при плановом обслуживании ВС. Еще одним вариантом использования криптосистем с открытым ключом заключается в использовании криптографии на эллиптических кривых в протоколе UAT (аналог используемого на территории РФ VDL-4). В протоколе UAT информационный обмен происходит посредством более длинных чем в 1090ES сообщений длиной 16 и 32 байта при передаче с ВС и 464 байта в наземных сообщениях. Однако несмотря на большее доступное пространство для аутентификации, авторы указывают на необходимость изменения формата блока данных UAT. Для протокола 1090 ES данный подход потребует все те же 5 сообщений для передачи подписи и временных меток, по причине чего масштабируемость решения в условиях большой загруженности каналов и помех не представляется возможной. Также ведется анализ различных решений для создания инфраструктур открытых ключей для общей системы распределения активов самолетов (AADS). Хотя в работе не обсуждается протокол АЗН-В, а вместо этого основное внимание уделяется распределению программ-

ного обеспечения и данных на наземной инфраструктуре, авторы определяют потребности и требования авиакомпании в инфраструктуре PKI, и представляется правдоподобным, что одна и та же система может быть используется для обеспечения безопасности данных управления воздушным движением. Согласно их анализу, специальный подход без центрального органа, использующего предварительно загруженные сертификаты доверия, может быть использован в качестве краткосрочного решения до тех пор, пока не будет разработана более структурированная долгосрочная инфраструктура открытых ключей. Очевидной идеей централизованного распределения ключей было бы предоставление органам государственного управления в области гражданской авиации, таким как FAA/Eurocontrol/Росавиация, прав центра сертификации. Но необходимо учитывать, что роль центра сертификации - непростая задача. Даже многим специализированным учреждениям приходилось сообщать о многочисленных нарушениях безопасности за последние десятилетия. Кроме того, если эта проблема будет решена достаточно успешно, остается вопрос о том, как воздушные суда в воздушных пространствах, уполномоченных различными органами, могут надежно взаимодействовать друг с другом.

Существуют некоторые естественные недостатки в использовании решения шифрования, которое невозможно преодолеть (либо это потребует существенных изменений в формате передачи данных): - несмотря на шифрование кадров данных, кадры управления не защищены; - шифрование любого вида нарушает совместимость с установленной технической базой; - обмен ключами, как известно, затруднен в беспроводных сетях ad-hoc, которые по определению не имеют централизованного управления. Они часто слишком динамичны и требуют постоянной адаптации. Это приведет к слишком большим накладным расходам как по количеству, так и по размеру сообщений; - открытый характер ADS-B широко рассматривается как особенность. Криптографическая система, реализованная способом, сопоставимым с ADS-S, не обеспечивает публичную широковещательную связь; - одноразовые подписи даже с использованием передовых методов, таких как Merkle-Winternitz, оказались неосуществимыми из-за их накладных расходов в 80 байт и более, для подписи 56 бит информации[9].

Необходимо отметить, что построение любых схем шифрования в рамках существующего стандарта 1090ES достаточно проблематично. Было доказано, что теоретически возможны схемы шифрования в протоколах АЗН-В с большей

пропускной способностью, таких как UAT и VDL-4, однако практическое доказательство масштабируемости и практичности такого решения еще не сделано. Кроме того, на данный момент маловероятно, что UAT/VDL-4 будут играть более значимую роль помимо использования в общей авиации. Таким образом, несмотря на возможности протоколов UAT/VDL-4, традиционная криптография в сочетании с нынешней архитектурой АЗН-В 1090 ES неэффективна и на данный момент очень трудна для реализации.

В противоположность аутентификации воздушных судов и шифрованию сообщений выступают методы верификации местоположения воздушного судна и методы машинного обучения. Главная идея этой группы методов заключается в сравнении информации о местоположении ВС из сообщения АЗН-В с информацией о местоположении, полученной косвенным путем - исходя из параметров распространения сигнала, а также других сопутствующих характеристик. Всего существует несколько способов достижения данной цели, причем некоторые уже применяются в системах АНС, в основном для повышения точности, такие как методы мультилатерации и калмановской фильтрации.

Технология мультилатерации (MLAT) в течении долгого времени применялась для наблюдения над ВС в зоне аэродрома. В настоящее время, эти же методы используются для зон более широкого аэронавигационного покрытия [10], таких как зоны навигационного обеспечения на маршрутах полета и зоны захода на посадку. Такие системы названы Широкозонными Мультилатерационными системами (WAMLAT). Мультилатерация является одной из форм ведения кооперативного независимого наблюдения – система, основанная на данной технологии, использует сигналы, переданные воздушным судном, для вычисления его местоположения по их временным характеристикам. Технология мультилатерации позволяет использовать существующие в настоящее время формы передачи данных, тем самым не требуя внесения изменений в бортовую инфраструктуру ЛА. Для обработки полученных сигналов, необходимы соответствующие требованиям приемники АЗН и центр обработки данных в режиме реального времени. Мультилатерационная система состоит из наземных станций (НС), принимающих сообщения АЗН-В от воздушных судов, и центральный узел обработки данных для вычисления позиции воздушных судов исходя из разницы времен прихода (РВП) сигналов, принимаемых разными

станциями (анализ разностей прихода сигналов от одного и того же источника до нескольких пар приемных пунктов).

Использование технологии мультилатерации в классическом понимании требует использования группировки вторичных радиолокаторов или транспондеров на канале Mode S. Данный метод получил широкое распространение в Европе благодаря тому, что в этом регионе воздушного пространства осуществлено многократное радарное перекрытие. Однако использование запросчиков для работы данного метода вдвое увеличивает трафик в полосе частот. Необходимость дополнительных запросов накладывает затраты на установку дополнительных запросчиков.

Широкозонные мультилатерационные системы или многопозиционные системы наблюдения (МПСН) имеют идентичный принцип работы, что и системы, описываемые выше. Отличительной особенностью данных систем является то, что она направлена на покрытие всего обслуживаемого ВП. Это достигается благодаря использованию группировки наземных станций. На данный момент введены в опытную эксплуатацию такие МПСН как "Мера"(АО «Концерн ВКО «Алмаз - Антей»), "Альманах"(ООО «НПП «ЦРТС») и «Тетра-М» (ПАО «НПО «АЛМАЗ» ТОП «ЛЭМЗ»). Использование пассивного режима позволяет отказаться от дополнительных запросчиков и обойтись лишь приемными станциями АЗН. Данный метод не создает дополнительного трафика в радиоканале, позволяет использовать уже существующее оборудование.

Применение группировки СКА для целей мультилатерации потребует больших затрат на вывод спутников на орбиту. Более того следует иметь ввиду, что для успешной работы системы такая группировка должна охватывать территорию аэронавигационного обеспечения всей страны.

Рассмотрим более подробно технологию мультилатерации, а также являющийся основой данной технологии гиперболический метод определения местоположения (МП) ВС. Разница времена прихода сигналов (РВП) между двумя приемниками соответствует, с математической точки времени, гиперболоиду, на поверхности которого находится ВС (Рис. 2.3). Когда четыре приемника детектируют сигнал, становится возможным определить позицию ВС в трех измерениях путем вычисления пересечений полученных гипербол . В ситуации, когда для вычислений РВП доступны только три приемника, позиция воздушного судна может быть определена лишь на плоскости, однако, если его высота

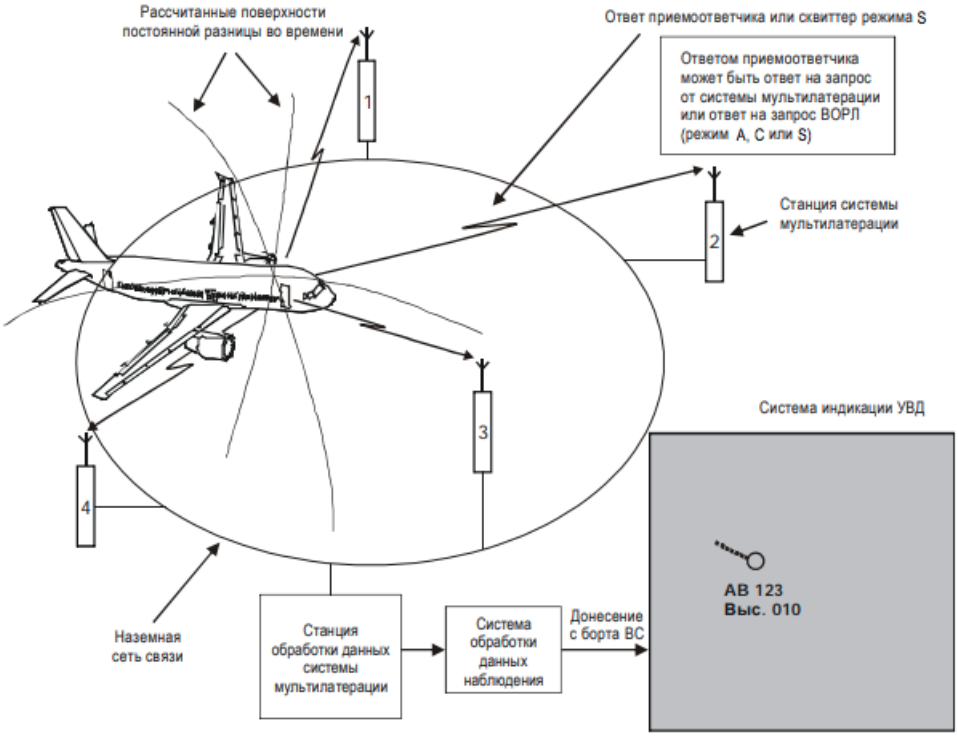



Рисунок 2.2 — Типичная архитектура системы MLAT для наблюдения в целях УВД [17]

известна (например, переданная по каналу Mode-C), может быть получено его положение в трехмерном пространстве. При использовании большего количества антенн, избыточная информация о РВП может быть использована для проверки точности измерений, произведенными другими средствами навигации, а также с целью повышения точности предоставляемой информации для АС УВД.

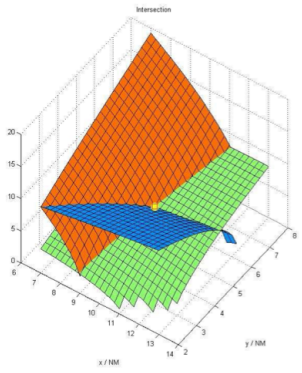



Рисунок 2.3 — Определение местоположения гиперболическим методом.

Мультилатерация представляет широкое поле для исследований. Практическое применение данной технологии с применением сигналов АЗН-В отражено в ряде научных работ. Мультилатерация рассматривается как способ резервирования АЗН-В [26] и как средство повышения точности определения координат судна, чего удается добиться в Северном море [38] и Мексиканском заливе [8], производится анализ возможности построения альтернативной навигационной системы в воздушном пространстве США [41]. Авторы обсуждают потенциальное использование уже развернутых датчиков для мультилатерации, отмечая при этом проблемы точности в гористой местности.

Оценка возможностей использования мультилатерационных систем в современных системах АНС также дана на самом высоком уровне - она приводится в официальном документе ИКАО [17]. В нем говорится, что "эффективность наблюдения с использованием систем ADS-B и MLAT выше или, по крайней мере, не ниже, чем с использованием эталонного вторичного обзорного радиолокатора (ВОРЛ) и соответственно они не менее безопасны, чем радиолокатор". Принимая в расчет выводы данного документа о безопасности и сопоставимой точности мультилатерационной системы, можно утверждать, что применение данного вида верификации не противоречит существующим стандартам АЗН-В и не приводит к снижению точности аэронавигационных систем. Однако в данном документе рассматривается возможность применения мультилатерации исключительно как метод определения местоположения судна, но не как часть системы верификации данных АЗН-В. Таким образом, необходимо произвести ряд мер по применению данной технологии к разрабатываемой системе анализа и фильтрации сообщений АЗН-В. Также существует множество математических моделей гиперболического метода определения источника сигнала, что в свою очередь требует дополнительного сравнительного анализа исходя из соображений точности и реализуемости на практике.

Несмотря на все положительные качества мультилатерационной техники определения координат, существует ряд недостатков:

1. Восприимчивость к многолучевому распространению.
2. Необходимость в корректном приеме и дешифровке сообщения несколькими удаленными приемниками.
3. Обязательна высокоточная синхронизация времени на приемных станциях.

4. Необходима постоянная связь с центральным узлом обработки данных.

Необходимость в наличии группы наземных станций, эксплуатационные расходы на поддержание их работы и зачастую невозможность их установки ввиду территориальных ограничений также снижает эффективность их использования, в первую очередь экономическую. В связи с этим на 39-й сессии ассамблеи ИКАО, технической комиссией со стороны ФГУП «ГосНИИ АС» было высказано следующее: «исследования ... подтвердили необходимость обязательного использования данных вторичной радиолокации или мультилатерации для верификации данных АЗН-В на базе ЛПД 1090 ES в системе УВД» и далее «в силу высоких затрат на ВРЛ и МПСН такое АЗН-В с экономической точки становится малоэффективным» [18].

Ещё одним вариантом верификации местоположения является применение дистанционно-ограниченных протоколов (Distance-bounding protocols). Изначально, группа данных методов применялась в RFID системах, однако она может быть использована и в таких системах как АЗН-В. Основная идея заключается в том, что каждый участник ВД, публикующий данные АЗН-В, производит доказательство собственной легитимности через определение расстояния до принимающей стороны - истинность сообщения проверяется путем вычисления времени распространения сигнала. Данный метод предполагает использования принципа "Запрос-Ответ то есть необходимо изменение действующего протокола, либо верификация воздушного судна посредством иных каналов связи, например ACARS или CPDLC.

В случае использования протокола Брандсона-Чаума в самом запросе содержится информация, которая впоследствии шифруется ключом проверяющего устройства (наземной станцией). В случае, если сообщение дешифровано успешно и условие местоположения источника информации выполняется (период отправки и получения вписывается во временные рамки), участники ВД удостоверяются в подлинности данных и, в дополнение, могут определить местоположение друг друга используя метод трилатерации. Трилатерация, в отличие от мультилатерации использует рассчитанные расстояния до источника излучения, а не временную разницу прихода сигнала. Помимо классического применения данного метода противодействия, существуют его различные вариации, например, с использованием мультилатерационных техник, информации

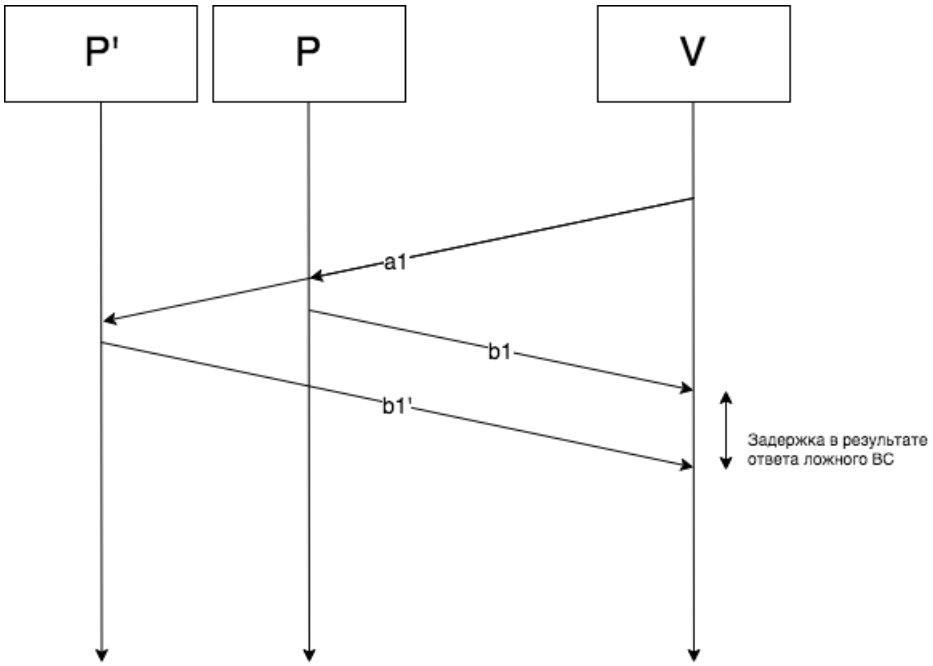



Рисунок 2.4 — Проверка истинности источника классическим дистанционно-ограниченым протоколом.

об уровне сигнала и прочих физических характеристик распространения сигнала.

Фильтры Калмана [23] уже широко используются в УВД, например, для фильтрации и сглаживания данных местоположения полученных от GPS. Калмановская фильтрация используется для наблюдения за серией зашумленных измерений, благодаря чему производится попытка статистически оптимально прогнозировать будущие состояния измеряемых переменных динамической системы. Процесс калмановской фильтрации состоит из двух различных этапов - этапа прогнозирования и этапа обновления. Поскольку процедура итеративна, ее можно легко использовать и обновлять в реальном времени, сохраняя в памяти лишь последнее состояние.

Используя вероятностную модель движения воздушного судна, становится возможным снизить воздействие шума и получить более точные оценки положения объекта в настоящий, будущий или прошедший момент времени. Фильтрация Калмана играет решающую роль в решении мультилатерационной задачи, устраняя шумные сигналы и сглаживая недостающие данные.

Также калмановская фильтрация является полезным инструментом для прогнозирования будущих значений функции на основе собранных исторических данных - она используется в наземных системах для фильтрации и про-

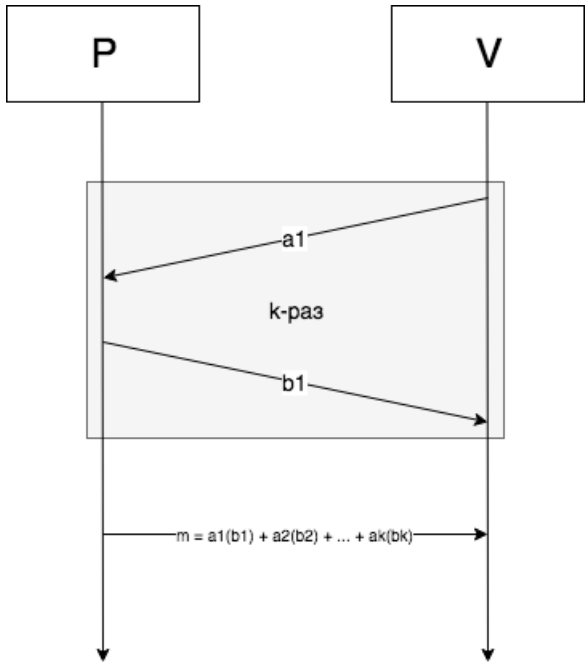



Рисунок 2.5 — Проверка истинности источника протоколом Брандсона-Чаума.

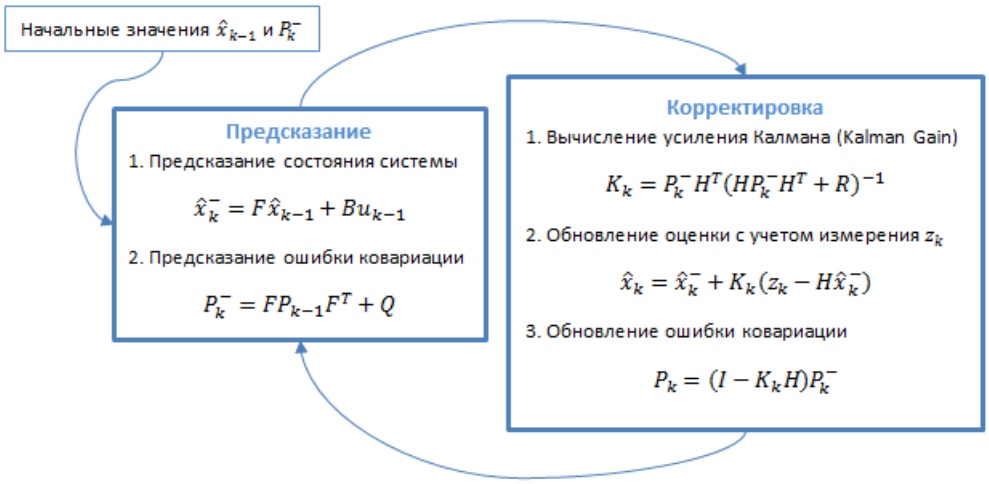



Рисунок 2.6 — Концепция работы фильтра Калмана.

верки векторов состояний и изменений траектории, сообщаемых самолетами по АЗН-В, а также проведения проверок достоверности этих данных.

Использование узконаправленных антенн позволяет определить угол места реального ВС. Таким образом данный тип системы частично позволяет отфильтровать мнимые ВС. Однако применение данного метода может быть крайне недостаточным, поскольку мнимое ВС может иметь тот же угол места, что и реальный самолет, но другие высоту и расстояние до наземной станции.

Использование плановой информации в качестве основы для подтверждения подлинности предоставляемых данных в ряде случаев можно считать недостаточным. Если для трассового ведения наблюдения данный метод допустимо

считать приемлемым, то при заходе на посадку или при экстренных ситуациях фактическая траектория полета не будет совпадать с предполагаемой траекторией по плану полета. Однако данный метод целесообразно включать в качестве дополняющего основную систему противодействия атакам.

Групповая проверка - еще одна концепция, предлагаемая для решения вопросов безопасности и конфиденциальности при использовании АЗН-В [32]. Она нацелена на обеспечение безопасности связи АЗН-В (IN) путем использования мультилатерации, выполненной группой воздушных судов для проверки местоположения участников ВД, не входящих в данную группу. В условиях большой плотности трафика данный метод имеет право на существование, поскольку в таком случае возможно нахождение более 4-х воздушных судов в зоне для инициации групповой проверки АЗН. В виду динамичности и непостоянства структуры данный метод имеет ряд недостатков. Прежде всего, такой подход требует большое количество дополнительных сообщений для успешного выполнения мультилатерации и радиообмена о валидности или невалидности воздушных судов. Поскольку работа протокола АЗН-В представляет собой однонаправленную трансляцию, для поддержки концепции группы необходим новый протокол. Что касается вопроса о том, какой протокол использовать, ряд исследователей упоминает применение протокола L-Band Digital AHA (L-DACS) как одну из возможностей. L-DACS разрабатывается в EUROCONTROL в качестве будущей IP технологии для связи «воздух-воздух», но, к сожалению, в среднесрочной перспективе о внедрении такой технологии нет никаких сведений. Если такой протокол можно успешно реализовать, остается центральная проблема того, как осуществлять безопасную аутентификацию членов группы, осуществляющей проверку. Также необходимо учитывать проблемы, связанные с высокой степенью синхронизации часов каждого из участников группы, возможности работы с переотраженными или зашумленными сигналами АЗН-В. С другой стороны применение такого метода позволит избежать уязвимостей традиционного метода мультилатерации и даже без введения дополнительной аутентификации успешно противодействовать теоретическим угрозам АЗН.

Моделирование трафика позволяет выявить отклонения от нормального поведения АЗН-В. Используя исторические данные, а также методы машинного обучения, становится возможным создать тепловую карту, построенную исходя из уровней принимаемого сигнала АЗН. Используя данные этих моде-

лей, можно делать косвенные выводы об аномалиях в воздушном пространстве, ограниченном зоной приема наземной станции. Кроме того, существует множество сравнительно простых правил, которые могут использоваться как индикаторы угроз системой обнаружения вторжений, не прибегая при этом к более сложным мерам. Ни одно из этих правил не является необходимым или достаточным для обнаружения постоянной атаки. Но в зависимости от сценария и изощренности атаки они могут указывать на необычные сообщения АЗН, которые должно быть дополнительно исследованы оператором или обработано с помощью технических средств. Такой подход к выявлению информационных аномалий позволит частично покрыть проблему спуфинга АЗН-В, вместе с тем делая предполагаемые атаки более дорогими для реализации.

Принципиально новым подходом по обеспечению безопасности системы АЗН-В является применение алгоритмов машинного обучения. Эффективность методов машинного обучения подтверждается их применением в таких отраслях как экономика, финансы, промышленность. В частности, данная передовая технология применяется в системе сбора и обработки данных о безопасности полетов [45]. Учитывая тот факт, что вся информация передаваемая как легитимными пользователями АЗН-В (воздушными судами), так и нелегитимными (несанкционированное вмешательство) является цифровой и удобна для хранения и последующей обработки, имеет место быть практическая возможность её накопления и последующего анализа. Благодаря данным за месяц становится возможным определить показатель уровня принимаемого сигнала для каждой точки обозреваемого пространства. Данные параметры зависят от диаграммы направленности, коэффициента усиления антенны, расположения посторонних объектов в поле действия приемника АЗН-В и прочих факторов. Информация об уровне принимаемого сигнала недоступна для посторонних лиц, осуществляющих атаку внедрения ложных сообщений АЗН-В, и, следовательно, может быть использована при классификации данных, поступающих в АС УВД.

Методы машинного обучения, а именно классификационные алгоритмы, позволяют отделить ложные сообщения, сгенерированных в результате несанкционированного вмешательства, от истинных сообщений. Для применения данного класса методов необходим массив накопленной информации, полученной по протоколу АЗН-В. Далее необходимо произвести имитацию несанкционированного вмешательства всеми возможными способами реализации атаки с

последующей маркировкой таких сообщений как ложные. Затем основываясь на промаркированных данных произвести анализ эффективности методов машинного обучения и произвести обработку данных АЗН-В без маркировки ложных сообщений. Данный процесс несет итерационный характер - сбор данных АЗН-В, искусственное несанкционированное вмешательство, машинное обучение, анализ эффективности при повторном несанкционированном вмешательстве без маркировки, применение алгоритма в реальном режиме времени для противодействия несанкционированному вмешательству.

В задаче верификации данных, результаты нескольких методов могут быть использованы в совокупности, что определяет еще один способ защиты системы АЗН-В от атак. Концепция может использоваться на разных этапах обработки данных, так в исследованиях [4], описывается слияние данных первичной радиолокации и АЗН-В и приводится доказательство того, что этот подход может улучшить качество наблюдения на практике. Метод заключается в сравнении данных АЗН-В с другими независимыми источниками, а именно, данными ПРЛ, мультилатерационных систем, данными планов полетов, и описанием гибридного алгоритма оценки. Такой подход не только позволяет выявить аномалии одной из систем, в виде, например, атаки подмены, но и определить корректность работы систем, рассматриваемых в рамках алгоритма оценки, выявить неисправности. Впоследствии могут быть выполнены автоматические технические или нетехнические процедуры, идентифицируя проблему и реагируя на них соответствующим образом. Этот процесс включает анализ достоверности данных, если система уязвима для несанкционированного доступа либо является недостаточно точной. Достоверность рассчитывается путем изучения корреляций и дополнительных характеристик, полученных посредством процессов машинного обучения, которые направлены на выявление аномалий в полученной информации, что является необходимым при создании системы анализа аэронавигационных данных.

Все вышеперечисленные меры по уменьшению влияния атак на работоспособность АЗН-В покрывают все уровни сети - от физического до уровня приложений, если рассматривать взаимодействие участников ВД с точки зрения модели OSI. Некоторые из них применимы исключительно для анализа трафика от воздушных судов к наземной станции, другие - могут быть применены для

анализа трафика непосредственно между судами, без участия наземных служб связи. К таким мерам в частности могут быть отнесены следующие:

- анализ сообщений о судах, которые внезапно появились в пределах зоны покрытия приемника;
- отсеивание сообщений, параметры сигнала которых, превышают установленные пороги и не соотносятся с реальным местоположением судна;
- оповещение о слишком большом количестве летательных аппаратов в заданной области, исходя из сообщений, полученных по каналу АЗН (превышение порога плотности);
- фильтрация сообщений о ВС, движущихся за пределами возможной скорости и высоты;
- оповещение о ВС, движущихся вне воздушных трасс, либо в запретных для полета зонах;
- оповещение о несоответствии местоположения ВС из сообщения плану полета;
- отсеивание сообщений с некорректными или отсутствующими полями;

В результате анализа технологий, которые могут быть использованы для противодействия несанкционированному вмешательству, можно сделать вывод о том, что технологии, применение которых не требует изменений в использовании системы АЗН-В являются ключевыми в задаче решения поставленной проблемы. Такими технологиями является мультилатерация и семейство методов машинного обучения, которые, в рамках решения задачи обеспечения достоверности сообщений АЗН-В были названы методом монолатерации.

## 2.2 Методы вычисления временных характеристик и синхронизации сигналов системы автоматического зависимого наблюдения

Мультилатерационный метод с практической точки зрения может быть осуществлен при выполнении двух условий: с высокой точностью может быть получено время прихода сигнала, все приемные станции синхронизированы по времени с точностью до наносекунд. В случае, если эти условия не выполня-

ются, точность определения местоположения может стать меньше регламентированной точности АЗН-В и система в конечном итоге, не сможет верифицировать данные вторичной радиолокации. Рассмотрим методы вычисления времени прихода сигналов и вопросы, связанные с синхронизацией приемных устройств.

Существует два метода вычисления РВП сигналов: вычисляется либо взаимная корреляция пары сигналов, либо фиксируется время прихода сигналов и на этом основании вычисляется разность их прихода. Последний метод применяется для тех сигналов, где благодаря форме сигнала легко может быть определен передний фронт. Такими качествами обладают сигналы ВРЛ и систем АЗН, основанных на расширенном сквиттере.

Рисунок 2.7 — Структурная схема кросскорреляционного метода

Рассмотрим кросскорреляционный метод. В основном системы, работающие с использованием данного подхода, используются в военных средствах радиоэлектронной борьбы (РЭБ). Упрощенная схема потоков данных представлена на рисунке 2.7. Преобразователь с понижением частоты принимает сигнал на частоте 1090 МГц и понижает ее до рабочей частоты. Блок АЦП преобразует аналоговую форму сигнала в цифровую. Блок кросскорреляции проводит серии кросскорреляционных операций с парами сигналов, принятых с различных передатчиков. Точность операции зависит от типа обрабатываемого сигнала, наличия в канале связи эффекта многолучевости и других факторов. Алгоритм обработки должен быть построен таким образом, чтобы обеспечить отсутствие в системе некорректных результатов измерений, вызванными использованием сигналов с низкими авто - и кросскорреляционными характеристиками. Получив от блока кросскорреляции РВП сигналов, алгоритм вычисления РВП используется для определения координат $x$,$y$,$z$. В конечном итоге передают-

ся данные о местоположении для отображения целей на оборудовании вывода данных. Кросскорреляционные системы принципиально отличаются от систем, основанных на оценке времени прихода сигнала, в том, что в кросскорреляционных системах никогда не вычисляется абсолютное время прихода сигнала - только относительное. Перейдем к рассмотрению метода, основанного на оценке времени прибытия.

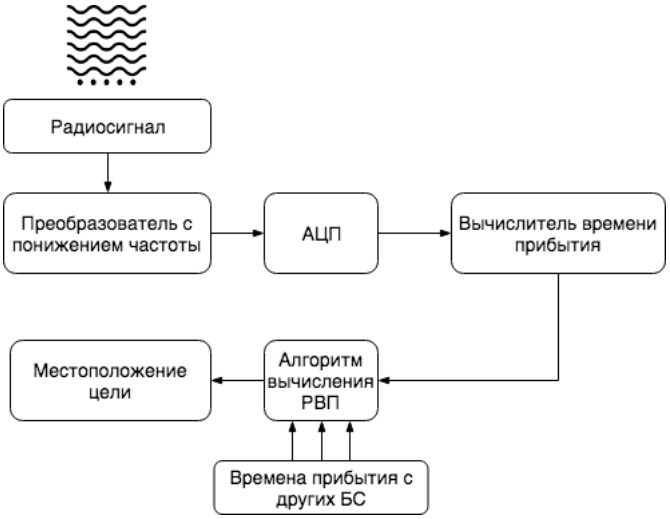



Рисунок 2.8 — Структурная схема метода оценки времени прихода

Системы на оценке времени прибытия широко используются при мультилатерации на ВРЛ. Схема 2.8 описывает потоки данных внутри этой системы. Работа системы проходит в следующей последовательности. Понижающий преобразователь частоты и АЦП преобразуют аналоговый сигнал и декодируют его. После декодирования, блок вычислителя времени прибытия определяет точное время прибытия для полученных сигналов. Дополнительно на данном этапе происходит идентификация сигналов для целей их последующей корреляции (для вычисления РВП сигналов, имеющих один и тот же идентификатор, которым может являться адрес судна). Далее вычисляется РВП сигналов для каждой пары приемников, для сигналов имеющих один и тот же идентификатор. Блок вычисления местоположения и устройство слежения действуют по тому же принципу, что и для кросскорреляционных систем.

Синхронизация является существенным принципом, заложенным для обеих описанных систем мультилатерации, несмотря на то, что способы их применения в основном отличаются. Для определения местоположения необходимо знать разности времен между приходом сигнала на одну антенну и приходом такого же сигнала на другую антенну в системе. Однако сигнал является дис-

кретизированным по времени в процессе АЦП, что вносит временные задержки, помимо задержки при преобразовании частоты. Для того, чтобы определить РВП сигнала, необходимо знать временные характеристики этих групповых задержек. Для сравнения оцифрованных сигналов также необходима одна и та же частота дискретизации. Кроме того, процессы оцифровки для каждого приемника цепи должны относиться к общей базе времени, в противном случае сигналы на различных участках будут ссылаться на различные часы и будут прямо не сопоставимы. Схема ниже описывает групповую задержку и компоненты синхронизации. Под синхронизацией здесь понимается способ, посредством которого процессы оцифровки сигналов на каждом отдельном элементе системы связаны вместе.

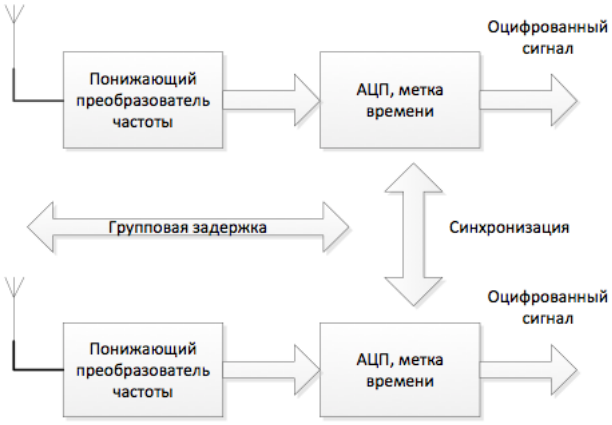



Рисунок 2.9 — Групповая задержка и компоненты системы синхронизации

Схема 2.10 описывает топологию различных методов синхронизации, используемых в системах WAM (как для TOA, так и для TDOA).

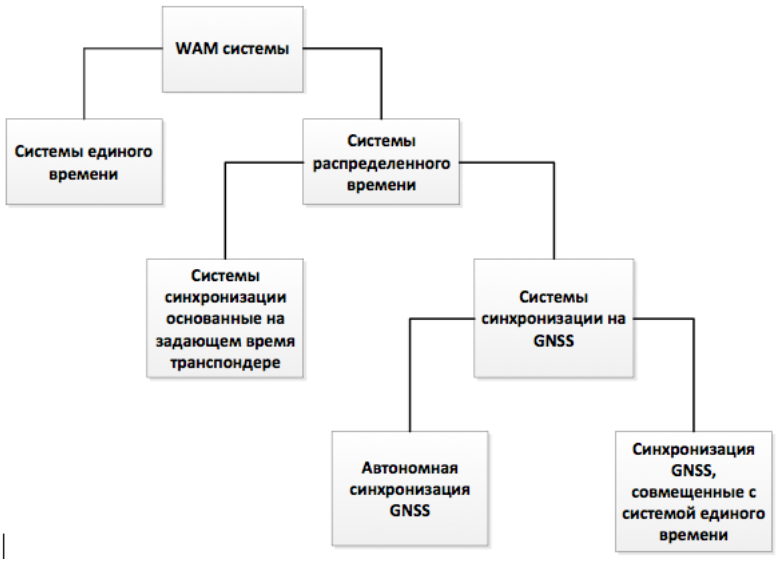



Рисунок 2.10 — Иерархия систем синхронизации

Рассмотрим системы единого времени, как один из вариантов синхронизации приемных устройств. Системы единого времени используют стандартные приемники радиосигнала, а процесс оцифровки и добавления метки времени осуществляется в центре обработки данных. Системы данного типа принимают радиосигналы от самолета и понижают частоту до промежуточной. Промежуточная частота передается от каждого приемника на блок обработки по нецифровому каналу связи. На этом этапе промежуточная частота понижается до рабочей, происходит оцифровка и декодирование, присвоение времени декодированному сигналу. Используя данную архитектуру, нет необходимости осуществлять синхронизацию каждого приемника. В связи с этим возникает необходимость в точной калибровке всех линий связи до центра обработки для вычисления групповой задержки. Как только будут использоваться приемники с большей базой, задержки в линии связи будут также увеличиваться, тем самым понижая общую точность системы. Так, например, если задержки известны в пределах 1% и существует требование к точности равное 1 нс, задержки в 100нс допустимы, но в 200нс уже нет[39]. Преимущество этой архитектуры состоит в том, что она использует простые приемники с низким электропотреблением и наибольшие затраты на себя берет центральный процессор мультилатерации. Однако, задержка сигнала в канале связи между приемником и центральным блоком обработки накладывает жесткие требования на тип связи и длину линии связи. Для таких систем обычно используются СВЧ линии передачи или оптоволоконный канал, как это показано ниже. Местоположение центра обработки сигналов должно быть в центре рабочей зоны для минимизации длины аналоговой линии связи. Эта архитектура используется в системах WAM компании ERA a. s.

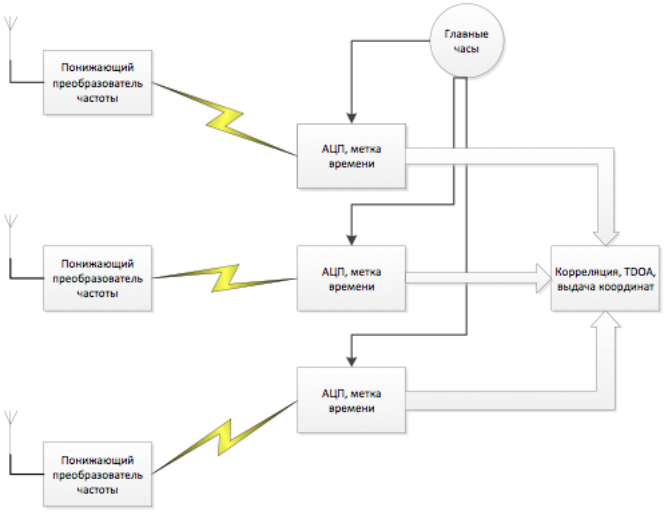



Рисунок 2.11 — Иерархия систем синхронизации

Другим вариантом синхронизации является использование систем распределенного времени. Системы распределенного времени используют более сложные приемники для уменьшения требований к линии передач. Радиосигнал понижается до основной частоты, декодируется, происходит измерение времени прихода, при этом все операции производятся на приемном устройстве. Таким образом, на центральный блок обработки данных приходит декодированный сигнал, содержащий 24-х битовый адрес и время прибытия сигнала в приемник. В случае данной архитектуры нет каких либо специальных требований для канала связи, потому что задержки в канале для данного случая не являются критичными. Однако, должен существовать механизм по синхронизации часов на каждом в отдельности приемнике. Этот алгоритм применяется компанией Sensis Corporation.

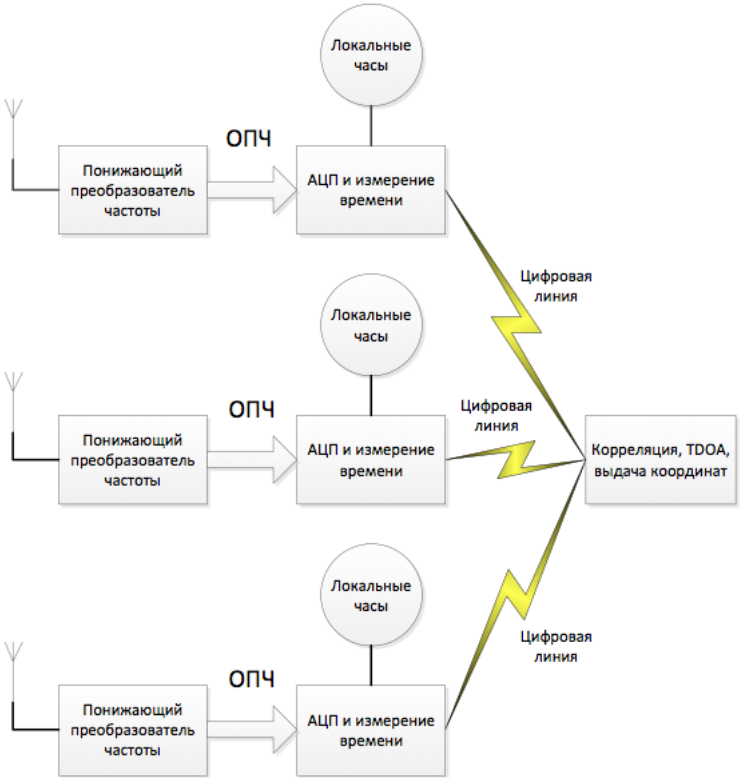



Рисунок 2.12 — Структурная схема системы синхронизации распределенного времени

Также для целей синхронизации может быть применен подход, основной принцип которого основан на использовании отдельного передатчика, который служит источником опорного синхронизирующего сигнала. Это означает, что задержка, вызванная смещением аналоговых компонентов, сводится на нет. Как и для всех предыдущих случаев, на точность системы влияет задержка, вызванная атмосферными искажениями. Данный подход использует компания Sensis Corporation

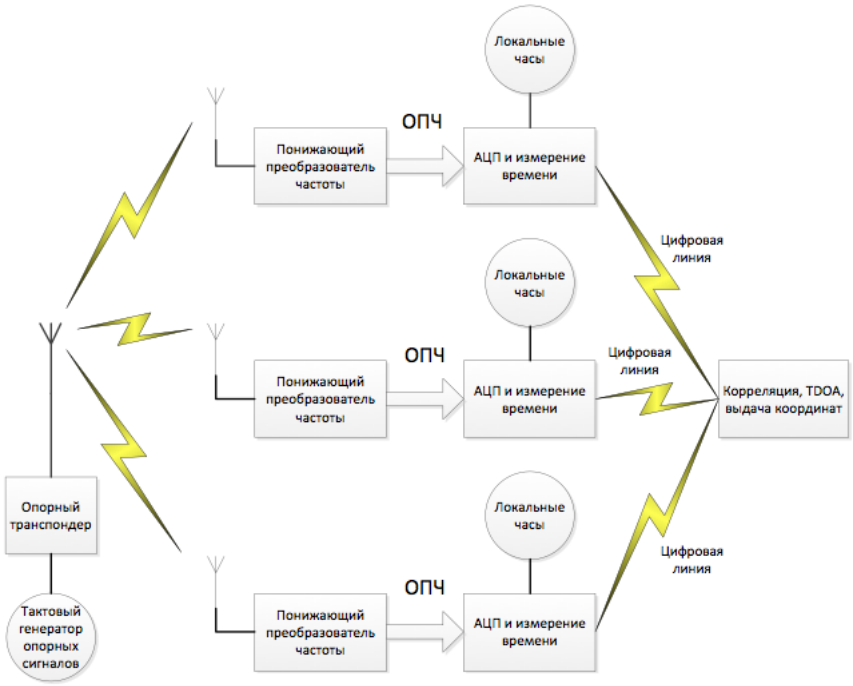



Рисунок 2.13 — Структурная схема системы синхронизации на задающем транспондере

Для целей синхронизации и обеспечения всех приемников единым отсчетом времени может быть использована Глобальная Спутниковая Навигационная Система (ГНСС), в частности – GPS или ГЛОНАСС. Согласование по времени в ГНСС системах осуществляется с высокой степенью точности, т.к. она влияет на точность определения положения пользователей данной системы. Для примера система GPS обеспечивает точное время в пределах 100 нс. Это время может быть использовано как опорное для приемников. Но для мультилатерационных систем важна лишь разность прихода сигналов, поэтому для выполнения этой задачи нет необходимости знать точное абсолютное время. Таким образом, возможно осуществить мультилатерацию с точностью в пределах 10-20 нс [39], используя при этом на каждом принимающем устройстве синхронизатор ГНСС. Внедрение систем синхронизации ГНСС гораздо менее затратно, чем внедрение систем единого времени или распределенных систем синхронизации на транспондерах, поскольку нет необходимости в точной установке задающего опорные сигналы оборудования и применении помехозащищенного канала связи. Подобные системы используются компанией Rannoch Corporation.

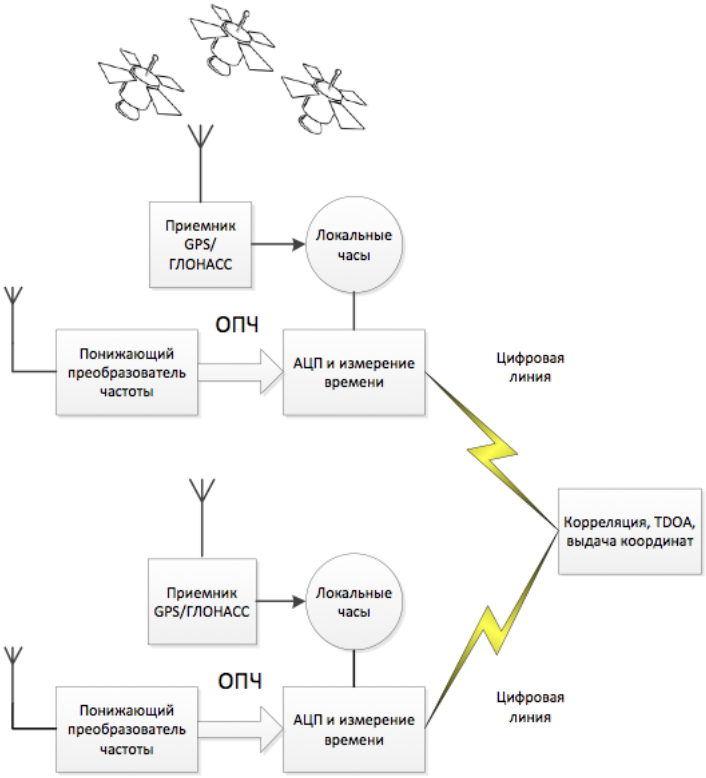



Рисунок 2.14 — Структурная схема автономной системы синхронизации ГНСС

В ситуациях, когда Автономная синхронизация GNSS обладает недостаточной точностью, применяется синхронизация GNSS Единого времени. Системы единого времени используют навигационные спутники, находящиеся в прямой видимости для всех приемников АЗН и рассчитывает разность прихода сигнала времени, полученного от спутников GPS/ГЛОНАСС. Это позволяет добиться высокой точности до десятых долей наносекунд. Подобные системы предложены компанией Roke Manor Research.

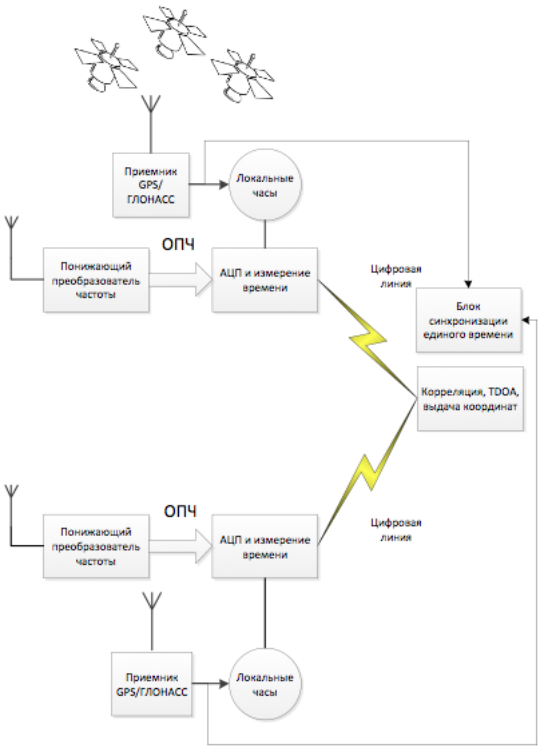



Рисунок 2.15 — Структурная схема системы синхронизации ГНСС единого времени

Приведем сводную таблицу различных систем синхронизации:

Таблица 2.1

Сравнительные характеристики систем синхронизации

| Система | Точность, нс | База | Канал | СПВ |
|---|---|---|---|---|
| Единого Времени | 2..20 | Средняя | СВЧ | + |
| | | | fiber | - |
| Задающий транспондер | 2..20 | Средняя | Любой | + |
| ГНСС | >20 | Любая | Любой | - |
| ГНСС ЕВ | <2 | Широкая | Любой | - |

Для осуществления целей синхронизации нежелательна установка большого количества дополнительного оборудования, так же как и нежелательно использование дополнительных каналов связи, поскольку это влечет за собой повышенные расходы на модернизацию и использование новой полосы частот. ГНСС Единого времени обладает наиболее выдающимися характеристиками и,

более того, применение данной технологии сможет повысить качество предоставляемой АС УВД навигационной информации. Отсутствие дополнительных каналов связи, кроме как общедоступных GPS/ГЛОНАСС, а также отсутствие необходимости в использовании дополнительных опорных мачт для приема сигнала, делает данную технологию наиболее приемлемой для решения поставленных задач.

## 2.3 Методы и алгоритмы машинного обучения в задаче определения события несанкционированного вмешательства

Благодаря современному цифровому подходу, заложенному в основу механизма работы системы АЗН-В, имеется возможность накапливать и обрабатывать данные АЗН-В для последующего изучения. В рамках задачи обнаружения несанкционированного вмешательства в канал связи АЗН-В, становится возможным использовать методы машинного обучения. Их можно разделить на три категории: классификация, кластеризация и регрессия. В случае с классификацией, стоит задача на основе накопленных данных определить к какому заранее известному классу относится каждая новая единица информации. В случае с кластеризацией, классы заранее не определены, а в случае с регрессией решается задача восстановления зависимости одной переменной от другой. Из-за того, что информация может быть либо истинной, либо ложной, для обнаружения несанкционированного вмешательства необходимо использовать классификационные алгоритмы машинного обучения. Использование методов машинного обучения классификационного типа позволяет осуществлять валидацию сообщений АЗН-В при помощи одной наземной станции приема. Исходя из возможности режима работы с использованием только одной станции, такой метод валидации в данной работе будет именоваться монолатерацией.

Наиболее популярными на данный момент являются следующие классификационные алгоритмы:

- Light Gradient Boosting (LGB);
- AdaBoost на основе решающих деревьев;
- Naive Bayes;

– метод опорных векторов;
– метод k-ближайших соседей;
– метод решающих деревьев;

Для определения эффективности алгоритмов необходимо произвести моделирование на реальных данных, предварительно промаркированных конечными классами (ложное/истинное сообщение).

Для всех перечисленных методов необходимо произвести обучение алгоритма. Под обучением понимают минимизацию эмпирического риска, т.е. средней величины ошибки на обучающей выборке. Для определения точности алгоритма применяют различные функции потерь, у каждой из которых, независимо от модели, аргументами являются - выходное значение модели $\gamma$ и ожидаемое истинное значение из промаркированной выборки $l$: $C(\gamma, l)$.

Обучение производится с кросс-валидацией, т.е. с разбиением обучающей выборки на несколько частей и обучением каждой из них.

В данной работе предлагается использовать следующий подход к определению эффективного алгоритма машинного обучения для выявления несанкционированного вмешательства:

1. получение обучающей выборки;
2. разбиение обучающей выборки на несколько частей;
3. отбор полезных признаков с использованием алгоритмов решающих деревьев;
4. настройка параметров модели обучения (глубина деревьев, количество итераций);
5. оценка модели на тестовой выборке с использованием различных метрик - Accuracy, precision, recall и AUC-ROC [11];

Рисунок 2.16 — Схема процесса определения оптимального алгоритма машинного обучения

Для получения обучающей выборки необходимо очистить данные от дубликатов, очевидно ненужных признаков и привести данные в единый формат для дальнейшей обработки.

Приведем основные алгоритмы машинного обучения, которые будут использованы для выявления факта несанкционированного вмешательства и определения истинности сообщения АЗН-В.

Выбор алгоритма машинного обучения необходим для создания эффективного классификатора. Для классификации, при обучении по выборке, применяются признаки объектов. Будем полагать, что на вход классификатора в качестве обучающей выборки размера m подается вектор объектов в виде $X^m = (x_1, ..., x_m)$, где $x_i$ — вектор, представляющий признаки объекта с номером $i$ и имеющий длину $n$. В рассматриваемой задаче определения истинности сообщения АЗН-В в соответствии с постановкой задачи вектор $x_i$ может быть представлен так:

$$x_i = \begin{pmatrix} attr_1 \\ attr_2 \\ ... \\ attr_n \end{pmatrix}$$

где $attr_i$ - признаки сообщения АЗН-В, такие как:

- пеленг приема сообщения;
- уровень сигнала;
- расстояние до ВС;
- координаты ВС;
- высота ВС;
- категория сообщения АЗН-В;
- направление полета ВС;

Также в распоряжении классификатора на этапе обучения имеется вектор, задающий принадлежность каждого объекта какому-либо классу: $Y^m = (y_1, ..., y_m)$, где каждая метка $y_i$ принадлежит множеству классов Y. В нашем случае имеет место бинарная классификация, то есть $y_i$ состоит из двух элементов — 0, 1, где 0 означает ложное сообщение, а 1 — истинное.

Решающее дерево (англ. — decision tree) — модель классификации, последовательно разбивающая объекты на подмножества исходя из значения признаков объектов. Эта модель представляет собой дерево, вершине которого соответствует все множество объектов из области определения. В каждой вершине задано некоторое правило относительно одного из признаков объекта и разбивающее множество объектов, соответствующих этой вершине, на несколько подмножеств (чаще всего на два подмножества), которые в свою очередь соответствуют дочерним вершинам данной вершине. В листьях дерева также содержится метка, которая соответствует всем объектам, относящимся к данному листу. Метод классификации случайный лес (англ. — Random forest) основывается на создании большого количества решающих деревьев и итоговой классификации объекта, основывающейся на предсказании всех созданных решающих деревьев. Таким образом, случайный лес усредняет предсказания деревьев решений. В качестве итогового предсказания обычно берется медиана всех предсказаний построенных решающих деревьев. Решающие деревья большой глубины обычно переобучаются на тренировочных данных, то есть имеют маленькое смещение (англ. — bias) своих предсказаний относительно правильных предсказаний, но также имеют очень большую вариабельность (англ. — variance) своих предсказаний. Цель случайного леса — снижение вариабельности предсказания отдельных решающих деревьев. Одним из ключевых методов, использующихся в методе случайного леса, является метод тренировки решающих деревьев на случайной подвыборке данных (англ. — bootstrap aggregating). Из исходного тренировочного набора выбирается K подвыборок данных (с повторениями), и на каждой из этих подвыборок тренируется решающее дерево. Этот подход позволяет в целом снизить вариабельность предсказаний без ущерба смещению, что объясняется слабым значениям корреляции каждой пары решающих деревьев в наборе. Вторым ключевым моментом является то, что при построении очередного решающего дерева и принятии решения о выборе признака для разделения множества объектов, принадлежащих очередной вершине, на два подмножества, используется случайное подмножество признаков. Этот подход позволяет еще более снизить корреляцию между парами деревьев в лесе, так как он снижает количество вхождений очень важных признаков, влияющих на итоговое предсказание, в вершины решающих деревьев. Одним из способов получения некоторой информации о важности признаков является

перебор признаков и сравнения, как настроенная модель работает с учетом и без учета перебираемого признака. Другим способом является подсчет количества неопределенности (неупорядоченности) поддерева, которое убирает разбиение по данному признаку. Мерой неопределенности может служить коэффициент Джини или энтропия. Оба подхода имеют право на существование, но тем не менее по-прежнему дают малое представление о процессе принятия решения для конкретного объекта. При рассмотрении решающего дерева, интуитивно понятно, что для каждого решения, принимаемого деревом (или лесом в совокупности), существует путь (или несколько путей) от корня к листу, состоящий из серии решений, определяемых значением некоторых признаков, и вносящих вклад в финальное предсказание. Решающее дерево с $M$ листьями разбивает пространство признаков на $M$ регионов $R_m$, $1 \leq m \leq M$. В классическом определении решающего дерева[19-Маг], предсказывающая функция дерева определяется так:

$$f(x) = \sum_{m=1}^{M} c_m I(x,R_m) \tag{2.1}$$

где $M$ — число листьев дерева, $R_m$ — регион пространства признаков, соответствующий листу $m$, $c_m$ — константа, соответствующая региону, а $I$ — индикаторная функция, возвращающая 1, если $x \in R_m$ и 0 иначе.

В данной работе алгоритм решающих деревьев применяется как слабый алгоритм для метаалгоритмов Adaboost и LightGBM, которые в свою очередь является представителем семейства алгоритмов бустинга.

На данный момент в машинном обучении одиночные модели используются крайне редко. Более того, повсеместное распространение получили ансамблевые алгоритмы (композиции алгоритмов), которые способны объединять множество базовых методов так, что итоговый алгоритм будет гораздо точнее, чем его отдельные составляющие. Популярность ансамблей заключается во множестве факторов, так, например, ансамбли способны аппроксимировать более сложные функции, чем базовые алгоритмы в отдельности. Кроме того, композиции алгоритмов имеют более высокую обобщающую способность, так как финальное предсказание вычисляется на основе ответов множества алгоритмов, что позволяет уменьшить влияние переобучения, с которым могут столкнутся отдельные модели. Эффективность такого подхода была подтверждена в работе Роберта

Шапира в 1990 году [35]. Существует два основных ансамблевых алгоритма - бэггинг и бустинг.

Бэггинг является метаалгоритмом композиционного обучения машин и предназначен для улучшения стабильности и точности алгоритмов машинного обучения, используемых в статистической классификации и регрессии. Данный алгоритм был предложен Лео Брейманом в 1994 для улучшения классификации путём комбинирования классификации случайно сгенерированных тренировочных наборов. В основе алгоритма заложены простые принципы - строятся независимые модели и затем они комбинируются используя некоторую модель усреднения (взвешенное среднее, голосование большинства или нормальное среднее).

Обычно используется случайная подвыборка данных для каждой модели, в результате этого все модели немного отличаются друг от друга. Выборка строится по модели выбора с возвращением. Из-за того что данная техника использует множество некореллирующих моделей для построения итоговой модели, это уменьшает СКО. Примером бэггинга служит модель случайного леса (Random Forest, RF)

Бустинг применяется, главным образом, для уменьшения смещения, а также дисперсии в обучении с учителем. Также определяется как семейство алгоритмов машинного обучения, преобразующих слабые обучающие алгоритмы к сильным. Основной принцип заключается в том, что каждая последующая модель обучается на ошибках предыдущей. Принцип металгоритма бустинга представлен на рисунке 2.17.

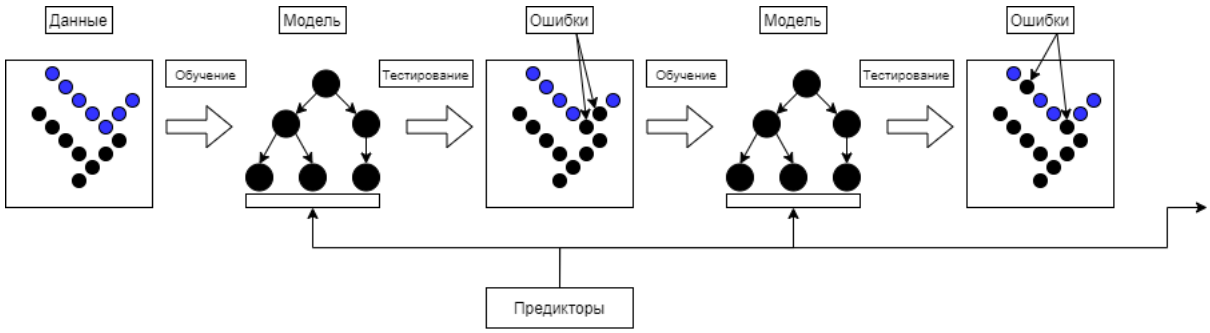



Рисунок 2.17 — Принцип работы алгоритма бустинга

Согласно исследованиям [1] более эффективным металгоритмом является бустинг. В данной работе для классификации сообщений АЗН-В будут применяться алгоритмы AdaBoost и Light Gradient Boosting на основе решающих

деревьев. Данные алгоритмы являются представителями градиентного и адаптивного бустинга соответственно.

Адаптивный бустинг (Adaboost) использует алгоритм для минимизации ошибок предыдущих моделей, при этом основной упор делается на недообученности алгоритма - при каждом новом предсказании алгоритм будет работать над сложными, неочевидными для предсказания подвыборками. Процесс итеративного обучения представлен на рисунке 2.18

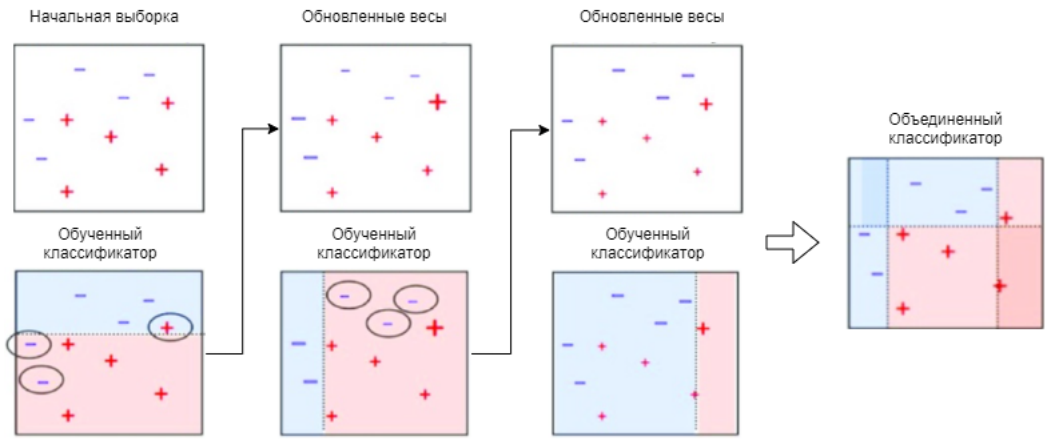



Рисунок 2.18 — Принцип работы алгоритма адаптивного бустинга

Для построения классификатора AdaBoost, за базовый алгоритм обычно используют решающее дерево. На каждой последующей итерации (обучение-тестирование), увеличиваются веса ошибочно классифицированных элементов, которые будут использованы для следующего обучения.

Шаги адаптивного бустинга:

- Всем объектам присвоены одинаковые веса
- Выбирается подвыборка ланных и производится построение модели
- По подвыборке создаются предсказания для всех данных
- Результаты сравниваются с маркированными данными, выявляются ошибки предсказания
- Наибольшие веса присваиваются объектам, на предсказании класса которых алгоритм ошибся
- Процесс обучения повторяется до тех пор, пока ошибки не будут меняться, либо будет достигнуто предельное количество предикторов

Алгоритм AdaBoost был разработан Йоавом Фройндом (Yoav Freund) и Робертом Шапиром (Robert Schapire) в 1996 году [13; 14] . Этот алгоритм ис-

пользуется для создания классификатора. Как известно, классификатор на входе принимает набор данных для обучения и пытается предсказать или классифицировать новые образцы данных, которые относятся к определенному классу (рис. 1.8). Алгоритм AdaBoost (см. алгоритм 1) построен на основе алгоритмов обучения (например, деревья решений) и объединения их. Цель состоит в том, чтобы создать один сильный классификатор на основе нескольких слабых классификаторов.

Градиентный бустинг отличается от адаптивного тем, что, в отличие от AdaBoost, изменяющего веса при каждой итерации, градиентный пытается обучать новые модели по остаточной ошибке прошлых итераций (двигаясь к минимуму функции потерь).

Процесс работы алгоритма градиентного бустинга в общем виде может быть описан так:

- ввод набора пар признаков $x$ и целевых переменных $y\{(x_i, y_i)\}_{i=1,\dots,n'}$, по которой будет восстанавливаться зависимость вида $y = f(x)$ с помощью приближений $\hat{f}(x)$
- ввод количества итераций $M$
- выбор функции потерь $L(y,f)$, которая будет минимизироваться:
  $y \approx \hat{f}(x)$,
  $\hat{f}(x) = \underset{f(x)}{arg\,min}\ L(y,f(x))$
- выбор базового алгоритма обучения $L_\theta(\hat{\theta})$
- поиск приближений с минимизацией функции потерь в среднем:
  $\hat{f}(x) = \underset{f(x)}{arg\,min}\ E_{x,y}[L(y,f(x))]$
- апроксимация искомой функции $f(x)$ параметризуемой функцией $\hat{f}(x)$
- решение задачи оптимизации параметров:
  $\hat{f}(x) = f(x,\hat{\theta}$,
  $\hat{\theta} = \underset{\theta}{arg\,min}\ E_{x,y}[L(y,f(x))]$
- подсчет эмпирической функции потерь:
  $L_\theta(\hat{\theta}) = \sum_{i=1}^{M} L(y_i, f(x_i, \hat{\theta}))$
- подсчет приближения за M итераций:
  $\hat{\theta} = \sum_{i=1}^{M} \hat{\theta}_i$
- инициализация начального приближения параметров $\hat{\theta} = \hat{\theta}_0$

– минимизация эмпирической функции потерь с помощью градиентного спуска.

Минимизация функции потерь может выполнена по следующему алгоритму для каждой итерации $t = 1, ..., M$:

– подсчет градиента функции потерь $\nabla L_\theta(\hat{\theta})$ при текущем приближении $\hat{\theta}$:
$\nabla L_\theta(\hat{\theta}) = \left[\frac{\partial L(y, f(x,\theta))}{\partial \theta}\right]_{\theta=\hat{\theta}}$

– задание текущего итеративного приближения $\hat{\theta}_t$ на основе подсчитанного градиента:
$\hat{\theta}_t \leftarrow -\nabla L_\theta(\hat{\theta})$

– обновление приближения параметров $\hat{\theta}$:
$\hat{\theta} \leftarrow \hat{\theta} + \hat{\theta}_t = \sum_{i=0}^{t} \hat{\theta}_i$

В итоге приближенная функция $\hat{f}(x) = f(x,\hat{\theta})$ может использоваться для классификации. Принцип работы градиентного бустинга представлен для регрессионной задачи на рисунке 2.19.

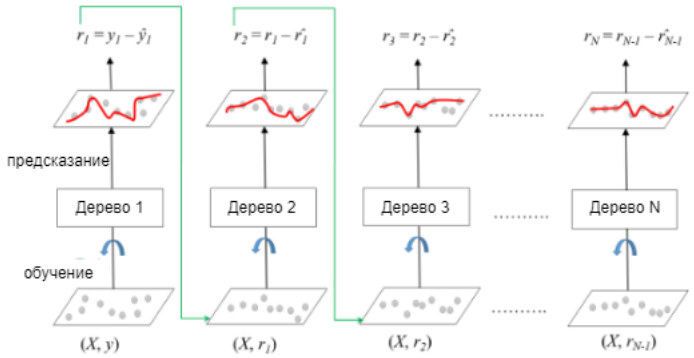



Рисунок 2.19 — Принцип работы алгоритма градиентного бустинга

Для определения эффективности того или иного метода машинного обучения, необходимо провести обучение алгоритма и дальнейшую классификацию на реальных данных АЗН-В.

## 2.4 Разработка математической модели каналов информационного обмена в условиях несанкционированного вмешательства

Математическая модель каналов информационного обмена и угроз необходима для построения эффективной системы анализа и фильтрации сообщений АЗН-В. Выявление и формализация взаимосвязей между системой анализа и фильтрации сообщений АЗН-В, легитимным поведением участников ВД - пользователей АЗН, потенциальными атаку на систему - является основной задачей построения модели. Для создания модели, проанализируем сетевой периметр системы АС УВД, а также составим матрицу возможных угроз в соответствии с методикой ФСТЭК. АЗН-В с точки зрения угроз находится на стыке сразу нескольких более частных моделей: с одной стороны модель можно рассматривать как сетевую, для описания которой необходимо использовать OSI (Open Systems Interconnection), с другой стороны - как физическую динамическую модель, учитывающей распространение сигнала и физические свойства среды. Также при построении необходимо учитывать модель злоумышленника, действия которого могут заключаться в искажении/создании сигналов с физической точки зрения, так и в изменении информационной составляющей сообщения АЗН-В.

Рассмотрим математическую модель угроз безопасности информационных ресурсов, поскольку именно информация является главной ценностью АЗН-В и объектом атаки со стороны злоумышленника. Примем за A множество параметрических моделей атак, где каждый из членов множества - значение параметра атаки, определяющего её тип. За B примем множество параметрических моделей злоумышленника, а за C - множество моделей противодействия атакам, где каждый элемент представляет собой необходимые меры противодействия атаке. Расчет риска будем производить исходя из вероятности осуществления угрозы.

Из таблицы 2.2 становится понятно, что необходимо использовать сочетание нескольких моделей, поскольку к проблеме необходимо подходить комплексно, прорабатывая отражение угроз на разных уровнях воздействия. Основываясь на приведенных моделях, опишем модель злоумышленного воздействия на систему АЗН-В.

Таблица 2.2

Соответствие различных моделей для описания угроз системы АЗН-В уровням сетевой модели OSI

| Сетевая (OSI) | Модель угроз | Физическая динамическая | Информационная |
|---|---|---|---|
| АЗН-В | + | + | + |
| Mode S | - | - | + |
| Воздушная среда | - | + | - |

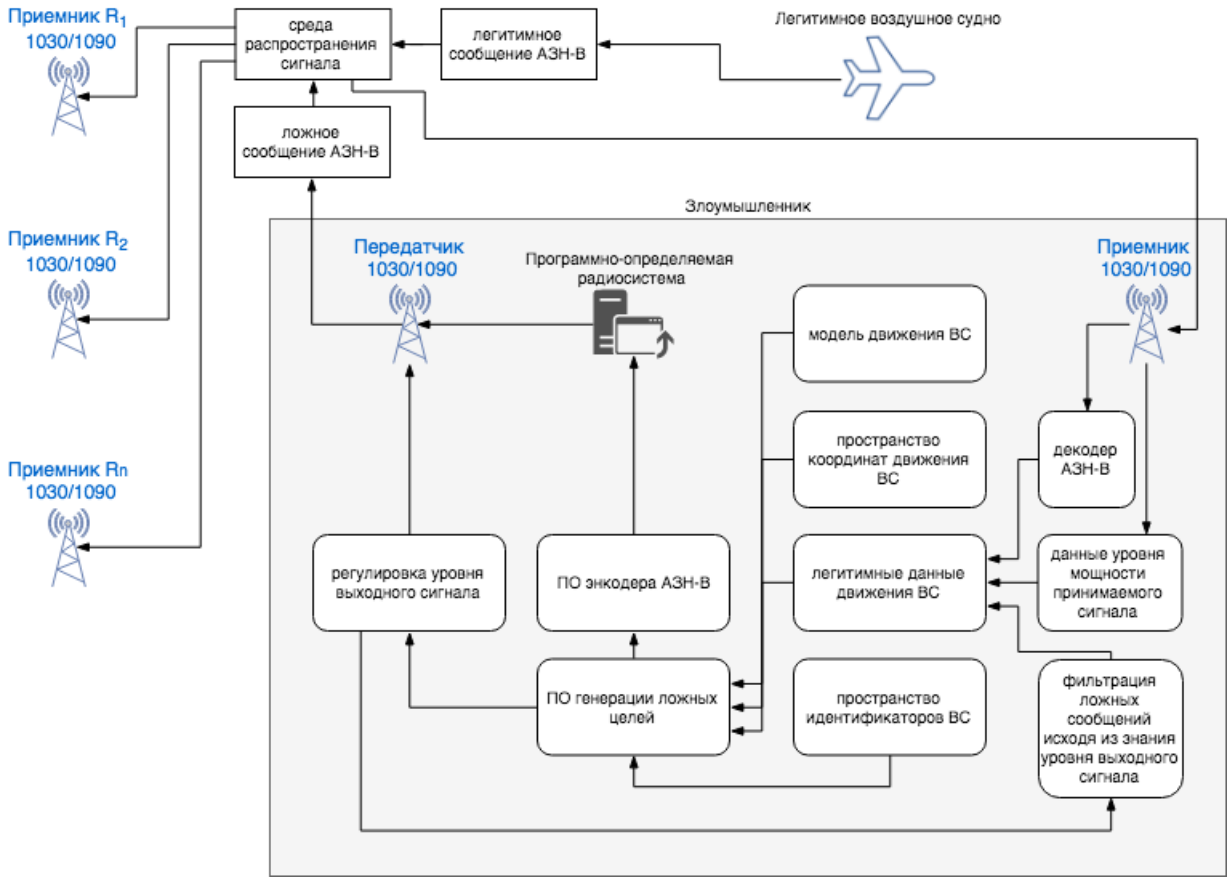



Рисунок 2.20 — Схема спуфинг атаки на систему АЗН-В.

В качестве модели каналов информационного радиообмена, в данной работе будет использован линейный фильтровой канал с переменными параметрами. Данная модель применяется при описании подвижной сотовой радиосвязи [62], а следовательно может быть использована применительно к АЗН-В. При использовании подобного подхода описания процессов, принимается в расчет тот факт, что при многопутевом распространении сигнала происходит его

ослабление. Используя линейный фильтр с переменными параметрами становится возможным описывать распространение сигнала в воздушной среде с учетом потерь применительно к любой точке приема данного сигнала. Линейные фильтры характеризуются меняющейся по времени импульсной характеристикой канала - $c(\tau,t)$, которая в свою очередь имеет вид:

$$c(\tau,t) = \sum_{k=1}^{L} a_k(t)\delta(\tau - \tau_k) \tag{2.2}$$

где $a_k(t)$ определяет возможные меняющиеся во времени коэффициенты затухания для $L$ путей расстояния, а $\tau_k$ - времена задержки соответствующие $L$. Принимаемый сигнал в таком случае будет описан как

$$r(t) = \sum_{k=1}^{L} a_k(t)s(\tau - \tau_k) + n(t) \tag{2.3}$$

Таким образом, полученный сигнал состоит из L компонентов распространения в пространстве, где каждый из них затухает в соответствии с $a_k(t)$, запаздывает на величину $\tau_k$ и зашумляется в соответствии с $n(t)$.

Злоумышленник не может влиять на параметры распространения сигнала и затухание, а лишь на его генерацию $s(\tau - \tau_k)$ и зашумление канала $n(t)$ если имеется целью блокирование работы наземной станции по каналу АЗН.

В случае проведения спуфинг атаки, математическая модель канала информационного радиообмена остается неизменной, при этом добавляется лишь ложный сигнал, отличающийся тем, что инкапсулированное содержимое информирует о несуществующем ВС, а запаздывание прихода сигнала не соответствует запаздыванию легитимного сигнала, отправленного из указанного в сообщении местоположения. В этом случае принимаемый сигнал в таком случае будет описан как

$$r(t) = \sum_{k=1}^{L} a_k(t)s^{'}(\tau - \tau_k^{'}) + n(t) \tag{2.4}$$

либо, в случае зашумления легитимного сигнала как

$$r(t) = \sum_{k=1}^{L} a_k(t)s(\tau - \tau_k) + n^{'}(t) \tag{2.5}$$

где $s^{'}(\tau - \tau_k^{'})$ - описывает сам сигнал, сгенерированный злоумышленником, а $n^{'}(t)$ - помехи, которые злоумышленник создал, препятствуя приему сообщений АЗН-В наземными станциями.

Далее необходимо учесть, что атака как типа спуфинг, так и зашумляющего типа воздействия может быть произведена в случайный момент времени, продолжительность которой так же случайна. То же самое относится и к легитимным сигналам - примем, что в зоне действия наземной станции воздушные суда появляются случайным образом, при этом продолжительность передачи сообщений также случайна. Сигнал, сформированный для передачи сообщения АЗН-В, как легитимного, так и сфальсифицированного, является недетерминированным. Рассмотрим процесс передачи сообщений с учетом данных характеристик и составим математическую модель случайного процесса передачи данных по каналу АЗН. Для построения модели примем показатели случайных величин времени детектирования сообщения, продолжительности сеанса связи, содержания сообщения и соответственно формы сигнала независимыми друг от друга. Исходя из топологии сети, передачу АЗН-В можно рассматривать как клиент-серверную модель, где в качестве сервера выступает передающее устройство АЗН, а в качестве клиента - наземные службы, оборудованные соответствующими приемными устройствами. Данная модель описывает передачу потоковых данных по каналу прямой связи. При этом канал обратной связи, в рамках которого происходит передача информации о состоянии основного канала, либо оповещений о доставке данных, отсутствует - согласно архитектуре АЗН-В. Примем, что передача данных производится без предварительного запроса, а сам процесс передачи данных состоит из передачи сообщений фиксированного размера (112 бит). Примем сообщение за элементарную единицу передачи, а последовательность сообщений от отправителя - блоком данных. Каждый отправленный получателю блок данных можно представить в виде потока данных $\vec{X}(g)$. Его значения есть ничто иное как множество комбинаций наличия сообщений в блоке данных, что, другими словами является множеством комбинаций над полем Галуа второго порядка $GF(g)$, где g - элемент двоичной группы $GF(2)$, поскольку при передаче данных может быть только два состояния - передача сообщения (1), либо отсутствие какой либо передачи. Пример передачи данных представлен на рисунке 2.21.

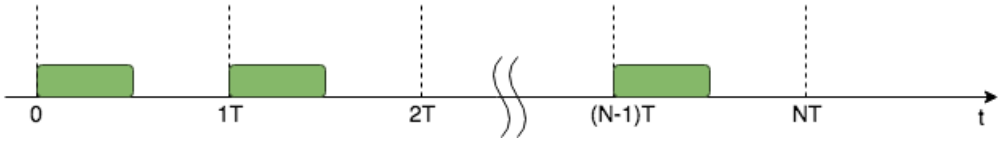



Рисунок 2.21 — Передача блока данных сообщений АЗН-В.

Поток данных $\vec{X}(g)$ представляет собой сочетание вектора данных $\vec{D}(g)$ и вектора избыточности $\vec{R}(g)$ размерности вектора потока $X$. В АЗН-В предусмотрена передача избыточных данных по каналу на другой частоте, для этого необходимо соответствующее оборудование приема-передачи. Рассмотрим составляющие вектора потока данных. Вектор избыточности определяется как $\vec{R}(g) = \{r_1, ...r_D, r_{D-1}, ..., r_{D-R}\} = \{0,...,0,1,...,1\}$. Вектор непосредственно данных может быть определен по следующей формуле: $\vec{D}(g) = \{d_1,d_2,...,d_X\} = \{1,...,1\}$. Принимая тот факт, что переданные по дополнительному каналу связи данные избыточности полностью повторяют данные основного канала, вектор потока данных вычисляется по формуле 2.6:

$$\vec{X}(g) = \vec{D}(g) \oplus \vec{R}(g) = d_1,d_2,...,d_X \oplus r_1, ...r_D, r_{D-1}, ..., r_{D-R} \qquad (2.6)$$

где $D$ и $R$ - число сообщений по основному и резервному каналу $\oplus$ - операция сложения по модулю 2. Пример реализации схемы с избыточностью приведен на рисунке 2.22

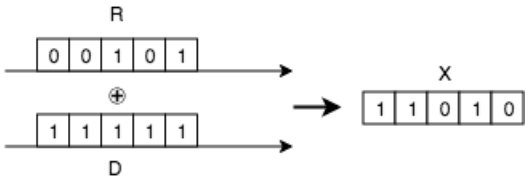



Рисунок 2.22 — Вектор потока данных с избыточностью

Как видно из примера, количество единичных элементов в векторе данных не соответствует количеству сообщений в блоке потока, поскольку часть сообщений является избыточной. На выходе, в векторе потока данных, элемент "1" обозначает присутствие сообщения на основном канале, а элемент "0" обозначает присутствие сообщения избыточности. Исходя из того, что данные в процессе передачи могут теряться по причинам разного характера, необходимо ввести вектор, определяющий потерю сообщений. Обозначим его за $\vec{W}(g)$, как вектор потерь. При его суммировании с вектором потока данных по модулю числа 2 получим вектор оценки $\vec{Z}(g)$. Таким образом, процесс информацион-

ного обмена может быть описан с использованием математического аппарата переменных состояния, согласно теории оценки и управления их можно описать следующим образом:

$$\vec{X}_{i-1}(g) = A(k+1,k)\vec{D}_i(g) \oplus C(k+1,k)\vec{R}_i(g) \tag{2.7}$$

$$\vec{W}_{i-1}(g) = B(k+1,k)\vec{W}_i(g) \tag{2.8}$$

$$\vec{Z}_{i-1}(g) = \vec{X}_{i-1}(g) \oplus \vec{W}_{i-1}(g) \tag{2.9}$$

где $A(k+1,k)$ - переходная матрица источника данных, $C(k+1,k)$ - переходная матрица избыточности, $B(k+1,k)$ - переходная матрица потерь, k - текущий номер вектора оценки. Исходя из 2.7, модель источника данных можно представить как $\vec{D}_{i-1}(g) = A(k+1,k)\ldots\vec{D}_i(g)$:

$$\vec{D}_{i-1}(g) = \begin{bmatrix} 1 & 0 & \vdots & 0 \\ 0 & 1 & \vdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \vdots & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \tag{2.10}$$

Данное уравнение описывает источник данных, то есть передатчик АЗН-В. Уравнение 2.7 описывает источник потерь, а 2.8 - результат приема сообщения на стороне наземной станции. Прямая коррекция потерь сообщений (Forward Error Correction) может быть описана через компенсирование потерь вводом избыточности. Введем вектор избыточности $\vec{Y}(g)$, в таком случае вектор оценки будет выглядеть следующим образом:

$$\vec{Z}(g) = \vec{X}(g) \oplus \vec{W}_(g) \oplus \vec{Y}(g) \tag{2.11}$$

В свою очередь вектор коррекции определяется через следующие соотношения:

$$\vec{Y}(g) = \begin{cases} \vec{W}(g) \mid \sum_{j-1}^{X} w_j \leq \sum_{j-1}^{X} r_j \\ 0 \mid \sum_{j-1}^{X} w_j \geq \sum_{j-1}^{X} r_j \end{cases} \tag{2.12}$$

где $w_j \in \bar{0,1}$ и $r_j \in \bar{0,1}$ - бинарные элементы аекторов избыточности и потерь.

Исходя из описания вектора коррекции, можно сказать, что избыточные сообщения компенсируют потерянные сообщения, если сумма единичных элементов в векторе потерь, соответствующая количеству потерянных сообщений будет равна или меньше количеству избыточных сообщений. При равенстве количества потерянных и избыточных сообщений, данные поддаются полному восстановлению, например при использовании кода Рида-Соломона.

Таким образом, дано описание математической модели каналов информационного обмена с избыточностью. В виду ее универсальности, в дальнейшем данная модель может быть применена в имитационном моделировании ситуации зашумления канала или обрыва связи. Поскольку модель спуфинг-атаки, или атака слепой подмены представляет собой передачу ложных сообщений по тому же каналу связи, вектор данной атаки описывается теми же уравнениями информационного радиообмена, как и в случае с легитимными сообщениями. Единственным отличием в данной работе будем считать отличающиеся времена прихода сигналов и мощность принимаемого ложного сигнала. Для решения задачи фильтрации перейдем к описанию мультилатерационной модели, а также модели непосредственно системы анализа и фильтрации данных, на основе которых, в дальнейшем будет производиться имитационное моделирование работы разрабатываемой системы.

## 2.5 Разработка математической модели мультилатерационного метода определения местоположения воздушного судна в условиях несанкционированного вмешательства

### 2.5.1 Разработка критериев достоверности данных системы автоматического зависимого наблюдения

Необходимым шагом для фильтрации сообщений является разработка группы критериев, согласно которым будет производится выделение группы ложных данных и их дальнейший анализ. Разрабатываемые критерии будут применяться для оценки точности мультилатерационного метода противодействия несанкционированному вмешательству. Основываясь на нормативных документах ИКАО, введем показатели максимальной суммарной ошибки по высоте и в горизонтальной плоскости. Данные критерии могут быть описаны следующим образом:

$$\begin{array}{ccc} k_h = 2 \cdot |E_{ADS}| & & d_{ADS} = d_t + E_{ADS}; \\ k_v = |h_{min}| & E_{TDOA} \leq E_{ADS} & d_{TDOA} = d_t + E_{TDOA}; \\ k_h > d_{ADS} - d_{TDOA} & & d_{min} > E_{TDOA} + E_{ADS}; \end{array} \tag{2.13}$$

Введены следующие обозначения: $h_{min}$– максимальная суммарная ошибка по высоте (90 м) [13]; $d_{min}$ – максимально допустимое стандартное отклонение погрешности выдерживания траектории в боковой плоскости (550 м) [19]; $E_{ADS}$ – точность АЗН-В (0.1 морская миля, или 185 м) [20]; $E_{TDOA}$– необходимая точность гиперболического метода; $d_{ADS}$ – расстояние от начала координат по АЗН-В; $d_{TDOA}$ – расчетное расстояние от начала координат; $d_t$ – истинное расстояние от начала координат.

Таким образом, если в полученном сообщении от АЗН-В передатчика указано положение 1 для ВС (см. 2.23), расстояние до которого от расчетного не превышает величины двукратной ошибки $E_{ADS}$ (370 м), то информация о координатах объекта полагается достоверной. В противном случае (положения ВС 2 и 3) такая информация будет считаться ложной. Такой подход позволя-

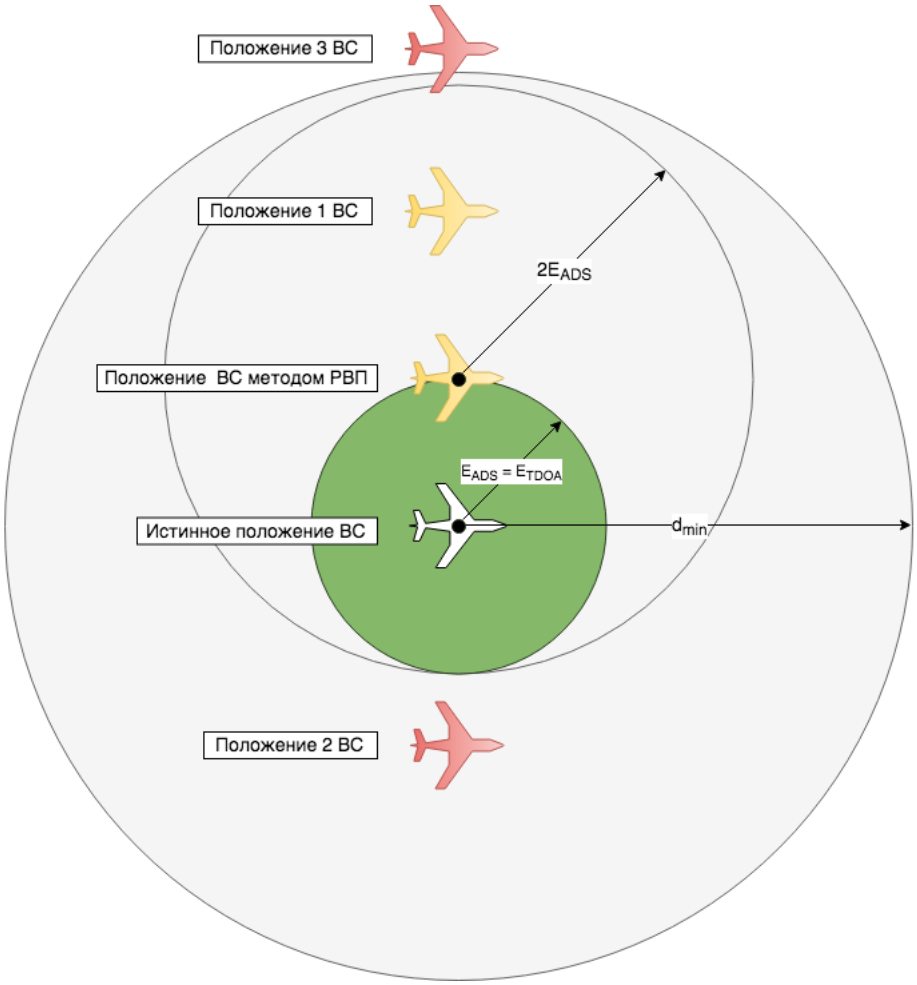



Рисунок 2.23 — Схема фильтрации в соответствии с критериями истинности

ет с одной стороны избежать ошибок первого рода, благодаря чему сообщение ВС, содержащее координаты в пределах $E_{ADS}$ (185 м), будет определено как истинное, а с другой стороны избежать ошибок второго рода, пометив ложным сообщение ВС, содержащее координаты вне радиуса $d_{min}$ (550 м). Учитывая ограничение снизу на число БС, их количество следует планировать с запасом, а это, в свою очередь, приводит к избыточности числа уравнений в задаче определения координат ВС.

### 2.5.2 Исследование математических моделей при работе с избыточными данными

Для успешного вычисления местоположения методом мультилатерации, оценки ошибки определения местоположения, и как следствие, успешной ра-

боты системы защиты информации от спуфинг атак была применена математическая модель гиперболической системы локации (разностно-дальномерный способ). Гиперболический метод (TDOA) основан на измерении разностей времен прихода сигналов (РВП) или расстояний от объекта до пунктов приема. Эти разности определяются путем измерения относительных временных задержек сигналов, принимаемых в различных пунктах приема. Для определения местоположения источника радиоизлучения в пространстве с помощью пассивной РТС с фиксированной базой гиперболическим методом необходимо знать результаты независимых измерений трех разностей расстояний, для чего требуется как минимум четыре пункта приема, при этом существует 2 варианта работы данного метода. Первый метод используется в навигационных системах ЛОРАН-С, в этом случае источник производит самостоятельный расчет местоположения. Второй метод, который, в свою очередь, используется в данной работе, применяется в системах экстренных служб (911/112) и расчет местоположения источника излучения происходит с помощью расчета разницы времен прихода.

После определения РВП сигналов между парами БС $T_10, T_20, T_30, ..., T_{n0}$ производится расчет разностей расстояний $d_{10}, d_{20}, d_{30}, ..., d_{n0}$. Для определения местоположения источника радиоизлучения в пространстве с помощью пассивной РТС с фиксированной базой гиперболическим методом необходимо знать результаты независимых измерений двух разностей расстояний, для чего требуется как минимум 3 пункта приема. Тривиальная система уравнений, позволяющая определить координаты источника излучения, имеет вид:

$$\begin{cases} \grave{T_{10}} = T_1 - T_0 \Longrightarrow d_{10} = \grave{T}_{10} \cdot c \\ \grave{T_{20}} = T_2 - T_0 \Longrightarrow d_{20} = \grave{T}_{20} \cdot c \end{cases} \tag{2.14}$$

где расстояния рассчитываются по формулам:

$$\begin{cases} d_{10} = \sqrt{(x_1 - x)^2 + (y_1 - y)^2} - \sqrt{(x_0 - x)^2 + (y_0 - y)^2} \\ d_{20} = \sqrt{(x_2 - x)^2 + (y_2 - y)^2} - \sqrt{(x_0 - x)^2 + (y_0 - y)^2} \end{cases} \tag{2.15}$$

Положение источника радиоизлучения на плоскости определяется как точка пересечения двух гипербол с фокусами в точках расположения пунктов приема [51] . Иллюстрация представлена на рисунке 2.24

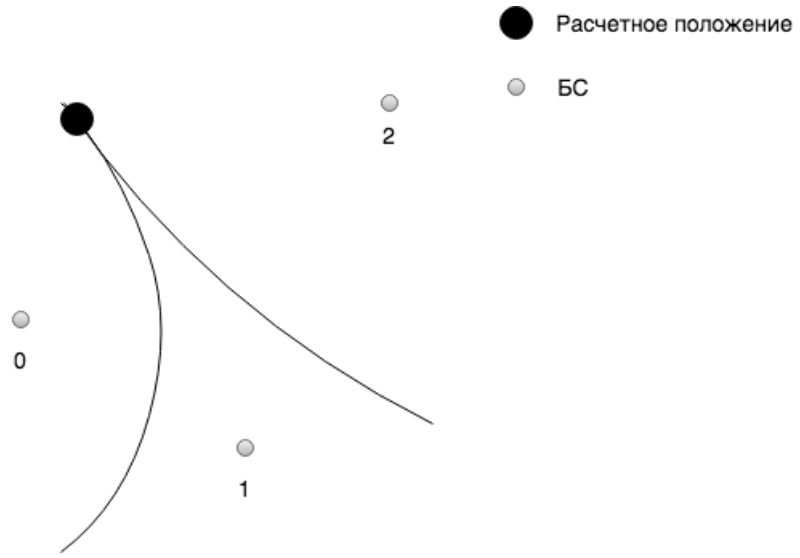



Рисунок 2.24 — Геометрическая иллюстрация к гиперболическому методу определения местоположения

Для точного определения момента времени прихода сигнала необходимо, чтобы группа БС имела единое время, то есть была синхронизирована с высокой точностью. Для достижения высокой точности могут применяться приемники временной синхронизации, например, СН-5831, среднеквадратичная погрешность которых составляет 15 нс [54].

Поскольку при определении местоположения цели таким методом зачастую происходит ситуация нахождения источника излучения в зоне приема нескольких наземных станций, возникает проблема избыточных данных, при использовании которых нельзя решить задачу тривиальным способом. Для успешного вычисления местоположения в условиях избыточных данных рассмотрим и применим две математические модели - метод наименьших квадратов (МНК) и метод рядов Тейлора.

Рассмотрим метод наименьших квадратов. Пусть (x,y) будут координатами источника излучения, а (Xi, Yi) ,будут заранее известными координатами базовой станции, где I = 1,2,3,..,M. M – конечное число наземных (базовых) станций (БС), принимающих участие в местонахождении источника излучения. Примем одну из станций в качестве опорной, пусть это будет БС№1. Разности расстояний между базовыми станциями и источником сигнала будут опреде-

ляться следующим выражением [39]:

$$\tau_{1i} = \frac{1}{c}\|S - S_1\| - \frac{1}{c}\|S - S_i\| = \frac{1}{c}(D_1 - D_i);\ d_{1i} = \tau_{1i} \cdot c = D_1 - D_i \tag{2.16}$$

$$D_1^2 - D_i^2 = \|S - S_1\|^2 - \|S - S_i\|^2 = x_1^2 - x_i^2 + 2x(x_i - x_1) + y_1^2 - y_i^2 + 2y(y_i - y_1) \tag{2.17}$$

$$D_1^2 - D_i^2 = 2D_1^2 d_{1i} - d_{1i}^2 \tag{2.18}$$

где $c$ - скорость распространения электромагнитной волны, $d_{i,1}$ - TDOA (разность времени прихода) между i–ой базовой станцией и опорной. В соответствии с [37] выражение 2.18 примет вид

$$(x - x_1)(x_i - x_1) + (y - y_1)(y_i - y_1) + d_{1i}D_i = \frac{1}{2}\left[(x_i - x_1)^2 + (y_i - y_1)^2 - d_{1i}^2\right] \tag{2.19}$$

Представим систему уравнений в матричной форме:

$$AX = b \tag{2.20}$$

Решением системы будет нахождение матрицы X [43], исходя из выражений 2.22 и 2.24:

$$A = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 & r_{21} \\ x_3 - x_1 & y_3 - y_1 & r_{31} \\ & \vdots & \\ x_m - x_1 & y_M - y_1 & r_{M1} \end{bmatrix} \tag{2.21}$$

$$X = \begin{bmatrix} x_s - x_1 & y_s - y_1 & r_1 \end{bmatrix}^T \tag{2.22}$$

$$b = \frac{1}{2}\begin{bmatrix} (x_2 - x_1)^2 + (y_2 - y_1)^2 - r_{21}^2 \\ (x_3 - x_1)^2 + (y_3 - y_1)^2 - r_{31}^2 \\ \vdots \\ (x_M - x_1)^2 + (y_M - y_1)^2 - r_{M1}^2 \end{bmatrix} \tag{2.23}$$

$$X = \left(A^T A\right)^{-1} A^T b \tag{2.24}$$

Учтем аддитивную ошибку определения времени прихода сигнала ($\epsilon$)

$$X = \left(A^T A\right)^{-1} A^T b \tag{2.25}$$

и произведем линейную аппроксимацию методом наименьших квадратов:

$$\hat{X} = arg \min_{X}(AX - b)^T(AX - b) = \left(A^T A\right)^{-1} A^T b = A^+ b \tag{2.26}$$

Другим подходом определения местоположения при наличии избыточных данных является итеративный метод рядов Тейлора. Разложение в ряд Тейлора может быть использовано для решения гиперболических уравнений. Обладая множеством накопленных данных о разностях времен прихода, данный метод подразумевает использование начального приближения и вычисляет отклонение оценки определения местоположения. Выражение 2.17 может быть переписано как функция

$$f_i(x,y) = \sqrt{(x - X_{i+1})^2 + (y - Y_{i+1})^2} - \sqrt{(x - X_1)^2 + (y - Y_1)^2} \tag{2.27}$$

где $i = 1,2,...,N-1$ Пусть $t_i$ будет временем приема сигнала i-ой базовой станции, тогда

$$f_i(x,y) = d_{i+1,1} + \epsilon_{i+1,1} \tag{2.28}$$

где

$$d_{i+1,1} = c \cdot (t_{i+1} - t_1) \tag{2.29}$$

$\epsilon$ - ошибка определения разности расстояний с ковариацией $R$. Пусть $(x_0, y_0)$ - начальное приближение координат цели, тогда

$$x = x_0 + \delta_x; y = y_0 + \delta_y \tag{2.30}$$

Разложив выражение 2.27 в ряд Тейлора согласно [12], получаем:

$$f_{i,0} + a_{i,1}\delta_x + a_{i,1}\delta_y(\quad)d_{i+1,1} + \epsilon_{i+1,1} \tag{2.31}$$

$$\begin{cases} f_{i,0} = f_i \cdot (x_0,y_0) \\ a_{i,1} = \left.\dfrac{\partial f_i}{\partial x}\right|_{x_0,y_0} = \frac{X_1 - x_0}{d_1} - \frac{X_{i+1} - x_0}{d_{i+1}} \\ \widehat{d_i} = \sqrt{(x_0 - X_i)^2 + (y_0 - Y_i)^2} \\ a_{i,2} = \left.\dfrac{\partial f_i}{\partial x}\right|_{x_0,y_0} = \frac{Y_1 - y_0}{d_1} - \frac{Y_{i+1} - y_0}{d_{i+1}} \end{cases} \tag{2.32}$$

Соотношение 2.31 может быть переписано в матричном виде:

$$A\delta = D + \epsilon \tag{2.33}$$

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \\ \vdots & \vdots \\ a_{N-1,1} & a_{N-1,2} \end{bmatrix};\ \delta = \begin{bmatrix} \delta_x \\ \delta_y \end{bmatrix};\ D = \begin{bmatrix} \widehat{d_{2,1}} - f_{1,0} \\ \widehat{d_{3,1}} - f_{2,0} \\ \vdots \\ \widehat{d_{N,1}} - f_{N-1,0} \end{bmatrix};\ \epsilon = \begin{bmatrix} \epsilon_{2,1} \\ \epsilon_{3,1} \\ \vdots \\ \epsilon_{N,1} \end{bmatrix}. \tag{2.34}$$

$$\delta = [A^T R^{-1} A]^{-1} \cdot A^T R^{-1} D \tag{2.35}$$

где $R$ - ковариационная матрица ошибок, определяемая в соответствии с [5] как

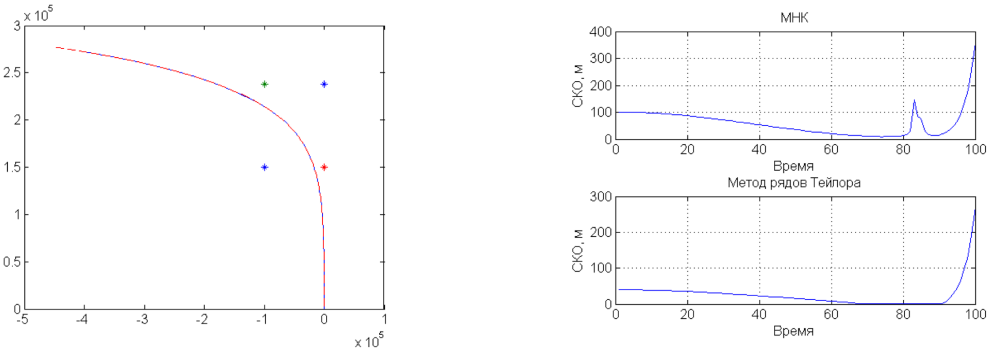
$$R = M(\epsilon) \cdot \begin{bmatrix} 1 & \cdots & 0.5 \\ \vdots & \ddots & \vdots \\ 0.5 & \cdots & 1 \end{bmatrix} \tag{2.36}$$

Итерации продолжаются до тех пор, пока девиация x и y не станет пренебрежительно малой. Метод рядов Тейлора дает точные результаты в случае если начальное приближение выбрано верно [2]. В качестве начального приближения может использоваться как плановая информация, так и информация, получаемая от других источников.

Для определения точности используемых моделей, проведем имитационное моделирование. Для этого примем, что ошибки в оценке положения ВС порождаются ошибками оценки времени прихода сигнала, которые для каждой БС независимы и в эксперименте полагаются равномерно распределенными от 0 до 15 нс. Количество БС варьируется от 4 до 8. Для решения системы уравнений методом Тейлора при моделировании использовалось 10 итераций, начальное приближение выбиралось случайно в радиусе 20 км (максимальная ширина воздушного коридора[65]) от истинного положения ВС. Поскольку траектория движения ВС непрерывна, для последующих моментов времени в качестве начального приближения выбиралось расчетное местоположение ВС в предыдущий момент времени. Для оценки точности определения местоположения для каждого метода рассчитывалось его СКО, определяемое по формуле:

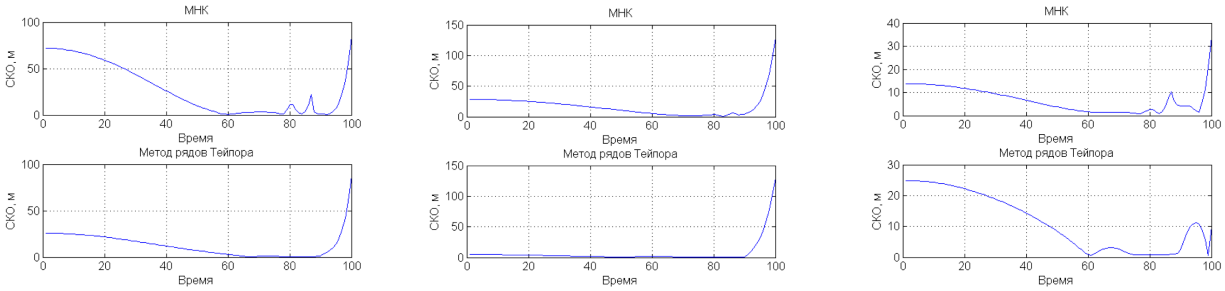
$$[H]D(t) = M\left[(x(t) - \hat{x}(t,\omega))^2 + (y(t) - \hat{y}(t,\omega))^2\right];\ \sigma(t) = \sqrt{D(t)} \tag{2.37}$$

где $(x,y)$ - реальные координаты объекта, $(\hat{x},\hat{y})$ - расчетные координаты объекта, $M$ - математическое ожидание, $\omega$ - элементарное событие. Для заданной траектории движения рассчитывались несколько вариантов определения местоположения в соответствии с числом БС. Результаты расчетов приведены на рисунках 2.25 и 2.26




а) б)

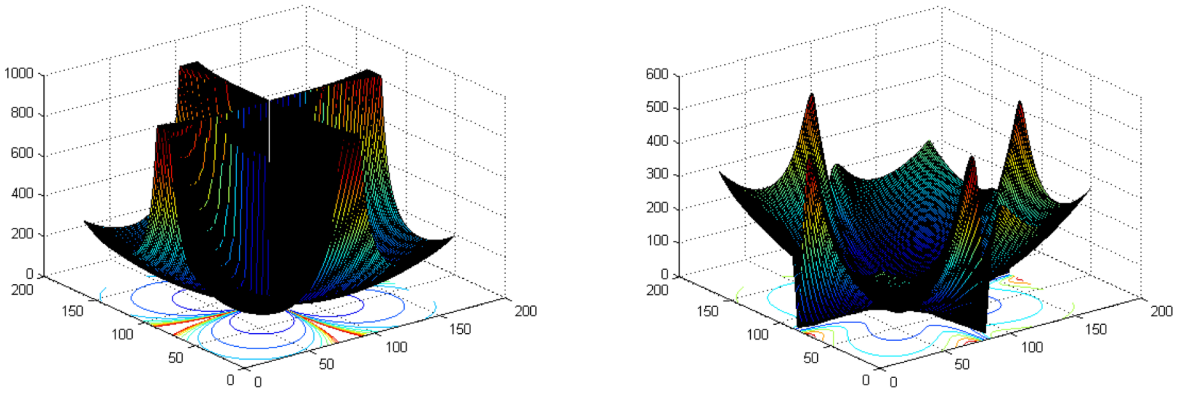
Рисунок 2.25 — Расчетная траектория ВС для 4-х БС (а) и сравнение СКО ошибки для МНК и метода рядов Тейлора (б)




а) б) в)

Рисунок 2.26 — СКО для МНК и метода рядов Тейлора. для 5-ти (а), 6-ти (б) и 8-ми (в) БС соответственно

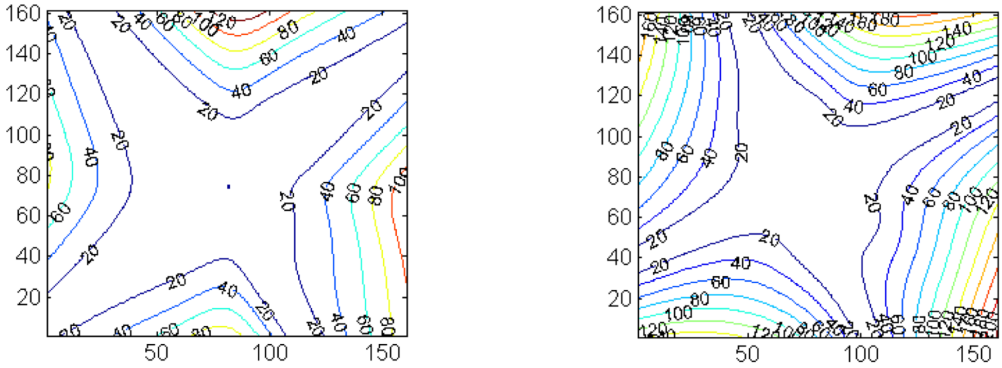
Как видно из приведенных графиков, наименьшее СКО наблюдается от 80 до 90 секунды – временем прохождения ВС через область группы между БС. При четырех БС ошибки МНК в несколько порядков превышают ошибки, возникшие в результате определения местоположения методом рядов Тейлора (рис. 2.27) Этим объясняются всплески ошибок МНК на рисунках 2.25 и 2.26




а) б)

Рисунок 2.27 — Поверхность ошибок (СКО, м) при 4-х БС для МНК (а) и метода рядов Тейлора (б)

Подробное описание подхода к имитационному моделированию изложено в приложении А. По результатом проведенного моделирования можно утверждать, что при числе БС от 4 до 6-ти метод рядов Тейлора показывает наилучшие результаты. При неравномерных ошибках на БС и/или для группы из восьми БС, точность определения местоположения методом рядов Тейлора становится ниже, чем для МНК (рис. 2.28).




а) б)

Рисунок 2.28 — Контурный график ошибок при 8-ми БС для МНК (а) и метода рядов Тейлора (б)

Проведенный имитационный эксперимент [52] позволил выявить следующие особенности применения МНК и метода рядов Тейлора:

1. При количестве БС от 4 до 6-ти метод рядов Тейлора в задаче определения местоположения ВС является наиболее точным (на 15-40 процентов точнее МНК, в зависимости от состава группы БС).
2. При количестве БС от 8-ми и более метод рядов Тейлора показывает одинаковые либо более худшие точностные характеристики по сравнению с МНК
3. При неравномерных ошибках (отличающихся в несколько раз) определения момента времени прихода сигналов, МНК показывает более точные результаты (количество БС$>$6)
4. Для метода рядов Тейлора СКО при числе БС от 4 до 8-ми гарантированно меньше критерия точности в радиусе 210 км от каждой из БС.

## 2.6 Разработка алгоритмов системы анализа и фильтрации сообщений АЗН-В

Спуфинг атака на систему АЗН-В может быть рассмотрена как DDOS-атака на информационную систему, в рамках которой вектором атаки являются ложные сообщения, транслируемые в эфир. При решении задачи создания информационной системы анализа и фильтрации необходимо обратиться к уже существующим системам по противодействию вторжению (IDS) и использованию методов по анализу и выявлению DDOS-атак. Для осуществления поставленных целей необходимо на основе предложенных математических алгоритмов определения истинного местоположения создать алгоритм фильтрации потока входных данных в реальном режиме времени, определить его облик и место в рамках современной АС УВД.

Рассмотрим алгоритм определения местоположения цели РВП-методом. На синхронизированные по GNSS станции приема поступает сообщение АЗН-В, содержащее информацию об ID воздушного судна и его координаты. Создается хэш (ассоциативный массив), в котором, помимо информации о ВС добавляется информация о времени прихода сигнала.

Листинг 2.1

Пример пакета данных в формате JSON

```
{
  "icao_aa": {
    "id": "AC82EC",
    "format": "hex"
   },
   "snr": "-61.7",
   "location": ["31.67853", "54.87412"],
   "toa": "1528059383111834921",
   "md5hash": "b0fecf7ae6d87776b11fd4a4ad69b82b"
}
```

Данные сообщения пересылаются в вычислитель местоположения РВП-методом, перед использованием полученных данных, определяется достоверность сообщения от приемной станции путем вычисления MD5-суммы от со-

держимого сообщения с общим секретом и её сравнения со значением внутри JSON.

Листинг 2.2

Пример проверки валидности сообщения на Python

```
import md5

def function(message,secret)
    recieved = message["md5hash"]
    signstring = message["icao_aa"]["id"] + message["icao_aa"]["format"] +
        ↪ message["snr"] + message["location"][0] + message["location"][1] +
        ↪ message["toa"]
    calculated = md5.new(signstring).hexdigest()
    if (str(recieved) == str(calculated)):
        return true
    else
        return false
```

Для каждого нового сообщения, прошедшего проверку, производится поиск соответствующего буфера памяти. Каждый буфер памяти предназначен для накопления данных по одному ВС. В случае если сообщение содержит ICAO адрес судна, которого нет ни в одном из буферов, происходит создание нового (буфера). По истечению заданного промежутка времени (10..100 мс) после появления первого сообщения АЗН, производится подсчет уникальных сообщений внутри буфера. Под уникальными понимаются сообщения, полученные от разных приемных станций. В случае, если в результате подсчета количество таких сообщений составляет от трёх и более, производится вычисление местоположения цели наиболее подходящим гиперболическим методом. Если же общее количество сообщений для одного ВС меньше трёх, сообщение АЗН-В, полученное первым для заданного ВС, передается в АС УВД с пометкой об отсутствии проверки. Содержимое буфера перемещается из памяти в СУБД.

Листинг 2.3

Пример содержимого буфера памяти в формате JSON

```
{
  "A8CE6F": {
    "creation_time": "1528134844173",
    "messages": [
      {
        "reciever": "0002",
        "toa": "1528134843940876",
        "location": ["31.67853", "54.87412"]
      },
      ***
      {
        "reciever": "0009",
        "toa": "1528134843940516",
        "location": ["31.67853", "54.87412"]
      }
    ]
  },
  "B2FE6A": {
    "creation_time": "1528134844184",
    "messages": [
      ***
    ]
  }
}
```

После расчета местоположения гиперболическим методом производится сравнение расчетного местоположения с массивом полученных местоположений для заданного ВС и времени прибытия первого сообщения данного ВС в буфер. Местоположения с разных станций приема извлекаются из базы данных - поиск производится по ключам "адрес воздушного судна"и "время прихода первого сообщения"(key = A8CE6F,1528134844173)

Листинг 2.4

Пример ассоциативного массива для сравнения данных АЗН-В

```
{
  "A8CE6F": {
    "creation_time": "1528134844173",
    "calculated_loc": ["31.67856", "54.87414"],
    "recieved_loc": [
      ["31.67853", "54.87412"],
      ["31.67853", "54.87412"],
      ["31.67853", "54.87412"],
      ["31.67853", "54.87412"],
      ["31.67853", "54.87412"]
    ]
}
```

В случае если были сообщены разные местоположения ВС, выбирается ближайшее к местоположению, вычисленным методом РВП. Если ни одно из сообщений не удовлетворяет критерием истинности, производится оповещение о спуфинг атаке и реальном местоположении ложной цели.

Листинг 2.5

Пример реализации механизма буферизации с очисткой на Python

```
import threading
import time

class TTLDict(dict):
    """ A dictionary with keys having specific time to live """
    def __init__(self, ttl=5):
        self._ttl = ttl
        # Internal key mapping keys of _d
        # to times of access
        self.__map = {}
        self._flag = True
        self._t = threading.Thread(target=self._collect)
        self._t.setDaemon(True)
        self._t.start()
```

Для наглядности обработки сообщений АЗН, приведем соответствующий алгоритм 2.29:

Рисунок 2.29 — Алгоритм определения местоположения ВС для протокола 1090 ES

Алгоритм предполагает следующую последовательность операций:

1. Данные поступают от источников АЗН на приемник сообщений 1090ES. Параллельно эти же сигналы, с той же содержащейся в них информацией, поступают на аналогичные приемники АЗН. Для успешной работы системы защиты информации их должно быть минимум 3 для определения местоположения на плоскости и 4 для определения местоположения в пространстве.
2. В паре с приемником АЗН сообщений используется синхронизатор ГНСС, необходимый для установки точного времени на приемном оборудовании. Синхронизатор ГНСС получает точные время и координаты, используя приемник ГЛОНАСС/GPS.
3. Приемник декодирует сообщения АЗН и помимо основной информации инкапсулирует данные о времени прихода сигналов и местоположении наземной станции.

4. Пакет данных передается по каналу связи, предусмотренному на этапе внедрения системы АЗН. В качестве канала может быть использована любая среда передачи данных, предусмотренная действующей системой АЗН.
5. Информация со всех источников поступает в центр обработки данных, происходит декодирование пакетов данных.
6. Параллельно в ЦОДе используется аналогичный синхронизатор, что и на приемных станциях. Таким образом достигается основная синхронизация всех объектов системы.
7. Для уменьшения влияния помех на синхронизацию устройств, производится дополнительная коррекция времени, основанная на вычислении задержки передачи данных по различным каналам. Сравнивается время от синхронизаторов на ЦОДе и на приемных РЛС.
8. Для каждого сообщения создается вектор, содержащий информацию об ID, вещаемых координатах, времени прихода. Данные векторы помещаются в буфер для временного хранения.
9. Производится выборка по векторам с одинаковым ID и одинаковыми координатами.
10. В том случае, если количество векторов меньше трех, программа отбрасывает эти данные
11. Если количество векторов больше или равно трем, производится расчет местоположения воздушного судна, основанный на вычислении РВП сигнала методами, описанными во второй главе.
12. Далее производится сравнение данных АЗН, полученных с помощью алгоритма, и данных, полученных от первоначального источника.
13. Координаты, полученные в ходе проведения алгоритма, записываются в память. Вычисляется скорость движения ВС.
14. Скорость ВС сравнивается с документированной скоростью ВС, имеющих на борту оборудование АЗН.
15. Производится сравнение траектории с плановой информацией.
16. Полученные сравнения агрегируются и принимается решение о фильтрации данных.
17. Отфильтрованные данные инкапсулируются в ASTERIX и отправляются в АС УВД.

Предложенный алгоритм имеет ограничения, связанные с особенностями гиперболического метода. По этой причине, в случае, если при работе системы анализа их будет менее трех, необходимо использовать другие способы определения истинности сообщений. В предыдущей части работы, наряду с разностно-временными методами определения местоположения были также рассмотрены методы машинного обучения (монолатерация). Одним из ограничений метода монолатерации является необходимость в периодическом обучении алгоритмов определения истинности сообщений, однако учитывая доступность и количество данных АЗН-В это ограничение накладывает лишь дополнительные расходы при проектировании системы.

Рассмотрим возможность использования метода монолатерации при анализе сообщений АЗН на предмет несанкционированного вмешательства. На этапе сбора информации, система, построенная на этом методе не будет принципиально отличаться от системы анализа с помощью РВП. Отличием такой системы в этой части будет лишь отсутствие буфера памяти для сообщений от одного воздушного судна - данный логический компонент является избыточным - обработка данных производится внутри СУБД (например Clickhouse) и не требует обязательного подсчета количества сообщений от конкретного ВС в единицу времени. Однако, переходя к анализу данных, при таком подходе используется совсем иная логика обнаружения ложных сообщений. Основываясь на данных полученных в результате имитационного моделирования несанкционированного вмешательствах, методы машинного обучения с учителем, позволяют классифицировать сообщения как ложные или истинные. Признаками, по которым производится обучение и последующий анализ, являются информационные параметры сообщений, а также информация о физических свойствах принимаемого сигнала. Исходя из того, что злоумышленник не обладает достаточной полнотой информации, такой как диаграмма направленности антенны приемного устройства и радиообстановка в точке приема, такой подход может быть рассмотрен в рамках разрабатываемой системы.

Для наглядности обработки сообщений АЗН данным методом, приведем соответствующий алгоритм 2.30:

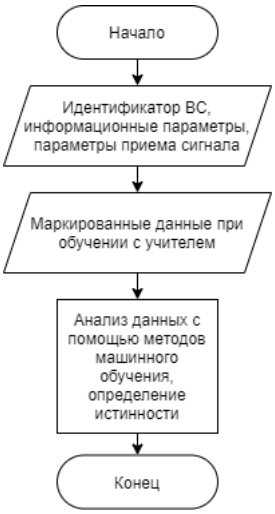



Рисунок 2.30 — Алгоритм определения местоположения ВС для протокола 1090 ES

Алгоритм обучения производится следующим образом:

1. Данные поступают от источников АЗН на приемник сообщений 1090ES.
2. Производится генерация ложных данных разных уровней сложности: случайные ложные данные, данные сгенерированные в соответствии с моделью движения ВС, данные сгенерированные в соответствии с реальными данными АЗН-В, дублированные данные АЗН-В.
3. Публикация ложных данных в радиоэфир.
4. Приемник декодирует сообщения АЗН и преобразовывает полученную информацию в единый формат для последующей обработки в центре обработки данных.
5. Пакет данных передается по каналу связи, в центр обработки данных.
6. Для каждого сообщения создается вектор, содержащий информацию об ID, вещаемых координатах, времени прихода, параметров приема сигнала. Также подсчитывается пеленг сигнала, исходя из сообщенной информации. Данные векторы помещаются в буфер для временного хранения.
7. Данные преобразовываются и очищаются - производится удаление дубликатов, очевидно избыточных признаков
8. Производится dummy-кодирование категориальных признаков (замена категориального признака на q бинарных признаков)
9. Осуществляется обработка несбалансированной выборки.
10. Выборка разделяется на обучающую и тестовую.

11. Производится анализ на обучающей выборки выбранным методом машинного обучения.
12. Рассчитывается точность алгоритма.
13. Производится изменение параметров алгоритма для минимизации функции потерь.
14. Производится анализ на тестовой выборки выбранным методом машинного обучения.

При реальном использовании алгоритма, предлагается следующая последовательность операций:

1. Данные поступают от источников АЗН на приемник сообщений 1090ES.
2. Приемник декодирует сообщения АЗН и преобразовывает полученную информацию в единый формат для последующей обработки в центре обработки данных.
3. Пакет данных передается по каналу связи, предусмотренному на этапе внедрения системы АЗН, в центр обработки данных. В качестве канала может быть использована любая среда передачи данных, предусмотренная действующей системой АЗН.
4. Для каждого сообщения создается вектор, содержащий информацию об ID, вещаемых координатах, времени прихода, параметров приема сигнала. Также подсчитывается пеленг сигнала, исходя из сообщенной информации. Данные векторы помещаются в буфер для временного хранения.
5. Данные преобразовываются и очищаются - производится удаление дубликатов, очевидно избыточных признаков
6. Производится dummy-кодирование категориальных признаков (замена категориального признака на q бинарных признаков)
7. Обработка несбалансированной выборки.
8. Производится анализ тестовой выборки выбранным методом машинного обучения.
9. Производится сравнение траектории с плановой информацией.
10. Полученные сравнения агрегируются и принимается решение о фильтрации данных.

11. Прошедшие проверку данные инкапсулируются в ASTERIX и отправляются в АС УВД.

Таким образом, разработанные алгоритмы обнаружения сообщений, полученных в результате несанкционированного вмешательства, могут применяться как в случае наличия полноценной группы приемных устройств, так и в случае работы только одного приемного устройства. Предложенные алгоритмы будут апробированы в ходе имитационных и натурных экспериментов в четвертой главе.

# Глава 3. Практическое применение методов и алгоритмов валидации сообщений системы автоматического зависимого наблюдения

Очевидно, что для построения системы анализа и фильтрации сообщений АЗН-В необходимо использование накопленной и постоянно обновляемой информации. В 2012 году група исследователей из Armasuisse, Технического университета Кайзерслаутерна и Оксфордского Университета выступило с инициативой создания некоммерческой организации Opensky-Network, основной деятельностью которой является предоставление данных АЗН-В для академических исследований. Информация о местоположении ВС доступна как для реального времени (с минимальными задержками), так и для прошедшего периода времени. На момент написания работы система располагает 210 приемниками расположенных по всему миру. Наработки, примененные при построении архитектуры Opensky-Network можно применить к разрабатываемой системе по причине обработки аналогичного количества данных и использованию современных подходов к построению ИТ-систем. Поскольку наиболее уязвимой к атакам подмены является технология АЗН, упор при построении архитектуры будет производиться с учетом обеспечения достоверности именно данных АЗН-В.

## 3.1 Определение местоположения ВС в условиях несанкционированного вмешательства на систему автоматического зависимого наблюдения

Задача определения местоположения в условиях несанкционированного вмешательства может быть решена с использованием комплексного подхода - с применением простых методов определения аномалий и последующим определением местоположения ВС с помощью гиперболического метода, либо классификацией сообщения методом монолатерации (машинного обучения). Это позволит повысить точность фильтрации и снизить вычислительную нагрузку. Для осуществления данного подхода необходимо произвести потоковую обработку данных в два этапа первый из которых заключается в поиске аномалий в реальном режиме времени с последующей пометкой сообщений, как подозрительные, а второй - в анализе непомеченных сообщений на основе методов пассивной радиолокации или машинного обучения. Данный алгоритм далее называется гибридым, поскольку в нем используется как метод мультилатерации, так и метод монолатерации.

Определим основные этапы анализа данных:

1. Получение данных АЗН-В.
2. Декодирование данных АЗН-В, извлечение сообщений.
3. Определение времени прихода сигналов, построение логических связей между сигналом и содержимым сообщения.
4. Определение наличия отклонений параметров сообщений АЗН-В.
5. Определение превышения интегрального показателя отклонений параметров.
6. Расчет местоположения гиперболическим методом.
7. При недостаточном количестве данных - классификация сообщений методами машинного обучения.
8. Пометка сообщений по результатам проведенного анализа данных.

Приведем алгоритм вычисления местоположения на диаграмме 3.1

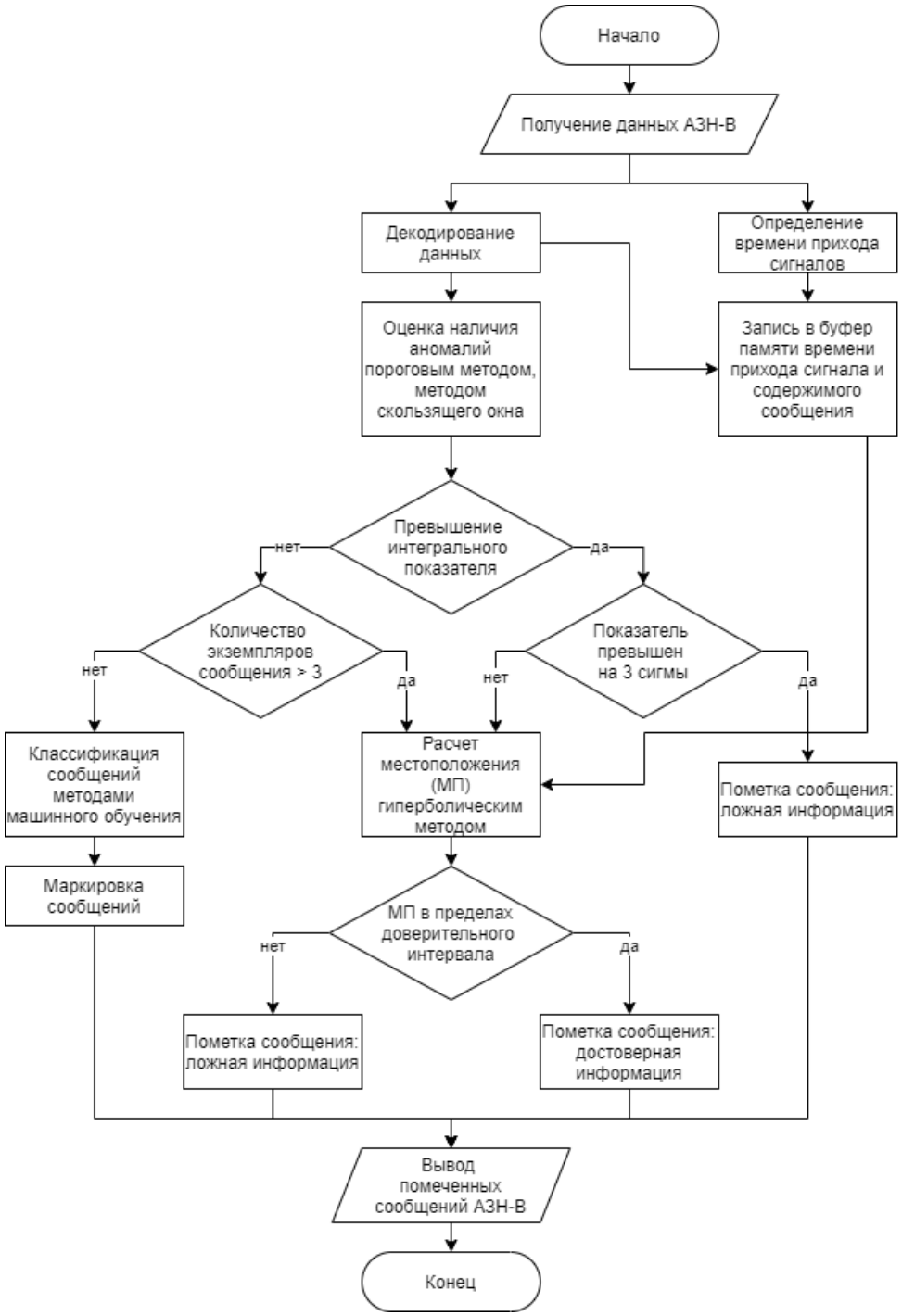



Рисунок 3.1 — Гибридный алгоритм определения местоположения судна в условиях несанкционированного вмешательства

Рассмотрим подробнее каждый из элементов гибридного алгоритма определения местоположения судна в условиях несанкционированного вмешательства.

Накопленные данные АЗН-В позволяют выделить показатели по каждому из параметров сообщения. Под показателями в данной работе будем подразумевать функцию над параметром сообщения АЗН-В. При постановке эксперимен-

та использовались следующие параметры: формат пакета (Downlink Format), тип сообщения АЗН-В (Type Code), код воздушного судна ИКАО (ICAO aircraft address), сообщаемое местоположение (Latitude/Longitude), барометрическая высота (Altitude), скорость (Velocity), направление (Heading), код рейса (Call Sign), время получения сообщения. Поскольку в каждом сообщении должен присутствовать код воздушного судна ИКАО, то в общем случае формирование показателя для воздушного судна может быть представлено как:

$$f_i(ICAO_addr, L_1...L_k) = agr_i(p_i(ICAO_addr, L_1...L_k)) \tag{3.1}$$

где $f_i(ICAO_addr, L_1...L_k)$ - $i$-ый показатель, для воздушного судна с кодом ($ICAO_addr$). Дополнительно, для формирования показателя могут применяться условия $L_1...L_k$, являющиеся значениями обязательных полей сообщения АЗН-В. Одним из таких условий может выступать формат сообщения. Над параметром сообщения $p_i$ применяется агрегатная функция $agr_i$.

Показатели рассчитываются для каждой секунды (1s), минуты(1m) и пяти минут(5m). Агрегатные функции могут быть составлены из нескольких функций. В данной работе использовались следующие показатели, в разрезе по каждому коду ICAO:

- количество сообщений каждого из m форматов;
- количество сообщений каждого из t типов сообщений АЗН-В (Type Code);
- количество уникальных сообщений каждого из m форматов;
- количество уникальных сообщений каждого из t типов сообщений АЗН-В (Type Code);
- пройденное расстояние;
- скорость ВС;
- высота полета ВС;
- направление полета ВС;
- разница (в узлах) между сообщенной скоростью и расчетной скоростью по пройденному расстоянию;
- разница (в угловых градусах) между сообщенным курсом и расчетным курсом;

Опишем формулы данных показателей с использованием функций аналитической СУБД Clickhouse:

Листинг 3.1

Пример расчета показателей

```
f(ICAO\_addr, DF_m, t) = count(ICAO\_addr, DF_m, t);
f(ICAO\_addr, TC_t, t) = count(ICAO\_addr, TC_t, t);
f(ICAO\_addr, DF_m, t) = count(ICAO\_addr, uniq(DF_m), t);
f(ICAO\_addr, TC_t, t) = count(ICAO\_addr, uniq(TC_t), t);
f(ICAO\_addr, [DF_17, TC_9..18], t) =
greatCircleDistance( DF_17(ICAO\_addr, TC_9..18, t)[0],
DF_17(ICAO\_addr, TC_9..18, t)[1],
DF_17(ICAO\_addr, TC_9..18, t-1)[0],
DF_17(ICAO\_addr, TC_9..18, t-1)[1]);
f(ICAO\_addr, [DF_17, TC_19], t) =
avg(DF_17(ICAO\_addr, TC_19, t));
f(ICAO\_addr, [DF_17, TC_9..18], alt, t) =
avg(DF_17(ICAO\_addr, TC_9..18, alt, t));
f(ICAO\_addr, [DF_17, TC_9..18], head, t) =
avg(DF_17(ICAO\_addr, TC_9..18, head, t));
f(ICAO\_addr, [DF_17, TC_19], t) =
avg(DF_17(ICAO\_addr, TC_19, t));
```

Аномалии в данных АЗН-В могут быть отнесены к одному из трех основных типов [6] - точечные, контекстуальные и коллективные.

Точечные аномалии возникают в ситуации, когда отдельный экземпляр данных может рассматриваться как аномальный по отношению к остальным данным. В случае с временным рядом данных такие аномалии представляют собой "выбросы"или "всплески"значений 3.2.

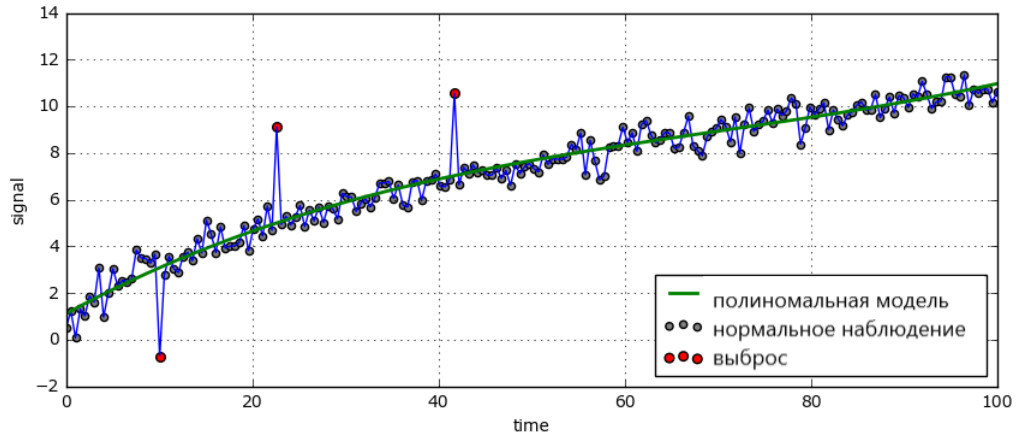



Рисунок 3.2 — Пример точечной аномалии

Контекстуальные аномалии наблюдаются, если экземпляр данных является аномальным лишь в определенном контексте, (данный вид аномалий также называется условным). Примером такого вида аномалии может быть отклонение показателя от периодической последовательности. Для определения аномалий этого типа основным является выделение контекстуальных и поведенческих атрибутов. Данный вид аномалий в условиях анализа данных в режиме реального времени может быть представлен как сдвиг 3.3.

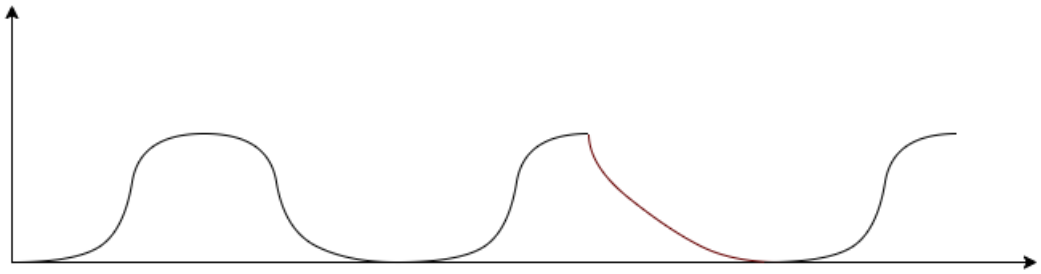


Рисунок 3.3 — Пример контекстуальной аномалии

Под типом коллективных аномалий подразумевается аномальная последовательность группы экземпляров данных по отношению к целому набору данных. Единичный экземпляр данных в такой последовательности может не подходить ни под одно из условий приведенных выше для точечных и контекстуальных аномалий, однако совместное появление таких экземпляров является коллективной аномалией 3.4.

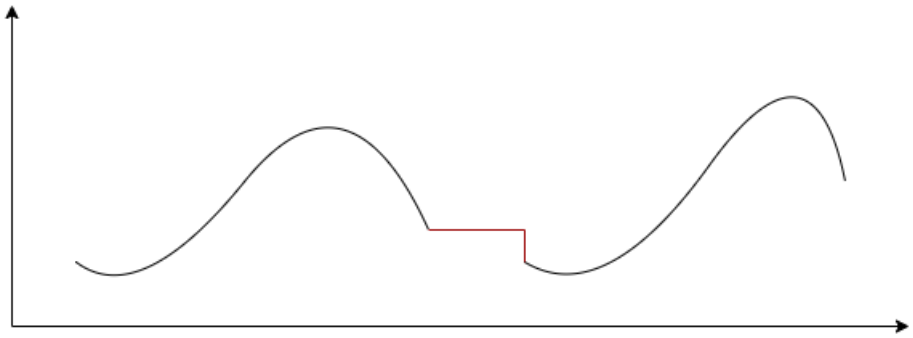


Рисунок 3.4 — Пример коллективной аномалии

Аномалии в данных АЗН-В могут быть выявлены как в режиме реального времени (поток данных), так и в режиме анализа исторических данных (архив). В зависимости от применяемого алгоритма результатом работы системы идентификации аномалий может быть либо метка экземпляра данных как аномального, либо оценка степени вероятности того, что экземпляр является аномальным.

Расчет аномалий производится по вычислению разницы между усредненными показателями за продолжительный период наблюдения и актуальными показателями в момент получения сообщений АЗН-В. При величине отклонения показателя от среднего значения более чем на 3 сигмы фиксируется аномалия и сообщение маркируется как подозрительное.

Поскольку конечной целью определения аномалий в трафике сообщений АЗН-В является выявление ложной информации о местоположении воздушных судов, необходимо, исходя из классов метрик подобрать наиболее эффективные модели обнаружения аномалий. Так вычисление общего количества сообщений не позволит сделать вывод о том, что конкретное сообщение является ложным - увеличение данного показателя в несколько раз может лишь косвенно доказывать наличие аномалии в целом, без выявления источника. Таким образом, в качестве аргумента функции параметра всегда должен быть уникальный идентификатор воздушного судна, поскольку именно данный параметр присутствует в каждом сообщении АЗН.

Существует множество различных способов детектирования аномалий, таких как статистические и модельные тесты, итерационные, метрические методы, однако учитывая возможность использования больших массивов данных, целесообразно использование классификационных методов машинного обучения совместно с простыми методами детектирования аномалий в результате чего вычислительные ресурсы системы будут использоваться эффективно. Для методов машинного обучения, параметры воздушного судна будут использоваться в качестве признаков при классификации данных - для отнесения их либо к ложным, либо к истинным данным. Поскольку необходимо определить истинность входных данных, а результат проверки является двоичным, в данной работе применена бинарная классификация.

Для осуществления поставленной задачи классификации, необходимо обладать достаточным набором данных, чтобы с заданной точностью определить истинность сообщения. Поскольку, согласно руководству по эксплуатации АЗН-В не существует обязательных требований по минимальной доступности системы, а согласно исследованиям <SAC2019> процент потерь пакетов зачастую превышает 50%, в данной работе будет произведен расчет точности выявления ложных сообщений с использованием массивов данных, варьирующихся от суточной выборки до недельной с добавлением случайных ложных сообщений,

сгенерированных согласно разработанной модели злоумышленника. В дальнейшем, полученные выводы станет возможным использовать при решении прикладной задачи выявления ложных сообщений и при проведении расчетов системы.

Существует несколько алгоритмов машинного обучения для осуществления бинарной классификации, среди которых Light GBM, логистическая регрессия, метод K-ближайших соседей, а также AdaBoost в сочетании с методом решающих деревьев. Данные методы были подробно описаны в предыдущей главе. В данной части работы произведено имитационное моделирование с использованием реальных сообщений АЗН-В воздушных судов и данных, полученных в результате работы модели злоумышленника. Машинное обучение производилось по следующим параметрам:

- координаты;
- расстояние от станции приема до ВС;
- высота ВС;
- синус угла пеленга ВС;
- косинус угла пеленга ВС;
- скорость, в т.ч. вертикальная;
- показатель уровня принимаемого сигнала;

Листинг 3.2

Пример исходных данных для расчета показателей


```
{
    "ts": "2020-09-19 00:00:01",
    "timestamp": "2020-09-18 23:59:58.923",
    "sensor": "rsp001",
    "hex": "155c13",
    "messages": 175,
    "rssi": -31.9,
    "seen": 3,
    "squawk": "null",
    "flight": "AFL1408 ",
    "category": "NA",
    "lon": 37.054222,
    "lat": 56.045403,
    "sin": 0.9256295,
    "cos": 0.37843108,
    "deg": 68,
    "altitude": 15575,
    "speed": 349,
    "vert_rate": 2688,
    "seen_pos": 14854,
    "nucp": 7,
    "track": 83
}
```


Для получения угла пеленга был произведен предварительный расчет на стороне приемного устройства - показатели "sin"(синус угла пеленга), "cos"(косинус угла пеленга) и "deg"(угол пеленга в градусах) формируются на основе координат приемного устройства и координат воздушного судна в сообщении АЗН-В. Затем сообщения передавались на удаленный сервер, где производилась их аггрегация. Всего за время анализа данных АЗН-В было собрано более 100 млн. сообщений АЗН-В.

## 3.2 Разработка архитектуры системы анализа и фильтрации сообщений автоматического зависимого наблюдения

Учитывая количество сообщений АЗН-В в единицу времени, а также необходимость в постоянном анализе поступающих данных, необходимо определить составляющие системы анализа и фильтрации сообщений АЗН-В, а также техническую реализацию частей разрабатываемой системы.

Исходя из логики работы системы, можно выделить следующие ключевые модули:

- модули приема и декодирования данных АЗН;
- модули синхронизации времени;
- модули определения момента прихода сигнала;
- модули формирования и отправки массива данных;
- модуль буферизации данных по каждому ВС;
- модуль вычисления местоположения разностно-временным методом;
- модуль записи и хранения данных;
- модуль сравнения данных вторичной радиолокации;
- модуль формирования и отправки верифицированных данных;
- модуль оповещения об угрозах безопасности;

Рисунок 3.5 — Облик системы анализа и фильтрации сообщений АЗН-В при использовании группы станций приема

В случае невозможности использования нескольких станций приема АЗН-В, либо в качестве дополнительного средства противодействия несанкционированному вмешательству, ключевые компоненты системы могут быть представлены следующими модулями:

- модули приема и декодирования данных АЗН;
- модули формирования и отправки массива данных;
- модуль буферизации данных по каждому ВС;
- модуль анализа данных с использованием методов машинного обучения;

– модуль записи и хранения данных;
– модуль сравнения данных вторичной радиолокации;
– модуль формирования и отправки верифицированных данных;
– модуль оповещения об угрозах безопасности;

Рисунок 3.6 — Облик системы анализа и фильтрации сообщений АЗН-В при использовании одной станции приема

Исходя из рисунков 3.5 и 3.6 систему можно рассматривать исходя из 3-х её составляющих, а именно: сбора, анализа и хранения информации. Для создания системы необходимо учитывать частоту прихода данных АЗН-В, количество воздушных судов в зоне действия системы, условия по доставке данных в АС УВД.

Рассмотрим более подробно систему сбора данных АЗН и варианты ее технической реализации. На данный момент существует достаточно большое количество программных декодеров сигнала Mode S, при этом, наиболее часто встречающимся в научных исследованиях протокола 1090 ES является декодер dump1090 [33] распространяемый под лицензией BSD, допускающей коммерческое использование. Примечательно, что декодирование сообщения Mode S с пакетами данных АЗН-В не является ресурсозатратной задачей при использовании dump1090 - так в работе [21] декодирование сигналов производится средствами одноплатного компьютера компактного форм-фактора Raspberry Pi. dump1090 обладает следующими возможностями, позволяющими использовать данного ПО в части сбора данных АЗН:

– надежное декодирование сообщений при слабом сигнале;
– поддержка потокового вывода декодированных сообщений по протоколу TCP в рамках установленной сессии;
– коррекция одиночных битовых ошибок с использованием 24-битного CRC;
– возможность декодирования сообщений DF11, DF17.

Для определения момента времени прихода сигнала, предполагается использовать метод, предложенный [27], при котором вычисляется время прихо-

да первого бита данных, декодированного при частоте дискретизации 2,4 МГц. При этом локальное время на приемном устройстве задается согласно подходу использования единого времени ГНСС. После вычисления времени прихода сигнала производится добавление соответствующей метки времени для каждого из декодированных сообщений АЗН. Массивы данных отправляются на вычислительный сервер в рамках установленного TCP-соединения.

В приложении Б описаны основные части кода по определению точного времени прихода и добавлении метки времени в пакет данных.

Для обработки данных на вычислительном сервере могут быть использованы специализированные вычислительные кластеры, позволяющие обрабатывать большие массивы данных в реальном времени. При этом необходимо учитывать возможность распределения нагрузки между кластерами в случае увеличения потока данных АЗН. Для этих целей необходимо использовать ПО, выполняющее функцию брокера сообщений, а также ПО, обеспечивающее равномерное распределение нагрузки и реплицирование потоков между вычислительными центрами. На современном этапе развития технологий функцию брокера выполняют такие прикладные системы как Rabbit MQ и Apache Kafka. Последняя позволяет не только принимать данные, но и выступать в роли буфера сообщений, которые затем могут быть запрошены другими вычислительными системами. Если сравнивать эти системы, то можно утверждать, что Rabbit MQ позволяет более комплексно распределять и доставлять потоки данных между потребителями, а Kafka ориентированна на быстрое предоставление данных как потребителям, производящим вычисления в реальном времени, так и потребителям, нуждающимся в агрегированном массиве информации. В качестве вычислителя местоположения могут быть также использованы системы обработки данных в реальном времени, такие как Apache Storm или Apache Spark. Преимущества данных систем состоит в том, что математические вычисления происходят непосредственно в оперативной памяти, в то время как использование таких систем как Apache Hadoop и применение в них модели MapReduce вынуждает использовать дисковую подсистему для работы с массивами данных.

Также необходимо свести задержки на обработку сигналов к минимуму, насколько это возможно. Для этой цели необходимо производить все вычисления без необходимости обращения к микросервису хранения, оперируя данными

исключительно в рамках буферов памяти, либо в рамках БД расположенной непосредственно в оперативной памяти.

В качестве подсистемы хранения предлагается использовать БД Clickhouse, используемую компанией Яндекс для обработки поисковых запросов. Отличительной особенностью данной системы является тот факт, что Clickhouse - столбцовая СУБД с физической сортировкой данных по первичному ключу. Итак, перечислим основныедостоинства данной СУБД:

- столбцовая СУБД;
- сжатие данных;
- хранение данных на диске;
- параллельная обработка запроса на многих процессорных ядрах;
- распределённая обработка запроса на многих серверах;
- поддержка SQL;
- обработка данных по векторам;
- обновление данных в реальном времени;
- наличие индексов;
- встроенный REST API;
- поддержка приближённых вычислений;
- репликация данных, поддержка целостности данных на репликах.

Таким образом, предложены необходимые технические системы для эффективной работы системы анализа и фильтрации. С точки зрения архитектуры, система представлена как распределенная ИТ-система, где каждый из модулей является микросервисом, то есть выполняет закрепленную за ним роль. Учитывая тенденции к увеличению ИВД, модульная архитектура позволяет наращивать объемы вычислительной мощности и устройств хранения за счет добавления аналогичных микросервисов. Поскольку операции над аэронавигационными данными являются критичными с точки зрения информационной инфраструктуры, необходимо производить резервирование всех основных узлов системы и при отказе обеспечивать непрерывную работу. Данному вопросу посвящена следующая часть работы.

## 3.3 Исследование мер по резервированию системы анализа и фильтрации сообщений АЗН-В

Рассмотрим более подробно процесс прохождения данных через разрабатываемую систему, при этом учтем необходимость в резервировании ключевых модулей.

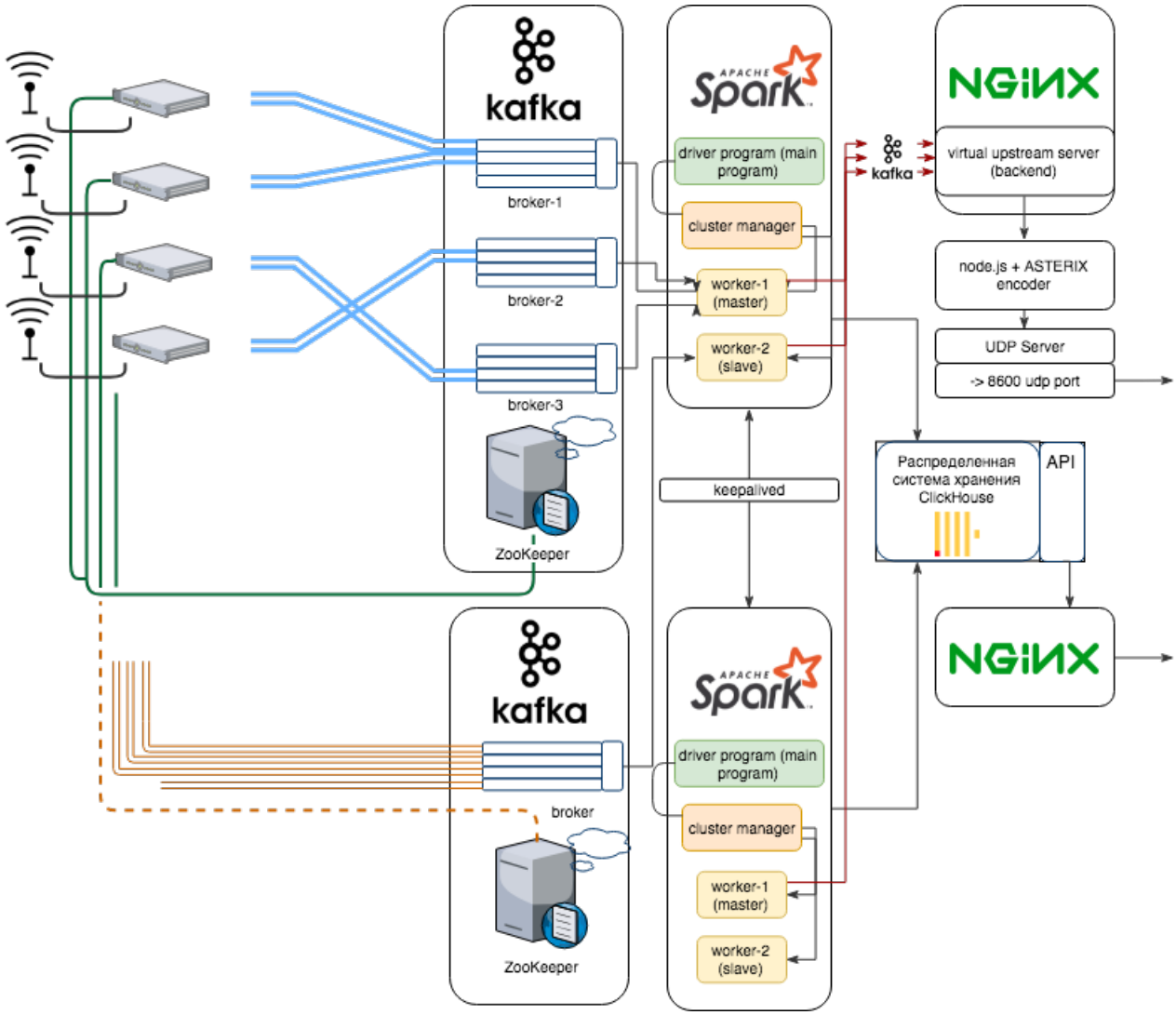



Рисунок 3.7 — Схема прохождения информационных потоков через ключевые микросервисы системы

Поскольку обработка данных АЗН-В должна происходить с минимальными задержками по времени и снижением возможных рисков по доставке сообщений, необходимо произвести доработки на каждом из уровней системы. В разрабатываемой архитектуре системы передача данных АЗН-В осуществляется путем установки TCP-сессии между приемной станцией и уровнем приема

сообщений. На данном уровне, одним из таких решений по оптимизации может быть использование протокола WebSocket. Протокол обеспечивает полнодуплексную связь поверх TCP [67], с однократным установлением соединения между клиентом (в данном случае устройством приема данных АЗН-В) и сервером (распределенным брокером сообщений). Разработанный для приложений, требующих минимальные задержки по времени, он позволит осуществлять гарантированную доставку сообщений без необходимости в использовании избыточных данных как в HTTP. Для снижения нагрузки на конечный слой необходимо производить кэширование объектов, запрашиваемых по HTTP. Таким образом необходимо использовать дополнительный проксирующий слой между клиентом и данной системой. Основой данного слоя может выступать кластер из веб-серверов nginx в режиме работы reverse-proxy. Балансировка между серверами может быть решена на уровне DNS (выдача A-записи наиболее ближайшего сервера), либо с использованием балансировщика запросов (переадресация на ближайший и менее нагруженный сервер). Также немаловажным моментом является вопрос легитимности самого приемника АЗН-В, с которого поступают данные в систему обработки. Для данных целей возможно использование механизма асинхронного шифрования (каждый приемник должен иметь открытый сертификат для проверки подлинности).

# Глава 4. Апробация системы анализа и фильтрации сообщений автоматического зависимого наблюдения

Современные АС УВД представляют собой информационные системы обработки данных, построенных по микросервисной архитекуре (MSA). Микросевисная архитектура - термин, описывающий архитектуру ИТ-систем, устройство которой заключается в использовании логических блоков, имеющих строго определенную минимальную функцию в рамках целой системы. Преимущество такого подхода заключается в том, что данные логические блоки могут быть заменены на аналогичные, отказ может быть быстро продиагностирован и каждый из блоков может быть многократно резервирован, исключая отказ системы в целом. Учитывая, что современные АС УВД, таких производителей как Альфа, НИТА, ВНИиРА и другие имеют схожую структуру и взаимодействие между логическими блоками производится с использованием клиент-серверной архитектуры, использование алгоритмов валидации возможно в виде промежуточного звена между получением данных и выводом этих данных на интерфейс диспетчерского пульта. Более того, частично данный функционал реализован - например в многопозиционной системе "Мера производителя ВНИИРА. Одной из целей данной системы является повышение достоверности данных. Предлагаемый подход в данной работе направлен на обеспечение максимально возможной точности определения истинного положения ВС - существует большое количество математических методов, которые могут быть применены, и у каждого из которых есть свои достоинства и недостатки. Использование оптимального метода для заданной конфигурации положения приемных станций, уровня шума и предполагаемого местоположения ВС и фильтрация ложных сообщений является основной задачей данного логического блока. Входные данные для блока валидации:

- данные о времени прихода сигнала АЗН-В;
- идентификатор ВС;
- текущий состав и координаты сети приемных устройств многопозиционной системы;
- данные о величине средней ошибки определения времени прихода сигналов для каждого из приемника;

– данные о сообщаемом местоположении;
– информация о барометрической высоте;

Выходные данные блока валидации:

– скорректированное местоположение ВС;
– идентификатор ВС;
– величина отклонения рассчитанного местоположения ВС от сообщаемого;
– флаг достоверности сообщения (правда/ложь);
– используемый метод расчета местоположения;

Поскольку для определения оптимального метода необходима выборка данных, предполагается проведение расчета точности каждого из методов при разном наборе входных данных методом Монте-Карло. Получение необходимой выборки невозможно в реальных условиях по причинам того, что реальные данные могут содержать ложные сообщения АЗН-В. На основе выборки станет возможным проведение анализа данных с использованием методов машинного обучения. Таким образом, помимо функции определения местоположения ВС, необходима функция выбора оптимального алгоритма определения цели.

Также, помимо определения истинного местоположения, возможно включение дополнительных проверок с использованием исторической информации. Таким образом можно будет сузить количество одновременно проверяемых воздушных судов до множества тех, которые вызывают подозрения. Для реализации поставленных задач необходимо произвести моделирование с использованием реальных исторических данных АЗН-В.

## 4.1 Моделирование угроз несанкционированного вмешательства на систему автоматического зависимого наблюдения

Представляя среду взаимодействия АЗН-В как информационную систему с распределенной архитектурой, опишем базовые составляющие, необходимые для моделирования.

Сеть передачи данных АЗН-В может быть представлена как N передающих и M принимающих устройств. Радиобмен между участниками информационного взаимодействия осуществляется в рамках дискретного времени, таким образом в единицу времени может быть доступно от 0 до n сообщений АЗН-В. Реальный процесс радиобмена может быть смоделирован путем записи сообщений АЗН-В с учетом относительного от начала наблюдения времени прихода сообщений. Сообщения должны быть записаны одновременно более чем тремя приемниками, синхронизированными по времени. Для моделирования несанкционированного воздействия необходимо произвести внедрение ложных сообщений в случайные моменты времени на заранее записанный и воспроизведенный радиоэфир. Диаграмма процесса моделирования представлена на рисунке 4.1

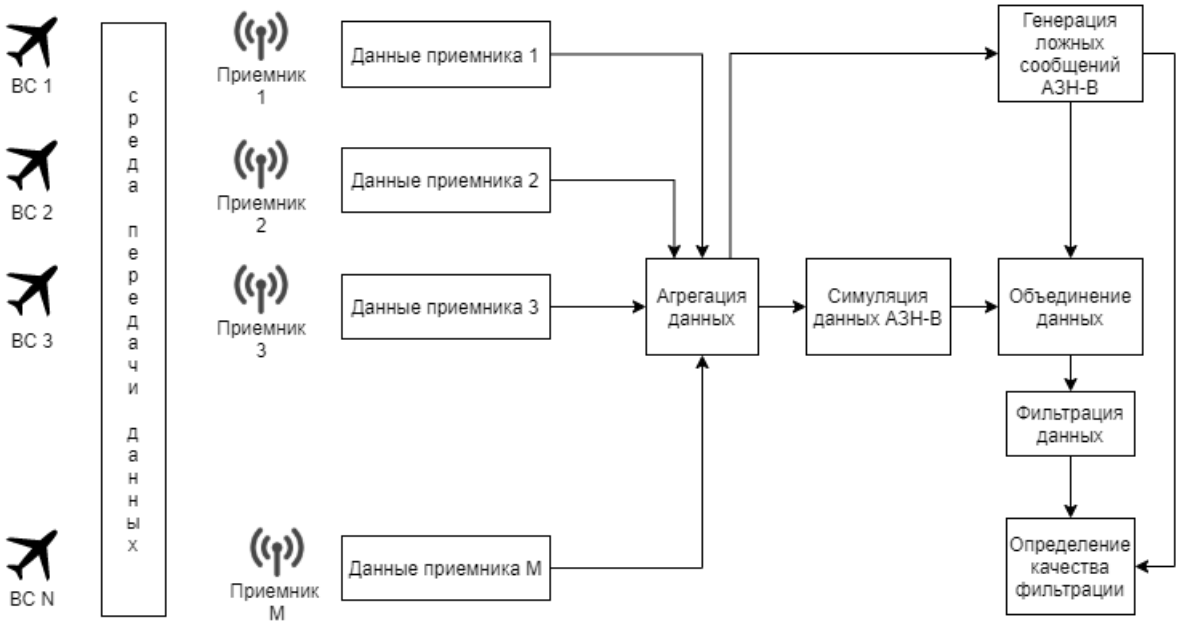



Рисунок 4.1 — Моделирование несанкционированного вмешательства с использованием реальных полетных данных

Моделирование может быть выполнено как на основе реальных данных, так и на основе сгенерированных сообщений АЗН-В, которые будут принимать-

ся за достоверные при проведении симуляции. Для определения качества алгоритмов определения положения воздушного судна предпочтителен первый вариант моделирования, а для проверки работы алгоритмов - второй. Перейдем к рассмотрению каждого из типов моделирования.

Опишем подробно процесс получения полетных данных. В данной работе реальные данные были получены с помощью программно-определяемых радиоприемников (SDR, Software Defined Radio), использующих чип RTL2838 для демодуляции сигнала АЗН-В. Это микросхема, содержащая два 8-битных АЦП с частотой дискретизации до 3,2 МГц (однако выше 2,8 МГц могут быть потери данных), и интерфейс USB для связи с компьютером. Эта микросхема на входе принимает I- и Q-потоки, которые должны быть получены другой микросхемой. В качестве обработки IQ потоков в устройстве приема был использован чип R820T - он представляет собой усилитель антенны, перестраиваемый фильтр и квадратурный демодулятор с синтезатором частоты. R820T работает в диапазоне 24–1766 МГц, который позволяет производить прием на частоте вещания АЗН-В (1090 МГц).

В качестве устройства обработки сигналов АЗН-В и преобразования сообщений из восьмеричного формата был использован одноплатный компьютер Raspberry Pi Model 3 с установленным программным обеспечением rtl-sdr и dump1090. С помощью программы rtl-sdr была произведена запись радиоэфира на частоте 1090 МГц за полчаса наблюдений. Запись производилась одновременно на трех географически удаленных друг от друга приемных устройств. Схема приема данных АЗН-В, использующаяся для моделирования в данной работе приведена на рисунке 4.2

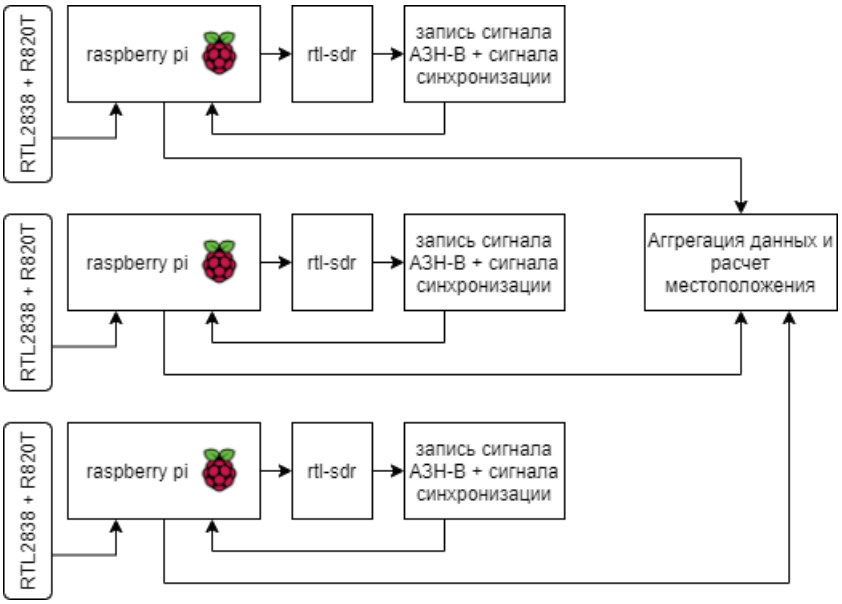



Рисунок 4.2 — Блок-схема сбора реальных полетных данных АЗН-В

Также помимо записи на частоте 1090 МГц производилась запись на частоте 97.6 МГц для осуществления синхронизации приемных устройств.

Далее полученные данные обрабатывались в программном комплексе Matlab - производилась оценка местоположения излучения сигналов и сравнение расчетного местоположения с местоположением ВС согласно сообщениям АЗН-В. Реальные данные показали незначительные отклонения от переданных.

Помимо записи сигналов АЗН-В для последующего воспроизведения производилось декодирование сообщений и сохранение полетных данных с указанием времени прихода сигнала с точностью до наносекунды.

Информация по декодировке данных АЗН-В доступна в общем доступе. Так, для декодирования номера рейса (Callsign) необходимо использовать таблицу символов для протокола Mode-S - после преобразования шестнадцатеричного кода поля данных в двоичный код, разбиения двоичной последовательности на группы по 6 битов и преобразования в десятичную систему, будут получены порядковые номера, каждому из которых будет соответствовать символ. Пример получения номера рейса представлен ниже:

Листинг 4.1

Пример декодирования ID рейса

```
ADS-B Message:
8D4840D6202CC371C32CE0576098
Message structure:
DF... CA. ICAO.. DATA..................... PI....
HEX: 8 D 4840D6 2 0 2CC371C32CE0 576098
BIN: 10001 101 ****** 00100 000 ************ ******
DEC: 17 5 4 0
TC *
Data conversion:
HEX: 20 2CC371C32CE0
BIN: 00100000 | 001011 001100 001101 110001 110000 110010 110011 100000
DEC: | 11 12 13 49 48 50 51 32
LTR: | K L M 1 0 2 3 _
```

Таким образом, прием и преобразование сообщений АЗН-В не представляет трудности - в приведенном примере из сообщения "8D4840D6202CC371C32CE0576098"был получен код рейса KLM1023. Данный процесс автоматизирован в программном обеспечении dump1090 - имеется возможность передачи декодированных данных в потоковом режиме в формате SBS-1.

Листинг 4.2

Пример декодированных данных АЗН-В

```
MSG,6,1,1,42437A,1,2020/02/20,20:31:31.17569187,
    ↪ 2020/02/20,20:31:31.32254189,,,,,,,2754,0,0,0,
MSG,3,1,1,42437A,1,2020/02/20,20:31:31.77597773,
    ↪ 2020/02/20,20:31:31.138098487,,27725,,,55.04915,37.61428,,,,,0
MSG,5,1,1,42437A,1,2020/02/20,20:31:31.134797534,
    ↪ 2020/02/20,20:31:31.191857973,,27725,,,,,,0,,0,
MSG,6,1,1,42437A,1,2020/02/20,20:31:31.135797784,
    ↪ 2020/02/20,20:31:31.193993790,,,,,,,2754,0,0,0,
MSG,4,1,1,42437A,1,2020/02/20,20:31:31.137638784,
    ↪ 2020/02/20,20:31:31.197201110,,,422,153,,,1536,,,,,0
```

Полученные декодированные данные были использованы в дальнейшем для выявления факта несанкционированного вмешательства и фильтрации нелегитимных сообщений.

Современные широкополосные программно-контролируемые радиопередатчики (SDR) позволяют передавать заранее сформированный сигнал, представленный в комплексной (квадратурной) форме в широком диапазоне частот (от 1 МГц до 6 ГГц). Современные реалии таковы, что данные устройства широко представлены на рынке и их возможности позволяют формировать и передавать сигналы на частоте вещания АЗН-В со всеми необходимыми характеристиками.

Моделирование несанкционированного вмешательства было произведено исходя из сценария создания ложных сообщений АЗН-В и передачи их в эфир таким образом, что при получении сообщений АЗН будут доступны как сообщения от реальных воздушных судов, так и сообщения от злоумышленника.

В качестве передающего устройства, при выполнении натурного эксперимента был использован программно-контролируемый радиопередатчик HackRF One. Комплексные сигналы с ложной информацией о коде ИКАО ВС, номере рейса, высоте полета, скорости (в том числе вертикальной), курсе и координатах были заранее сгенерированы на ПК, к которому был подключен радиопередатчик. Полезная информация в сигналах была записана с учетом траектории движения несуществующего ВС. При передачи данных в радиоэфир мощность излучения была снижена до 5мВТ с целью предотвращения влияния на реальный радиообмен по протоколу 1090ES. Процесс моделирования представлен на рисунке 4.3

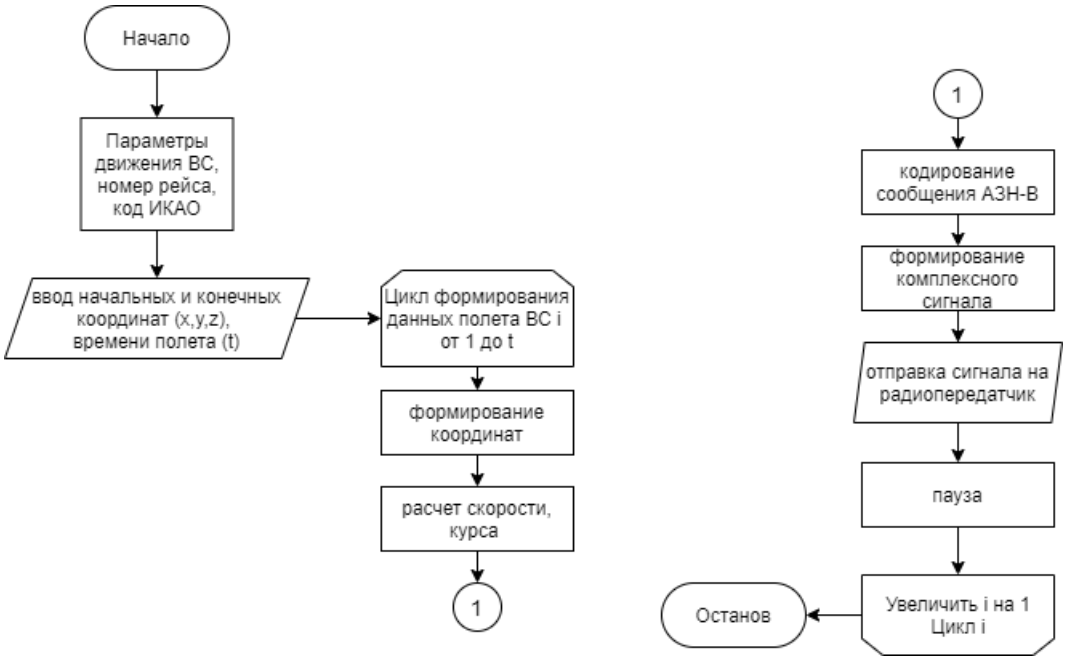



Рисунок 4.3 — Алгоритм проведения спуфинг-атаки

В качестве приемных устройств при постановке данного эксперимента были использованы радиолюбительские приемники построенные на схемотехнической базы R820T + RTL2838. Для подтверждения возможности проведения атаки и демонстрации влияния несанкционированного вмешательства на работу наземных служб была произведена учебная атака в лабораторных условиях - передающим устройством генерировался последовательность сигналов имитирующих реальный сигнал от движущегося воздушного судна, а приемным устройством производилось сканирование радиоэфира таким образом, что были доступны как сообщения от реальных ВС, так и ложные сообщения. Рассмотрим схему проведения эксперимента 4.4 и полученные результаты.

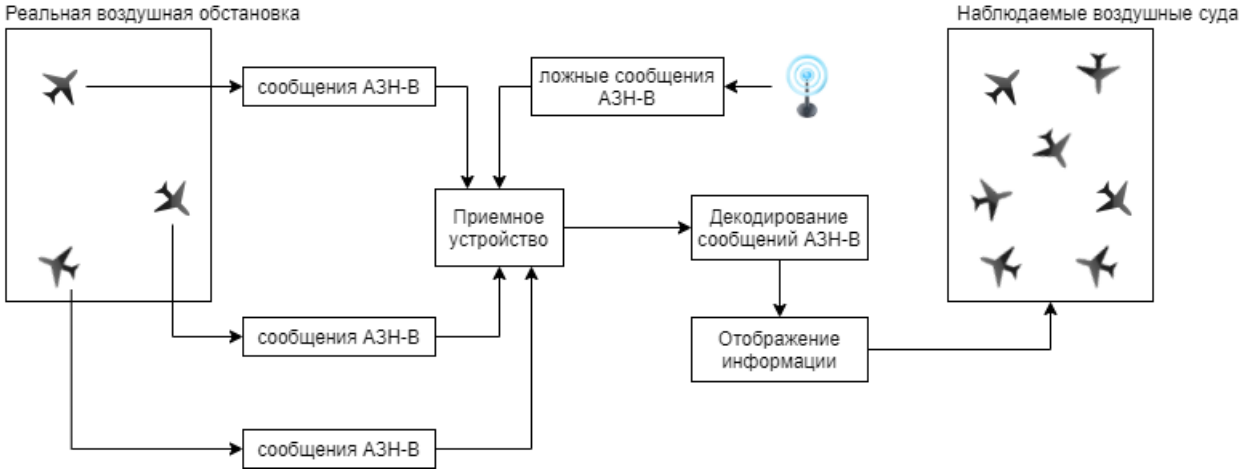
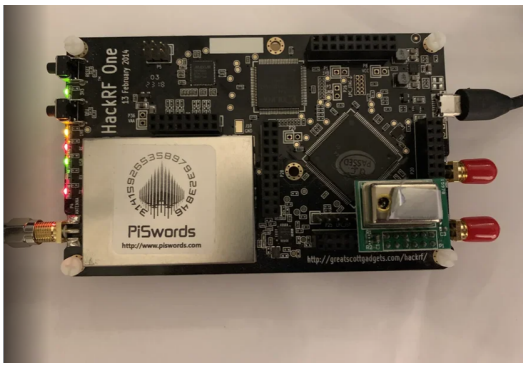



Рисунок 4.4 — Схема постановки эксперимента

Оборудование генерации и приема сообщений АЗН-В показаны на рисунке 4.5. Для передачи использовалась программно-определяемая радиосистема (SDR) HackRF One, управляемая через USB-интерфейс. В качестве приемного устройства использовался одноплатный компьютер Raspberry Pi 3B+, с подключенным к нему "донглом SDR, работающей в диапазоне частот АЗН-В и имеющей необходимые показатели частоты дискретизации.

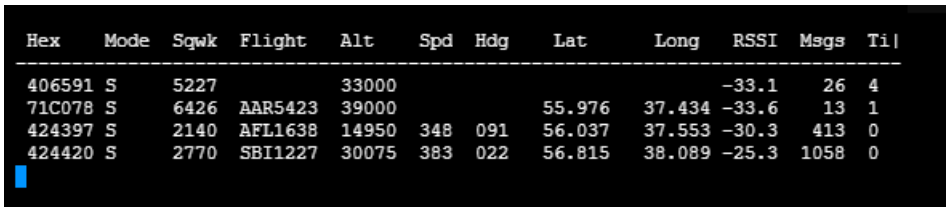



а) Оборудование для передачи сообщений АЗН-В

б) Оборудование для приема сообщений АЗН-В

Рисунок 4.5 — Техническая база для проведения эксперимента

Приведем скриншот из программы-декодера сообщений АЗН-В dump1090. На момент создания скриншота, несанкционированное воздействие не проводилось.



| Hex | Mode | Sqwk | Flight | Alt | Spd | Hdg | Lat | Long | RSSI | Msgs | Ti\| |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 406591 | S | 5227 | | 33000 | | | | | -33.1 | 26 | 4 |
| 71C078 | S | 6426 | AAR5423 | 39000 | | | 55.976 | 37.434 | -33.6 | 13 | 1 |
| 424397 | S | 2140 | AFL1638 | 14950 | 348 | 091 | 56.037 | 37.553 | -30.3 | 413 | 0 |
| 424420 | S | 2770 | SBI1227 | 30075 | 383 | 022 | 56.815 | 38.089 | -25.3 | 1058 | 0 |

Рисунок 4.6 — Вывод программы декодирования сообщений АЗН-В dump1090 - без несанкционированного вмешательства

Далее была произведена атака - с учетом модели движения ВС, было произведено автоматическое формирование параметров сообщения, IQ-сигнал был записан в файл и передан на интерфейс HackRf One, мощность сигнала корректировалась исходя из передаваемых координат. В качестве названия рейса использовался несуществующий - "BADF100". Работа программы представлена на рисунке 4.7.

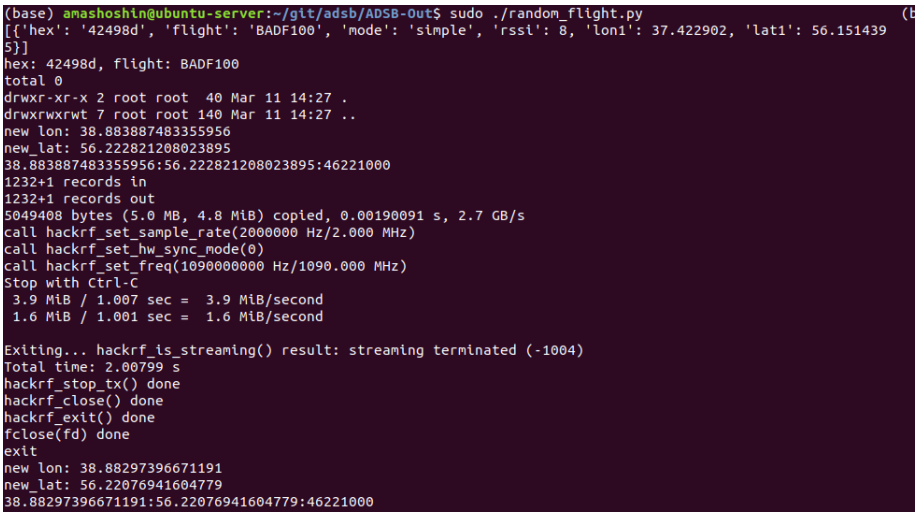



Рисунок 4.7 — Вывод программы формирования ложных сообщений АЗН-В

Через несколько секунд, данные отобразились на интерфейсе приема сообщений АЗН-В. Результат атаки представлен на рисунке 4.8

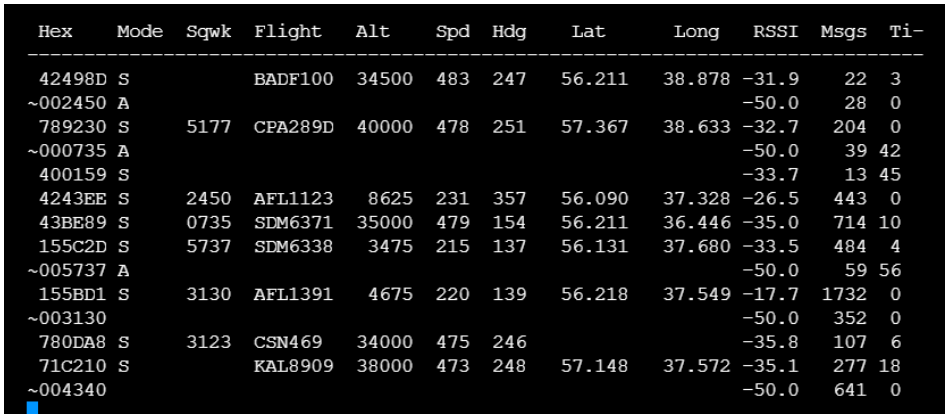



Рисунок 4.8 — Вывод программы декодирования сообщений АЗН-В dump1090 - несанкционированное вмешательство

Поскольку физически невозможно обеспечить низкую мощность ложного сигнала и его прием географически разнесенной группировкой приемных устройств, полноценное моделирование производилось для системы, состоящей только из одного приемника. В качестве результатов работы гиперболических методов примем результаты имитационного моделирования, представленных во второй главе. Далее будут представлены результаты полунатурного эксперимента по фильтрации сообщений АЗН-В с использованием методов машинного обучения.

## 4.2 Результаты работы системы анализа и фильтрации сообщений системы автоматического зависимого наблюдения

Несанкционированное вмешательство в систему АЗН-В может быть произведено с использованием различных подходов по генерации ложных сообщений АЗН-В. Наиболее доступным из них, с точки зрения ресурсозатрат на подготовку, является метод генерации, заключенный в создании сообщений со случайным ИКАО адресом, местоположением и прочими параметрами. Такой подход является самым простым в задаче проведения несанкционированного вмешательства и интуитивно понятно, что атака с таким методом создания сообщений легко может быть обнаружена статистическими методами анализа, такими как:

- пороговый анализ;
- метод среднеквадратичных отклонений;
- анализ распределений интенсивности передачи/приема пакетов;
- цепи Маркова;
- метод хи-квадрат;

Однако, помимо простой атаки несанкционированного вмешательства с использованием случайных параметров, может быть произведена атака, учитывающая модель движения воздушного судна, эшелонирование, реальные ИКАО коды ВС, типовые маршруты, схемы заходов на посадку и так далее. В этом случае простые статистические методы не позволят корректно классифицировать сообщение АЗН-В. При наличии информации о координатах приемной станции, может быть произведена регулировка мощности для каждого сообщения - так при генерации сообщения, через координаты мнимого воздушного судна и реальных координат станции приема АЗН-В может быть рассчитана дальность, и как следствие может быть произведена аттенюация мощности передачи. Предполагая потенциальную возможность успешного использования данного метода, а также наличие научного интереса, была произведена его проработка и поставлен натурный эксперимент отражения атаки. В качестве методов отражения были использованы методы машинного обучения - градиентный и адаптивный бустинг, метод К-ближайших соседей.

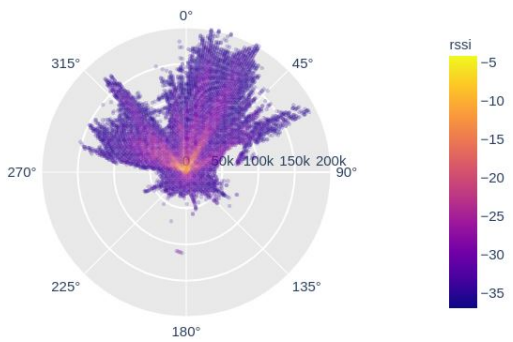
В данной части будет рассмотрена ситуация обнаружения и отражения угрозы несанкционированного вмешательства при наличии только одного приемного устройства. Таким образом возможно применение только метода монолатерации. В качестве основы фильтрационных алгоритмов были взяты методы машинного обучения. Для нескольких приемных устройств, описанные принципы валидации будут аналогичными, за исключением того, что необходимо учитывать дополнительный признак - идентификатор станции приема сообщения.

Для генерации ложных сообщений был разработан следующий алгоритм:

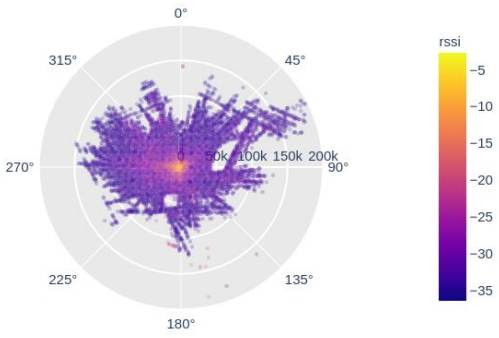
1. Указание граничных координат для генерации ложных сообщений, с координатами ВС внутри заданной зоны атаки
2. Ввод файла с указанием перечня ИКАО-кодов воздушных судов, наблюдавшихся в заданной зоне атаки за последний месяц
3. Выбор случайного числа для определения этапа полета (взлет, набор высоты, выход на опорные пункты маршрута, снижение, заход на посадку)
4. Выбор случайного числа для определения категории воздушного судна (региональный, транспортный, местных авиалиний, специального назначения)
5. Выбор случайных чисел для определения начальных координат, курса
6. Определение скорости, высоты, вертикального ускорения исходя из выбранной категории воздушного судна и этапа полета
7. Определение пройденного расстояния за единицу времени, исходя из скорости, начальных координат и курса
8. Определение координат для генерации следующего сообщения, исходя из рассчитанного пройденного расстояния и начальных координат
9. Генерация пакета с помощью программного обеспечения ADSB_Encoder.py. В качестве аргументов данного скрипта используется:
   - код ИКАО ложного ВС в восьмеричном формате
   - широта и долгота ложного ВС
   - высота полета ложного ВС
   - номер рейса ложного ВС
   - выходной файл для записи сгенерированного сигнала в квадратурном представлении

10. Отправка сгенерированного сигнала с помощью интерфейса программно управляемой радиосистемы (SDR) HackRF One (hackrf_transfer). При этом указываются:
    - файл ложного сигнала
    - несущая частота (1090 МГц)
    - частота дискретизации (10 МГц)
    - мощность передачи сигнала (случайная/в зависимости от расстояния до атакуемой станции приема)

Помимо генерации ложных сообщений, необходимо обладать информацией о движении реальных воздушных судов в пространстве, на которое нацелена атака. Для данной цели были использованы 2 одноплатных компьютера Raspberry PI, расположенных в разных окружениях - на открытом воздухе и внутри помещения. Всего за время проведения натурного эксперимента было собрано 20.1 млн сообщений АЗН-В (период 2020.11.05 - 2021.11.28) при осенних погодных условиях и 20.5 млн сообщений АЗН-В (период 2021.01.04 - 2021.01.24) при зимних погодных условиях. В данные периоды оба приемных устройства собирали информацию одновременно, что в последствии позволило организовать более сложную атаку повторения реальных данных АЗН-В. Рассмотрим полярные диаграммы 4.9, 4.10 приема сигналов системы АЗН-В для каждого из приемных устройств, для каждого из периода наблюдений.



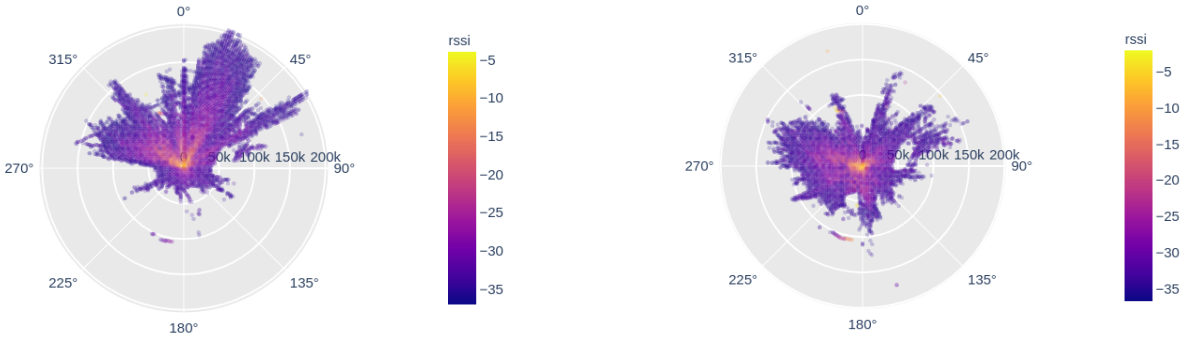

а) Внутри помещения




б) Вне помещения

Рисунок 4.9 — Диаграммы уровня принимаемого сигнала для приемных устройств, размещенных в различных условиях. Период наблюдений - 2020.11.05 - 2021.11.28

При построении полярных диаграмм использовалось расстояние до воздушного судна, пеленг и показатель уровня принимаемого сигнала. Пеленг рассчитывался исходя из координат воздушного судна, заключенных в сообщении




а) Внутри помещения б) Вне помещения

Рисунок 4.10 — Диаграммы уровня принимаемого сигнала для приемных устройств, размещенных в различных условиях. Период наблюдений - 2021.01.04 - 2021.01.24

АЗН-В, далее он будет именоваться как "виртуальный пеленг". Из полученных графиков становится понятно, что существуют зоны воздушного пространства, по которым нет информации по причине наличия физических преград распространения сигнала, либо отсутствия полетов (запретные для полета зоны). Также очевидно влияние погодных условий на прием сигнала вне помещения - слой снега, полностью закрывший штыревую антенну, ухудшил прием сигналов. Диаграммы представлены для отображения неравномерности уровня сигнала в зоне обзора воздушного пространства, и знаниями об этой неравномерности (или полного отсутствия) сигнала не обладает злоумышленник. Уровень принимаемого сигнала, виртуальный пеленг, координаты воздушного судна, воздушная скорость горизонтального полета, вертикальная скорость, высота полета - это признаки для каждого сообщения, по которым в данной работе производилась бинарная классификация сообщений на истинные и ложные методами машинного обучения. Помимо перечисленных признаков, также могут использоваться - порядковый номер станции приема, погодные условия, наличие вспышек на солнце и прочие.

Рассмотрим результаты натурного эксперимента [53] при моделировании угрозы несанкционированного вмешательства путем генерации ложных сообщений АЗН-В. За основу был взят период наблюдений 13.10.2020 - 14.10.2020. Использовались методы градиентного и адаптивного бустинга, метод K-ближайших соседей, а также наивный байесовский классификатор.

Результаты при искусственной генерации сообщения представлены в таблице 4.1

Таблица 4.1

Сравнение точности методов машинного обучения в задаче бинарной классификации сообщений АЗН-В

| Метод | Ошибка I рода | Ошибка II рода | Точность, % |
|---|---|---|---|
| Метод K-ближайших соседей | 4/856 | 9/17988 | 99.93 |
| Градиентный бустинг | 3/857 | 8/17989 | 99.94 |
| Адаптивный бустинг | 8/852 | 12/17985 | 99.89 |
| Наивный байесовский классификатор | 858/2 | 1/17996 | 95.44 |

При проведении обучения и работы метода была произведена оценка важности каждого из признаков, результаты представлены на рисунке 4.11

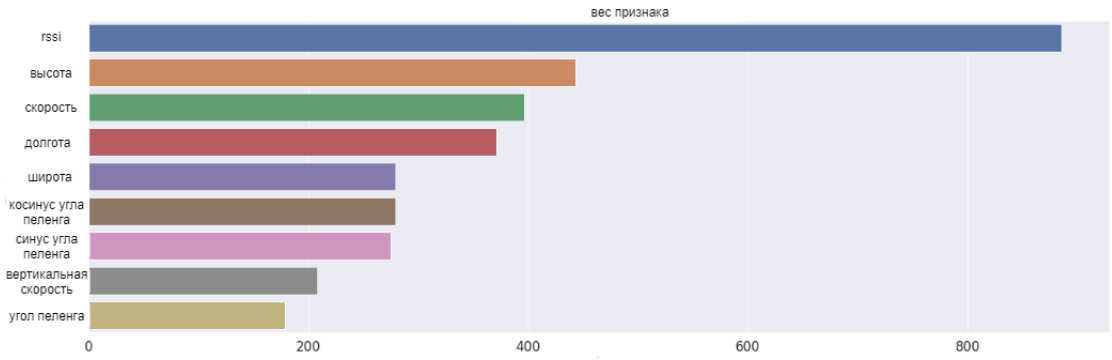



Рисунок 4.11 — Вклад признаков при классификации сообщений АЗН-В

Исходя из полученных результатов, можно судить об успешности методов K-ближайших соседей и градиентного бустинга в случае искусственной генерации сообщения. Оценим эффективность системы анализа и фильтрации для модели, в рамках которой злоумышленник может полностью повторить полученный сигнал. Для достижения всех необходимых условий, взамен генерации сообщений производилось "подмешивание"сообщений, полученных с приемной станции вне помещения. Схема моделирования представлена на диаграмме 4.12

Рисунок 4.12 — Реализация угрозы несанкционированного вмешательства путем повторения сигналов АЗН-В

Для исключения погрешностей при формировании сигнала (неточность испускаемой мощности), вместо аттенюации сигнала, его отправки и дальнейшего приема, сообщения АЗН-В от приемника вне помещения аддитивно добавлялись к сообщениям, полученным приемником внутри помещения. При проведении классификации не учитывалось название приемной станции, а следовательно, единственным признаком, по которому методы машинного обучения могли обнаружить ложные сообщения был уровень принимаемого сигнала. Все остальные признаки являлись истинными - поскольку принадлежали реально существующему ВС, и лишь в связке с уровнем сигнала, такие повторно высланные сообщения могли быть обнаружены. Для тестирования использовались данные за период с 11 по 12 ноября. При этом количество ложных сообщений (дублированных) примерно равно количеству легитимных сообщений.

Результаты при повторении реальных сообщений представлены в таблице 4.2

Таким образом, даже при идеальных условиях проведения угрозы несанкционированного вмешательства и наличии только одной активной станции приема, эффективность отражения такой атаки составляет 91%. В случае же генерации сообщений, а не их дублирования, практически отсутствует риск возникновения ошибок первого и второго рода. Расчеты точности были произведены для определения истинности уникальных сообщений. В реальной ситуации, решение об истинности сообщений с одинаковым идентификатором воздушного судна может быть принято на основе нескольких проанализированных сообщений - это позволит минимизировать риск некорректной оценки истинности

Таблица 4.2

Сравнение точности методов машинного обучения в задаче бинарной классификации сообщений АЗН-В. Несанкционированное вмешательство: повторение сигналов

| Метод | Ошибка I рода | Ошибка II рода | Точность, % |
|---|---|---|---|
| Метод K-ближайших соседей | 1636/15526 | 1449/18346 | 91.65 |
| Градиентный бустинг | 2557/14605 | 2780/17015 | 85.56 |
| Адаптивный бустинг | 3488/13674 | 3324/16471 | 81.56 |
| Наивный байесовский классификатор | 17133/29 | 0/17795 | 53.64 |

сообщений от воздушного судна. Также необходимо указать на то, что теоретически, при осуществлении атаки с возможностью перебора всех сочетаний признаков, система, состоящая из одной активной станции приема не сможет корректно классифицировать сообщение. Однако, практически осуществить данную атаку невозможно - даже если при осуществлении атаки с использованием реальных полетных данных удастся подобрать уровень сигнала, то без наличия обратной связи от АС УВД, маловероятно безошибочно подобрать значение данного признака для последующих сообщений. Побочной стороной данного метода является компрометирование реальных воздушных судов - так, при нескольких неудачных попытках осуществления угрозы несанкционированного воздействия, все сообщения от ВС, параметры которых ранее были расценены как ложные, на установленное время будут помечены как некорректные. При последующих поступлениях на систему анализа заданного количества сообщений от ВС с корректными параметрами, сообщения вновь будут отображаться в системе как корректные. Частичным решением этой проблемы может стать определение коридора в рамках которого сообщения будут считаться истинными, но более предпочтительным вариантом решения проблемы будет использование дополнительного признака, например информации о параметрах приема сигнала с помощью антенны, обладающей иными характеристиками. В конфи-

гурации системы анализа и фильтрации, состоящей из более чем трех приемных станций, показатели эффективности фильтрации непосредственно связаны с точностью определения местоположения судна. Поскольку поставить натурный эксперимент несанкционированного воздействия на систему в данном варианте не представляется возможным, в качестве результатов приведем полученные показатели точности, полученные в результате имитационного моделирования. Так ошибка определения местоположения при использовании метода рядов Тейлора или МНК (выбор метода в зависимости от количества активных станций приема) меньше допустимого стандартного отклонения погрешности выдерживания траектории в боковой плоскости и меньше двукратной величины ошибки АЗН-В (370 м). Метод мультилатерации, за счет использования физических свойств распространения сигнала является более надежным с точки зрения точности, произвести атаку подмены или дублирования ВС при использовании такой системы не представляется возможным. Результаты применения методов и алгоритмов валидации показали возможность использования их в рамках системы анализа и фильтрации сообщений системы АЗН-В. Они могут применяться в качестве основных алгоритмов для обеспечения работы МПСН, так и самостоятельно, являясь вспомогательной системой, производящей маркировку данных.

# Заключение

В диссертационной работе представлено решение актуальной, имеющей важное значение для транспортной инфраструктуры Российской Федерации **научно-технической задачи** противодействия несанкционированному вмешательству при управлении воздушным движением, требующей разработки на основе единого научно-методического аппарата методов и алгоритмов валидации сообщений системы автоматического наблюдения. Решение научно-технической задачи опиралось на проведенный автором и представленный в работе проблемный анализ состояния защищенности системы автоматического зависимого наблюдения, позволяющий выявить сложившееся несоответствие между перспективами внедрения технологии автоматического зависимого наблюдения и потенциальными угрозами несанкционированного вмешательства в рассматриваемую систему, проявляющее себя в:

- противоречии практического характера между современными требованиями к уровню безопасности и регулярности полетов и отсутствием киберзащищенности системы АЗН-В;
- противоречии научного характера между необходимостью повышения достоверности информации, получаемой от АЗН-В, и отсутствием единого научно-методического аппарата комплексной обработки сообщений АЗН-В.

**Разрешение названных противоречий** решается в рамках разработки методов и алгоритмов валидации сообщений системы автоматического наблюдения. Основные результаты работы заключаются в следующем:

1. Разработана модель угроз АЗН-В на основе модели угроз ФСТЭК, позволяющая оценить степень воздействия различных типов несанкционированного вмешательства на систему АЗН-В. Система АЗН-В является объектом критической информационной инфраструктуры гражданской авиации.
2. Определены критерии достоверности данных системы АЗН-В, позволяющие оценить эффективность математических моделей, используемых в методе мультилатерации. Для оценки метода мультилатерации

используется показатель среднеквадратического отклонения при определении местоположения ВС - так при превышении СКО МП ВС от истинного МП на более чем 370 м, сообщение АЗН-В считается недостоверным.

3. Разработан алгоритм выбора математической модели метода мультилатерации, обеспечивающий наилучшее определение местоположения ВС при заданном количестве станций приема.
4. Разработан метод монолатерации, использующий алгоритмы машинного обучения для валидации сообщений АЗН-В. Метод позволяет производить валидацию сообщений в условиях недостаточного количества станций приема (1 - 3 станции), а оценка достоверности при использовании данного метода выражается в виде вероятности корректной классификации сообщений.
5. Разработан гибридный алгоритм, основанный на использовании методов моно- и мультилатерации, обеспечивающий валидацию сообщений АЗН-В при различном количестве станций приема.
6. Разработана и апробирована система анализа и фильтрации сообщений АЗН-В, являющаяся прототипом подсистемы валидации сообщений АЗН-В в АС УВД.
7. Проведена оценка эффективности математических моделей метода мультилатерации при различном количестве станций приема:
    - при наличии 4-5 равноудаленных станций приема, метод наименьших квадратов не должен быть применен при обработке данных, поскольку СКО МП ВС при в некоторых точках пространства на порядок превышает допустимые критерии достоверности данных системы АЗН-В, а метод разложения в ряд Тейлора может быть применен в радиусе 100 км от геометрического центра расположения приемных станций (максимальное СКО в этом радиусе составляет 170м);
    - при наличии 6 станций приема, математический метод разложения в ряд Тейлора показывает максимальное СКО МП ВС равное 165м при ведении наблюдения за воздушным движением в пространстве радиусом 150 км от геометрического центра расположения приемных станций;

- при наличии 7-8 равноудаленных станций приема лучшие результаты по точности показал метод МНК.

8. Проведена оценка эффективности алгоритмов машинного обучения метода монолатерации при различных типах несанкционированного вмешательства:
   - при любом типе несанкционированного вмешательства из четырех алгоритмов машинного обучения (метод K-ближайших соседей, градиентный бустинг (LightGBM), адаптивный бустинг (AdaBoost) и наивный байесовский классификатор) наилучшие результаты показали 2 алгоритма - LightGBM и K-ближайших соседей;
   - при искусственной генерации сообщений АЗН-В (использование реальных кодов ИКАО, повторение траектории движения ВС, аттенюация мощности передатчика) вероятность корректной классификации составила 0.993 для метода K-ближайших соседей и 0.994 для LightGBM;
   - при идеальных условиях проведения несанкционированного вмешательства (полное дублирование реальных данных АЗН-В с повторением характеристик сигнала) вероятность корректной классификации составила 0.916 для метода K-ближайших соседей и 0.8556 для LightGBM.

Дальнейшее направление исследований в рамках рассматриваемой научно-технической задачи можно сформулировать следующим образом:

1. Анализ применения нескольких станций приема для классификации сообщений АЗН-В методом монолатерации.
2. Оценка эффективности алгоритмов монолатерации в зависимости от количества сообщений АЗН-В.
3. Оценка применимости методов моно- и мультилатерации при наблюдении в зоне аэродрома.
4. Совершенствование метода монолатерации за счет использования узконаправленных антенн на станциях приема.

## Список сокращений и условных обозначений

**АЗН-В** - Автоматическое зависимое наблюдение-вещание

**АНС** - Аэронавигационная система

**АОН** - Авиация общего назначения

**АРП** - Автоматический радиопеленгатор

**АС УВД** - Автоматизированная система управления воздушным движением

**АЦП** - Аналого-цифровой преобразователь

**БД** - База данных

**БС** - Базовая станция

**ВД** - Воздушное движение

**ВК** - Вычислительный комплекс

**ВОРЛ** - Вторичный обзорный радиолокатор

**ВП** - Воздушное пространство

**ВПП** - Взлётно-посадочная полоса

**ВРЛ** - Вторичный радиолокатор

**ВС** - Воздушное судно

**ГЛОНАСС** - Глобальная Навигационная Спутниковая Система

**ГНСС** - Глобальная навигационная спутниковая система

**ГЦ** - Главный центр

**ЕВ** - Единого времени

**ЕС ОрВД** - Единая Система организации воздушного движения

**ЗИ** - Защита информации

**ЗЦ** - Зональный центр

**ИБ** - Информационная безопасность

**ИВД** - Интенсивность воздушного движения

**ИТ** - Информационные технологии

**ЛА** - Летательный аппарат

**МНК** - Метод наименьших квадратов

**МП** - Местоположение

**МПСН** - Многопозиционная система наблюдения

**МПУ** - Магнитный путевой угол

**НС** - Наземная станция

**ОВД** - Организация воздушного движения

**ОРЛ** - Обзорный радиолокатор

**ПВП** - Правила визуальных полетов

**ПДКИ** - Подсистема доступа к конфиденциальной информации **ПИ** - Плановая информация

**ПК** - Персональный компьютер

**ПО** - Программное обеспечение

**ППП** - Полеты по приборам

**ПРЛ** - Первичный радиолокатор

**ПСВС** - Подсистема связи с воздушным судном

**ПСИ** - Подсистема сбора информации

**ПСПИ** - Подсистема связи и передачи информации

**РВП** - Разность времен прихода

**РЛИ** - Радиолокационная информация

**РЛС ОЛП** - Радиолокационная станция обзора летного поля

**РТС** - Радиотехническая система

**РЭБ** - Радиоэлектронная борьба

**СВЧ** - Сверхвысокая частота

**СЗИ** - Средство защиты информации

**СКА** - Спутниковый космический аппарат

**СКО** - Среднеквадратическое отклонение

**СПВ** - Сигнал проверки времени

**СУБД** - Система управления базой данных

**УВД** - Управление воздушным движением

**ФАВТ** - Федеральное агентство воздушного транспорта

**ФИМ** - Фазово-импульсная модуляция

**ЧМИ** - Человеко-машинный интерфейс

**ЧС** - Чрезвычайная ситуация

**ЭЦП** - Электронная цифровая подпись

**ACARS** - Адресно-отчётная система авиационной связи

**ADS-B** - Автоматическое зависимое наблюдение-вещание

**API** - Программный интерфейс приложения

**ASTERIX** - Многоцелевой структурированный обмен информацией наблюдения Евроконтроля

**AUC-ROC** - Площадь под ROC-кривой

**BSD** - Система распространения программного обеспечения в исходных кодах

**CPDLC** - Связь "диспетчер-пилот"по линии передачи данных

**CRC** - Циклический избыточный код

**DDOS** - Распределённая атака типа «отказ в обслуживании»

**DNS** - Система доменных имён

**DOS** - Атака типа «отказ в обслуживании»

**ECDSA** - Алгоритм построения цифровой подписи с использованием эллиптических кривых

**FAA** - Федеральное управление гражданской авиации США

**GBM** - Градиентный бустинг

**GNSS** - Глобальная навигационная спутниковая система

**GPS** - Система глобального позиционирования

**HTTP** - Протокол передачи гипертекста

**ICAO** - Международная организация гражданской авиации

**IDS** - Система противодействия вторжению

**IP** - Межсетевой протокол

**JSON** - Текстовый формат обмена данными, основанный на JavaScript

**MLAT** - Мультилатерационная система

**OSI** - Сетевая модель стека сетевых протоколов OSI/ISO

**PKI** - Инфраструктура открытых ключей

**REST** - Передача состояния представления

**RFID** - Радиочастотная идентификация

**ROC** - Рабочая характеристика приёмника

**RSA** - Криптографический алгоритм с открытым ключом

**SDR** - Программно-управляемая радиосистема

**SQL** - Язык структурированных запросов

**TCAS** - Система предупреждения столкновения самолётов в воздухе

**TCP** - Протокол управления передачей

**TDOA** - Разница времен прихода

**TOA** - Времена прихода

**UAT** - Приемопередатчик универсального доступа

**VDL** - Канал передачи сверхвысокой частоты

**WAM** - Широкозонная мультилатерационная система

## Список литературы


1. A comparison of the bagging and the boosting methods using the decision trees classifiers / K. Machova [и др.] // Computer Science and Information Systems. — 2006. — Т. 3, № 2. — С. 57—72. — DOI: 10.2298/csis0602057m.
2. *Aatique M.* Evaluation of Tdoa Techniques for Position Location in Cdma Systems //. — 1997.
3. *Administration(FAA) F. A.* Current Equipage Levels [Электронный ресурс]. — 2021. — URL: https://www.faa.gov/nextgen/equipadsb/installation/current_equipage_levels/ (visited on 03/13/2021).
4. *Baud O.*, *Honore N.*, *Taupin O.* Radar / ADS-B data fusion architecture for experimentation purpose // 2006 9th International Conference on Information Fusion. — 07.2006. — С. 1—6. — DOI: 10.1109/ICIF.2006.301555.
5. *Chan Y. T.*, *Ho K. C.* A simple and efficient estimator for hyperbolic location // IEEE Transactions on Signal Processing. — 1994. — Авг. — Т. 42, № 8. — С. 1905—1915. — DOI: 10.1109/78.301830.
6. *Chandola V.*, *Banerjee A.*, *Kumar V.* Anomaly Detection: A Survey. — 2009. — Июль. — DOI: 10.1145/1541880.1541882. — URL: https://doi.org/10.1145/1541880.1541882.
7. *Costin A.*, *Francillon A.* Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. — 2012. — Июль.
8. *Daskalakis A.*, *Martone P.* A technical assessment of ADS-B and multilateration technology in the Gulf of Mexico // Proceedings of the 2003 IEEE Radar Conference (Cat. No. 03CH37474). — 05.2003. — С. 370—378. — DOI: 10.1109/NRC.2003.1203428.
9. *David Grizzle M. G.* Report from the ADS–B In Aviation Rulemaking Committee to the Federal Aviation Administration. — 2011.
10. *EUROCONTROL.* 16. Wide Area Multilateration, Report on EATMP TRS 131/04. — 2005.

11. *Fawcett T.* An introduction to ROC analysis // Pattern Recognition Letters. — 2006. — Т. 27, № 8. — С. 861—874. — DOI: https://doi.org/10.1016/j.patrec.2005.10.010. — URL: https://www.sciencedirect.com/science/article/pii/S016786550500303X ; ROC Analysis in Pattern Recognition.

12. *FOY W. H.* Position-Location Solutions by Taylor-Series Estimation // IEEE Transactions on Aerospace and Electronic Systems. — 1976. — Март. — Т. AES—12, № 2. — С. 187—194. — DOI: 10.1109/TAES.1976.308294.

13. *Freund Y.*, *Schapire R. E.* Experiments with a New Boosting Algorithm // Proceedings of the Thirteenth International Conference on International Conference on Machine Learning. — Bari, Italy : Morgan Kaufmann Publishers Inc., 1996. — С. 148—156. — (ICML'96). — ISBN 1558604197.

14. *Freund Y.*, *Schapire R. E.* A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting // Journal of Computer and System Sciences. — 1997. — Т. 55, № 1. — С. 119—139. — DOI: 10.1006/jcss.1997.1504.

15. *Haines B.* Hacking Airplanes. — 2012.

16. *ICAO.* Aeronautical Surveillance Manual (Doc 9924). — Монреаль, 2020.

17. *ИКАО.* Оценка наблюдения с использованием систем ADS-B и мультилатерации в целях обеспечения обслуживания воздушного движения и рекомендации по их внедрению. — Монреаль, 2013.

18. *ИКАО.* Ассамблея, 39 сессия (A39-WP/2961). Наблюдение дистанционно пилотируемых воздушных судов и вопросы кибербезопасности. — Монреаль, 2016.

19. *ИКАО.* Руководство по применению минимума вертикального эшелонирования в 300 м (1000 фут) между ЭП 290 и ЭП 410 включительно, издание третье. — Монреаль, 2012.

20. *ICAO.* 14. Guidance Material on Comparison of Surveillance Technologies (GMST). — Монреаль, 2007.

21. Indoor Localization with Aircraft Signals / M. Eichelberger [и др.]. — 2017. — Нояб.

22. Investigation of Signal and Message Manipulations on the Wireless Channel / C. Pöpper [и др.] // Computer Security – ESORICS 2011 / под ред. V. Atluri, C. Diaz. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. — С. 40—59. — ISBN 978-3-642-23822-2.

23. *Kalman R. E.* A New Approach to Linear Filtering and Prediction Problems // Journal of Basic Engineering, Transactions of ASME, Series D. — 1960. — Т. 82, № 1. — С. 35—45.

24. *Mccallie D. L.* Exploring Potential ADS-B Vulnerabilities in the FAA's NextGen Air Transportation System. — BiblioScholar, 2012. — ISBN 1288318480. — URL: https://www.amazon.com/Exploring-Potential-Vulnerabilities-NextGen-Transportation/dp/1288318480?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1288318480.

25. *McCallie D.*, *Butts J.*, *Mills R.* Security analysis of the ADS-B implementation in the next generation air transportation system // International Journal of Critical Infrastructure Protection. — 2011. — Т. 4, № 2. — С. 78—87. — DOI: https://doi.org/10.1016/j.ijcip.2011.06.001. — URL: http://www.sciencedirect.com/science/article/pii/S1874548211000229.

26. Methods to Provide System-Wide ADS-B Back-Up, Validation and Security / A. Smith [и др.] // 2006 ieee/aiaa 25TH Digital Avionics Systems Conference. — 10.2006. — С. 1—7. — DOI: 10.1109/DASC.2006.313681.

27. Nanosecond-precision Time-of-arrival Estimation for Aircraft Signals with Low-cost SDR Receivers / R. Calvo-Palomino [и др.] // Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks. — Porto, Portugal : IEEE Press, 2018. — С. 272—277. — (IPSN '18). — ISBN 978-1-5386-5298-5. — DOI: 10.1109/IPSN.2018.00055. — URL: https://doi.org/10.1109/IPSN.2018.00055.

28. *Oliver Jowett O. N.* dump1090-hptoa. — 2018. — https://github.com/openskynetwork/dump1090-hptoa.

29. *Perrig A.*, *Doug Tygar J.* Secure Broadcast Communication in Wired and Wireless Networks. — 01.2003. — ISBN 978-0-7923-7650-7.

30. *Purton L.*, *Abbass H.*, *Alam S.* Identification of ADS-B System Vulnerabilities and Threats. — 2010. — Янв.

31. *RTCA*. Development and Implementation Planning Guide for Automatic Dependent Surveillance (ADS-B) Applications RTCA SC-186. DO-249. — 10.1999.

32. *Sampigethaya K.*, *Poovendran R.* Security and privacy of future aircraft wireless communications with offboard systems // 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011). — 01.2011. — С. 1—6. — DOI: 10.1109/COMSNETS.2011.5716527.

33. *Sanfilippo S.* dump1090. — 2017. — https://github.com/antirez/dump1090.

34. *Schäfer M.*, *Lenders V.*, *Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication // Applied Cryptography and Network Security / под ред. M. Jacobson [и др.]. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. — С. 253—271. — ISBN 978-3-642-38980-1.

35. *Schapire R. E.* The strength of weak learnability // Machine Learning. — 1990. — Т. 5, № 2. — С. 197—227. — DOI: 10.1007/bf00116037.

36. Short Paper: Reactive Jamming in Wireless Networks: How Realistic is the Threat? / M. Wilhelm [и др.] // Proceedings of the Fourth ACM Conference on Wireless Network Security. — Hamburg, Germany : ACM, 2011. — С. 47—52. — (WiSec '11). — ISBN 978-1-4503-0692-8. — DOI: 10.1145/1998412.1998422. — URL: http://doi.acm.org/10.1145/1998412.1998422.

37. *Smith J.*, *Abel J.* Closed-form least-squares source location estimation from range-difference measurements // IEEE Transactions on Acoustics, Speech, and Signal Processing. — 1987. — Дек. — Т. 35, № 12. — С. 1661—1669. — DOI: 10.1109/TASSP.1987.1165089.

38. *Thomas P.* North sea helicopter ADS-B/MLat pilot project findings // 2011 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles. — 09.2011. — С. 53—58.

39. *Trofimova Y.* 29. Multilateration error investigation and classification. Error Estimation // Transport and Telecommunication. — 2007. — Т. 8, № 2. — С. 28—37.

40. *Wei-Jun Pan Zi-Liang Feng Y. W.* ADS-B Data Authentication Based on ECC and X.509 Certificate // Journal of Electronic Science and Technology. — 2012. — Март. — Т. 10, № 1. — С. 51—55.

41. Wide Area Multilateration for Alternate Position, Navigation, and Timing (APNT) / F. Niles [и др.] // FAA's WAM WhitePaper. — 09.2012. — С. 1—26.

42. *Wilhelm M.*, *Schmitt J.*, *Lenders V.* Practical Message Manipulation Attacks in IEEE 802.15.4 Wireless Networks. — 2012. — Март.

43. *YANG K.*, *AN J.*, *XU Z.* A Quadratic Constraint Total Least-squares Algorithm for Hyperbolic Location // International Journal of Communications, Network and System Sciences. — 2008. — Т. 1, № 2. — С. 130—135. — DOI: 10.4236/ijcns.2008.12017.

44. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. — Москва : Федеральная служба по техническому и экспортному контролю, 2008. — 69 с.

45. *Будзко В. И.*, *Демин С. С.* Система управления безопасностью авиационной деятельности – основной элемент перспективной авиатранспортной системы // Научный вестник ГосНИИ ГА. — 2020. — Т. 32. — С. 121—131.

46. *Высоцкий В. З.* Коэффициент загрузки диспетчера УВД как показатель безопасности полетов // Научный вестник МГТУ ГА. — 2006. — Т. 99.

47. *Зинкевич А. В.* Исследование возможности идентификации АЗН-В сигналов с помощью нейросетей // Вестник ТОГУ. — 2021. — Т. 2. — С. 81—88.

48. *Калинцев А. С.*, *Рубцов Е. А.* Методика выявления ложных преднамеренно формируемых сигналов АЗН-В // T-Comm - Телекоммуникации и Транспорт. — 2020. — Т. 14. № 11. — С. 4—13.

49. Концепция развития систем связи, навигации и наблюдения для ОрВД Российской Федерации. — Москва : Росаэронавигация, 2007.

50. Концепция создания и развития аэронавигационной системы России и План мероприятий по реализации Концепции создания и развития Аэронавигационной системы России (одобрены Правительством Российской Федерации- протокол заседания Правительства Российской Федерации

№35 от 4 октября 2006. — Москва : Правительство Российской Федерации, 2006.

51. *Лыонг Ч. В.* Гибридные алгоритмы оценивания координат источника радиоизлучения с применением неподвижного и подвижного пунктов приема : автореф. дис. ... канд. тех. наук : 05.12.04. — Рязань, 2014. — 144 с.

52. *Машошин А. О.* Вопросы избыточности в задаче определения местоположения воздушного судна разностно-временным методом // Научный вестник МГТУ ГА. — 2016. — Т. 224. — С. 147—157.

53. *Машошин А. О.* Определение истинности сообщений системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства на управление воздушным движением за счет метода монолатерации // Научный вестник ГосНИИ ГА. — 2021. — Т. 37. — С. 136—145.

54. *ООО "НВС Навигационные Технологии"*. Приемник временной синхронизации [Электронный ресурс]. — URL: https://navis.ru/assets/files/ANAI-469635-002-RE_RUS_E_4.pdf (дата обр. 23.03.2015).

55. *ООО "НИТА"*. Система защиты информации "СФЕРА" [Электронный ресурс]. — 2017. — URL: http://www.nita.ru/catalog/sistema-zashchity-informatsii-sfera/.

56. *Печенский В. К., Сазонова А. М.* Оценка влияния загруженности сектора управления воздушным движением на экономическую эффективность полетов воздушных судов // Научный вестник МГТУ ГА. — 2014. — Т. 209.

57. Постановление о Единой системе организации воздушного движения Российской Федерации №901 от 28 августа 2015 года. — Москва : Правительство Российской Федерации, 2015. — 1 с.

58. Постановление об утверждении Федеральных правил использования воздушного пространства Российской Федерации №1084 от 22 сентября 1999 (ред. от 14.12.2006). — Москва : Правительство Российской Федерации, 2006. — 1 с.

59. Приказ Министерства транспорта РФ от 26 сентября 2012 г. N 362 Об утверждении Федеральных авиационных правил "Осуществление радиосвязи в воздушном пространстве Российской Федерации". — Москва : Министерство транспорта РФ, 2012. — 1 с.

60. Приказ от 25 апреля 2016 г. N 282 об утверждении перечня оперативных органов Единой системы организации воздушного движения Российской Федерации. — Москва : Федеральное Агенство Воздушного Транспорта, 2016. — 1 с.

61. Приказ ФСТЭК России от 14 марта 2014 г. N 31. — Москва : Федеральная служба по техническому и экспортному контролю, 2014. — 1 с.

62. *Прокис Д.* Цифровая связь. — Москва : Радио и связь, 2000. — С. 21. 800 с.

63. Протокол совещания по выполнению подпункта «а» пункта 1 Перечня поручений Президента Российской Федерации по вопросу повышения уровня безопасности полетов. 29.04.2016 № Пр-800. — Москва : Министерство транспорта Российской Федерации, 2016.

64. *Рудельсон Л. Е.* Программное обеспечение автоматизированных ситсем управления воздушным движением. — Москва, 2008. — С. 18.

65. Федеральные правила использования воздушного пространства Российской Федерации Российской Федерации, Постановление Правительства Российской Федерации №138 от 11 марта 2010 г. — Москва : Правительство Российской Федерации, 2010. — 1 с.

66. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". — Москва : Государственная Дума Российской Федерации, 2017. — 1 с.

67. *Шестаков В.*, *Сагидуллин А.* Применение технологии websocket в web-приложениях технологического назначения // Приборостроение. — 2015. — № 4.

## Список рисунков

1.1 Структурная схема АС УВД . . . . . 16
1.2 Схема информационного взаимодействия ПО АС УВД с периферийными источниками полетных данных и смежными системами . . . . . 18
1.3 Общая схема модели угроз АЗН-В . . . . . 22
1.4 Схема архитектуры современных систем наблюдения. . . . . 23
1.5 Стек протоколов Mode S. . . . . 25
1.6 Общая схема состава сообщения АЗН-В. . . . . 26

2.1 Структурная схема методов защиты системы АЗН-В от потенциальных угроз . . . . . 36
2.2 Типичная архитектура системы MLAT для наблюдения в целях УВД [17] . . . . . 43
2.3 Определение местоположения гиперболическим методом. . . . . 43
2.4 Проверка истинности источника классическим дистанционно-ограниченым протоколом. . . . . 46
2.5 Проверка истинности источника протоколом Брандсона-Чаума. . 47
2.6 Концепция работы фильтра Калмана. . . . . 47
2.7 Структурная схема кросскорреляционного метода . . . . . 52
2.8 Структурная схема метода оценки времени прихода . . . . . 53
2.9 Групповая задержка и компоненты системы синхронизации . . . 54
2.10 Иерархия систем синхронизации . . . . . 54
2.11 Иерархия систем синхронизации . . . . . 56
2.12 Структурная схема системы синхронизации распределенного времени . . . . . 57
2.13 Структурная схема системы синхронизации на задающем транспондере . . . . . 58
2.14 Структурная схема автономной системы синхронизации ГНСС . . 59
2.15 Структурная схема системы синхронизации ГНСС единого времени . . . . . 60
2.16 Схема процесса определения оптимального алгоритма машинного обучения . . . . . 62

2.17 Принцип работы алгоритма бустинга . . . . . 66
2.18 Принцип работы алгоритма адаптивного бустинга . . . . . 67
2.19 Принцип работы алгоритма градиентного бустинга . . . . . 69
2.20 Схема спуфинг атаки на систему АЗН-В. . . . . 71
2.21 Передача блока данных сообщений АЗН-В. . . . . 74
2.22 Вектор потока данных с избыточностью . . . . . 74
2.23 Схема фильтрации в соответствии с критериями истинности . . . 78
2.24 Геометрическая иллюстрация к гиперболическому методу определения местоположения . . . . . 80
2.25 Расчетная траектория ВС для 4-х БС (а) и сравнение СКО ошибки для МНК и метода рядов Тейлора (б) . . . . . 84
2.26 СКО для МНК и метода рядов Тейлора. для 5-ти (а), 6-ти (б) и 8-ми (в) БС соответственно . . . . . 84
2.27 Поверхность ошибок (СКО, м) при 4-х БС для МНК (а) и метода рядов Тейлора (б) . . . . . 85
2.28 Контурный график ошибок при 8-ми БС для МНК (а) и метода рядов Тейлора (б) . . . . . 85
2.29 Алгоритм определения местоположения ВС для протокола 1090 ES 91
2.30 Алгоритм определения местоположения ВС для протокола 1090 ES 94

3.1 Гибридный алгоритм определения местоположения судна в условиях несанкционированного вмешательства . . . . . 99
3.2 Пример точечной аномалии . . . . . 101
3.3 Пример контекстуальной аномалии . . . . . 102
3.4 Пример коллективной аномалии . . . . . 102
3.5 Облик системы анализа и фильтрации сообщений АЗН-В при использовании группы станций приема . . . . . 106
3.6 Облик системы анализа и фильтрации сообщений АЗН-В при использовании одной станции приема . . . . . 107
3.7 Схема прохождения информационных потоков через ключевые микросервисы системы . . . . . 110

4.1 Моделирование несанкционированного вмешательства с использованием реальных полетных данных . . . . . 114
4.2 Блок-схема сбора реальных полетных данных АЗН-В . . . . . 116

4.3 Алгоритм проведения спуфинг-атаки . . . . . 119
4.4 Схема постановки эксперимента . . . . . 119
4.5 Техническая база для проведения эксперимента . . . . . 120
4.6 Вывод программы декодирования сообщений АЗН-В dump1090 - без несанкционированного вмешательства . . . . . 120
4.7 Вывод программы формирования ложных сообщений АЗН-В . . . 121
4.8 Вывод программы декодирования сообщений АЗН-В dump1090 - несанкционированное вмешательство . . . . . 121
4.9 Диаграммы уровня принимаемого сигнала для приемных устройств, размещенных в различных условиях. Период наблюдений - 2020.11.05 - 2021.11.28 . . . . . 124
4.10 Диаграммы уровня принимаемого сигнала для приемных устройств, размещенных в различных условиях. Период наблюдений - 2021.01.04 - 2021.01.24 . . . . . 125
4.11 Вклад признаков при классификации сообщений АЗН-В . . . . . 126
4.12 Реализация угрозы несанкционированного вмешательства путем повторения сигналов АЗН-В . . . . . 127

# Список таблиц

1.1 Сравнительная таблица атак на систему АЗН-В . . . . . 30

2.1 Сравнительные характеристики систем синхронизации . . . . . 60
2.2 Соответствие различных моделей для описания угроз системы АЗН-В уровням сетевой модели OSI . . . . . 71

4.1 Сравнение точности методов машинного обучения в задаче бинарной классификации сообщений АЗН-В . . . . . 126
4.2 Сравнение точности методов машинного обучения в задаче бинарной классификации сообщений АЗН-В. Несанкционированное вмешательство: повторение сигналов . . . . 128

# Приложение А

## Примеры кода имитационного моделировнаия

Код имитационного моделирования метода рядов Тейлора представлен на листинге А.1.

Листинг А.1

Задание координат для 8-ми станций приема

```
    function [] = WAM( BS1, BS2, BS3, BS4, BS5, BS6, BS7, BS8 )
%UNTITLED Summary of this function goes here
%   Detailed explanation goes here
t = 0:0.1:1.6;
l = -pi : pi/8 : pi;
X = rand()*(cos(l)-sin(l));
Y = rand()*t;
% BS1 = [-1*(10^5),2.38*(10^5)];
% BS2 = [0*(10^5),2.38*(10^5)];
% BS3 = [0*(10^5),1.5*(10^5)];
% BS4 = [-1*(10^5),1.5*(10^5)];

% BS1 = [-1.18*(10^5),2*(10^5)];
% BS2 = [-0.7*(10^5),2.51*(10^5)];
% BS3 = [0*(10^5),2.37*(10^5)];
% BS4 = [-1*(10^5),1.5*(10^5)];
% BS5 = [0.2*(10^5),1.74*(10^5)];
% BS6 = [-0.26*(10^5),1.33*(10^5)];

% BS1 = [-1*(10^5),2.38*(10^5)];
% BS2 = [-0.48*(10^5),2.53*(10^5)];
% BS3 = [0*(10^5),2.38*(10^5)];
% BS4 = [0.2*(10^5),1.9*(10^5)];
% BS5 = [0*(10^5),1.5*(10^5)];
% BS6 = [-0.48*(10^5),1.3*(10^5)];
% BS7 = [-1*(10^5),1.5*(10^5)];
% BS8 = [-1.2*(10^5),1.9*(10^5)];

% BS1 = [-1.13*(10^5),2.23*(10^5)];
% BS2 = [-0.48*(10^5),2.53*(10^5)];
% BS3 = [0.09*(10^5),2.23*(10^5)];
% BS4 = [0*(10^5),1.5*(10^5)];
% BS5 = [-1*(10^5),1.5*(10^5)];
```

Листинг А.2

Вычисление псевдодальностей

```
    R21 = sqrt(((BS2(1)-BS1(1))^2)+((BS2(2)-BS1(2))^2));
R31 = sqrt(((BS3(1)-BS1(1))^2)+((BS3(2)-BS1(2))^2));
R41 = sqrt(((BS4(1)-BS1(1))^2)+((BS4(2)-BS1(2))^2));

R51 = sqrt(((BS5(1)-BS1(1))^2)+((BS5(2)-BS1(2))^2));
R61 = sqrt(((BS6(1)-BS1(1))^2)+((BS6(2)-BS1(2))^2));
R71 = sqrt(((BS7(1)-BS1(1))^2)+((BS7(2)-BS1(2))^2));
R81 = sqrt(((BS8(1)-BS1(1))^2)+((BS8(2)-BS1(2))^2));

%-----------------------------------------------------------------

x21 = BS2(1)-BS1(1);
x31 = BS3(1)-BS1(1);
x41 = BS4(1)-BS1(1);

x51 = BS5(1)-BS1(1);
x61 = BS6(1)-BS1(1);
x71 = BS7(1)-BS1(1);
x81 = BS8(1)-BS1(1);


y21 = BS2(2)-BS1(2);
y31 = BS3(2)-BS1(2);
y41 = BS4(2)-BS1(2);

y51 = BS5(2)-BS1(2);
y61 = BS6(2)-BS1(2);
y71 = BS7(2)-BS1(2);
y81 = BS8(2)-BS1(2);
```

Листинг А.3

Условия моделирования

```
    X(1)=0;
Y(1)=0;



for t =1:100
    l = pi/8;
        %X(t+1) = 1.1317*(X(t)+rand()*(cos(l*t)-sin(l*rand()*t)));
        %Y(t+1) = Y(t)+110*t*rand();
        X(t+1) = 1.1317*(X(t)+0.5*(cos(l*t)-sin(l*0.5*t)));
        Y(t+1) = Y(t)+110*t*0.5;
```

Листинг А.4

Использование заданного ряда ошибок

```
ERR1(1) = 2.0498*10^-9;
ERR2(1) = 1.2876*10^-8;
ERR3(1) = 2.9975*10^-9;
ERR4(1) = 9.1101*10^-9;
ERR5(1) = 8.1457*10^-9;
ERR6(1) = 2.4349*10^-9;
ERR7(1) = 8.4796*10^-9;
ERR8(1) = 1.1572*10^-8;
```

Листинг А.5

Имитация вычисления псевдодальностей с учетом заданного уровня ошибок

```
R1(t) = sqrt(((X(t)-BS1(1))^2) + ((Y(t)-BS1(2))^2));
        R2(t) = sqrt(((X(t)-BS2(1))^2) + ((Y(t)-BS2(2))^2));
        R3(t) = sqrt(((X(t)-BS3(1))^2) + ((Y(t)-BS3(2))^2));
        R4(t) = sqrt(((X(t)-BS4(1))^2) + ((Y(t)-BS4(2))^2));
        R5(t) = sqrt(((X(t)-BS5(1))^2) + ((Y(t)-BS5(2))^2));
        R6(t) = sqrt(((X(t)-BS6(1))^2) + ((Y(t)-BS6(2))^2));
        R7(t) = sqrt(((X(t)-BS7(1))^2) + ((Y(t)-BS7(2))^2));
        R8(t) = sqrt(((X(t)-BS8(1))^2) + ((Y(t)-BS8(2))^2));



        tau1(t) = R1(t)/300000000 + ERR1(t);
        tau2(t) = R2(t)/300000000 + ERR2(t);
        tau3(t) = R3(t)/300000000 + ERR3(t);
        tau4(t) = R4(t)/300000000 + ERR4(t);

        tau5(t) = R5(t)/300000000 + ERR5(t);
        tau6(t) = R6(t)/300000000 + ERR6(t);
        tau7(t) = R7(t)/300000000 + ERR7(t);
        tau8(t) = R8(t)/300000000 + ERR8(t);
```

Листинг А.6

Расчет времени прихода сигнала

```
rand_delay =  rand(1)*10^-5;

        ERR1(t+1) = ERR1(t)/1.04;
        ERR2(t+1) = ERR2(t)/1.04;
        ERR3(t+1) = ERR3(t)/1.04;
        ERR4(t+1) = ERR4(t)/1.04;
        ERR5(t+1) = ERR5(t)/1.04;
        ERR6(t+1) = ERR6(t)/1.04;
        ERR7(t+1) = ERR7(t)/1.04;
        ERR8(t+1) = ERR8(t)/1.04;


        %tau1(t) = R1(t)/300000000 + (rand_delay);
        %tau2(t) = R2(t)/300000000 + (rand_delay+(rand(1)*10^-7));
        %tau3(t) = R3(t)/300000000 + (rand_delay+(rand(1)*10^-7));
        %tau4(t) = R4(t)/300000000 + (rand_delay+(rand(1)*10^-7));


        tau21(t) = tau2(t)-tau1(t);
        tau31(t) = tau3(t)-tau1(t);
        tau41(t) = tau4(t)-tau1(t);

        tau51(t) = tau5(t)-tau1(t);
        tau61(t) = tau6(t)-tau1(t);
        tau71(t) = tau7(t)-tau1(t);
        tau81(t) = tau8(t)-tau1(t);


        r21(t) = tau21(t)*300000000;
        r31(t) = tau31(t)*300000000;
        r41(t) = tau41(t)*300000000;

        r51(t) = tau51(t)*300000000;
        r61(t) = tau61(t)*300000000;
        r71(t) = tau71(t)*300000000;
        r81(t) = tau81(t)*300000000;
```

Листинг А.7

Расчет местоположения методом рядов Тейлора

```
A{t}=[x21 y21 r21(t); x31 y31 r31(t); x41 y41 r41(t); x51 y51 r51(t); x61 y61 r61(t);
        %--Dodelat po analogii
        b{t}= [(x21^2)+(y21^2)-(r21(t)^2);(x31^2)+(y31^2)-(r31(t)^2);(x41^2)+(y41^2)-
        xe{t}=((A{:,t}.'*A{:,t}))\A{:,t}.'*b{:,t};
        SX(t)=(xe{t}(1)+BS1(1));
        SY(t)=(xe{t}(2)+BS1(2));
        SRX(t)= SX(t).';
        SRY(t)= SY(t).';

        X_diff(t) = X(t)-SRX(t);
        Y_diff(t) = Y(t)-SRY(t);
        fun(t)=(SRX(t)-X(t))^2;
        E(t)=sqrt(((X(t)-SRX(t))^2)+((Y(t)-SRY(t))^2));
```

Листинг А.8

Отрисовка графика поверхности ошибок

```
disp('X');
disp(X(83));
disp('Y');
disp(Y(83));
disp('R1(5)');
disp(R1(5));
disp('tau21(5)');
disp(tau21(5));
disp('tau2(5)');
disp(tau2(5));
disp('tau1(5)');
disp(tau1(5));

disp('xs Xreal');
disp (xe{83}(1));
disp (X(1)-BS1(1));
disp('ys Yreal');
disp (xe{83}(2));
disp (Y(1)-BS1(2));

disp('A1');
disp (A{1}(1,3));


disp(X_diff(20));
disp(Y_diff(20));
```

Листинг А.9

Отрисовка графика поверхности ошибок

```
figure(1);
subplot(2,1,1), plot(X_diff);
grid on; xlabel('time'); ylabel('Fluctuation'); title('Xfluct');

subplot(2,1,2),plot(Y_diff);
grid on; xlabel('time'); ylabel('Fluctuation'); title('Yfluct');

figure(3);
subplot(2,1,1),plot(E);
grid on; xlabel('time'); ylabel('MALEs'); title('MALE');


figure(2);
plot(SRX,SRY,'b-',X,Y,'--red',BS2(1),BS2(2),'*',BS1(1),BS1(2),'*',BS3(1),BS3(2),'*',BS
```

Код имитационного моделирования методом МНК представлен на листинге А.14.

Листинг А.10

Задача расположения приемных станций

```
a= inputdlg('BS1: enter x y coordinates','BS1');
BS1=str2num(a{1})*10^5;
if isempty(BS1)
    BS1 = [-0.7*(10^5),1.62*(10^5)];
end
a= inputdlg('BS2: enter x y coordinates','BS2');
BS2=str2num(a{1})*10^5;
if isempty(BS2)
    BS2 = [-1*(10^5),1.6*(10^5)];
end
a= inputdlg('BS3: enter x y coordinates','BS3');
BS3=str2num(a{1})*10^5;
if isempty(BS3)
    BS3 = [-1*(10^5),1.5*(10^5)];
end
a= inputdlg('BS4: enter x y coordinates','BS4');
BS4=str2num(a{1})*10^5;
if isempty(BS4)
    BS4 = [-0.7*(10^5),1.5*(10^5)];
end
a= inputdlg('BS5: enter x y coordinates','BS5');
BS5=str2num(a{1})*10^5;
if isempty(BS5)
    BS5 = [-1*(10^5),1.5*(10^5)];
end
a= inputdlg('BS6: enter x y coordinates','BS6');
BS6=str2num(a{1})*10^5;
if isempty(BS6)
    BS6 = [-1*(10^5),1.5*(10^5)];
end
a= inputdlg('BS7: enter x y coordinates','BS7');
BS7=str2num(a{1})*10^5;
if isempty(BS7)
    BS7 = [-1*(10^5),1.5*(10^5)];
end
a= inputdlg('BS8: enter x y coordinates','BS8');
BS8=str2num(a{1})*10^5;
if isempty(BS8)
    BS8 = [-1*(10^5),1.5*(10^5)];
end
```

Листинг А.11

Определение расстояния между приемными станциями

```
R21 = sqrt(((BS2(1)-BS1(1))^2)+((BS2(2)-BS1(2))^2));
R31 = sqrt(((BS3(1)-BS1(1))^2)+((BS3(2)-BS1(2))^2));
R41 = sqrt(((BS4(1)-BS1(1))^2)+((BS4(2)-BS1(2))^2));

R51 = sqrt(((BS5(1)-BS1(1))^2)+((BS5(2)-BS1(2))^2));
R61 = sqrt(((BS6(1)-BS1(1))^2)+((BS6(2)-BS1(2))^2));
R71 = sqrt(((BS7(1)-BS1(1))^2)+((BS7(2)-BS1(2))^2));
R81 = sqrt(((BS8(1)-BS1(1))^2)+((BS8(2)-BS1(2))^2));
```

Листинг А.12

Определение псевдодальностей между приемными станциями

```
x21 = BS2(1)-BS1(1);
x31 = BS3(1)-BS1(1);
x41 = BS4(1)-BS1(1);

x51 = BS5(1)-BS1(1);
x61 = BS6(1)-BS1(1);
x71 = BS7(1)-BS1(1);
x81 = BS8(1)-BS1(1);


y21 = BS2(2)-BS1(2);
y31 = BS3(2)-BS1(2);
y41 = BS4(2)-BS1(2);

y51 = BS5(2)-BS1(2);
y61 = BS6(2)-BS1(2);
y71 = BS7(2)-BS1(2);
y81 = BS8(2)-BS1(2);
```

Листинг А.13

Определение начальных условий ошибки отппределения времени пприхода сигнала

```
X(1)=0;
Y(1)=0;

ERR1 = 15*rand(1)*10^-9;
ERR2 = 15*rand(1)*10^-9;
ERR3 = 15*rand(1)*10^-9;
ERR4 = 15*rand(1)*10^-9;
ERR5 = 15*rand(1)*10^-9;
ERR6 = 15*rand(1)*10^-9;
ERR7 = 15*rand(1)*10^-9;
ERR8 = 15*rand(1)*10^-9;

ERR = [ERR2-ERR1;ERR3-ERR1;ERR4-ERR1;ERR5-ERR1;ERR6-ERR1;ERR7-ERR1;ERR8-ERR1];

% Covarince matrix of errors
Q = mean(ERR*ERR.');
```

Листинг А.14

Определение операции моделирования процесса

```
for t =1:100
    l = pi/8;
        %X(t+1) = 1.1317*(X(t)+rand()*(cos(l*t)-sin(l*rand()*t)));
        %Y(t+1) = Y(t)+110*t*rand();
        X(t+1) = 1.1317*(X(t)+0.5*(cos(l*t)-sin(l*0.5*t)));
        Y(t+1) = Y(t)+110*t*0.5;
```

Листинг А.15

Определение нелинейной системы уравнений для 8 точек приема

```
R1(t) = sqrt(((X(t)-BS1(1))^2) + ((Y(t)-BS1(2))^2));
        R2(t) = sqrt(((X(t)-BS2(1))^2) + ((Y(t)-BS2(2))^2));
        R3(t) = sqrt(((X(t)-BS3(1))^2) + ((Y(t)-BS3(2))^2));
        R4(t) = sqrt(((X(t)-BS4(1))^2) + ((Y(t)-BS4(2))^2));
        R5(t) = sqrt(((X(t)-BS5(1))^2) + ((Y(t)-BS5(2))^2));
        R6(t) = sqrt(((X(t)-BS6(1))^2) + ((Y(t)-BS6(2))^2));
        R7(t) = sqrt(((X(t)-BS7(1))^2) + ((Y(t)-BS7(2))^2));
        R8(t) = sqrt(((X(t)-BS8(1))^2) + ((Y(t)-BS8(2))^2));
```

Листинг А.16

Определение времени прихода сигнала с поправкой на заданные показатели ошибок

```
tau1(t) = R1(t)/300000000 + ERR1;
        tau2(t) = R2(t)/300000000 + ERR2;
        tau3(t) = R3(t)/300000000 + ERR3;
        tau4(t) = R4(t)/300000000 + ERR4;

        tau5(t) = R5(t)/300000000 + ERR5;
        tau6(t) = R6(t)/300000000 + ERR6;
        tau7(t) = R7(t)/300000000 + ERR7;
        tau8(t) = R8(t)/300000000 + ERR8;
```

Листинг А.17

Определение имитируемых разностей прихода сигнала

```
tau21(t) = tau2(t)-tau1(t);
        tau31(t) = tau3(t)-tau1(t);
        tau41(t) = tau4(t)-tau1(t);

        tau51(t) = tau5(t)-tau1(t);
        tau61(t) = tau6(t)-tau1(t);
        tau71(t) = tau7(t)-tau1(t);
        tau81(t) = tau8(t)-tau1(t);
```

Листинг А.18

Определение имитируемых псевдодальностей

```
r21(t) = tau21(t)*300000000;
        r31(t) = tau31(t)*300000000;
        r41(t) = tau41(t)*300000000;

        r51(t) = tau51(t)*300000000;
        r61(t) = tau61(t)*300000000;
        r71(t) = tau71(t)*300000000;
        r81(t) = tau81(t)*300000000;
```

Листинг А.19

Подготовка данных для вычисления методом МНК

```
XRT(1)=0;
        YRT(1)=0;


        r1(t) = sqrt(((BS1(1)-XRT(t))^2)-((BS1(2)-YRT(t))^2));
        r2(t) = sqrt(((BS2(1)-XRT(t))^2)-((BS2(2)-YRT(t))^2));
        r3(t) = sqrt(((BS3(1)-XRT(t))^2)-((BS3(2)-YRT(t))^2));
        r4(t) = sqrt(((BS4(1)-XRT(t))^2)-((BS4(2)-YRT(t))^2));
        r5(t) = sqrt(((BS5(1)-XRT(t))^2)-((BS5(2)-YRT(t))^2));
        r6(t) = sqrt(((BS6(1)-XRT(t))^2)-((BS6(2)-YRT(t))^2));
        r7(t) = sqrt(((BS7(1)-XRT(t))^2)-((BS7(2)-YRT(t))^2));
        r8(t) = sqrt(((BS8(1)-XRT(t))^2)-((BS8(2)-YRT(t))^2));
```

Листинг А.20

Подготовка данных для вычисления методом МНК

```
g11(t) = ((BS1(1)-XRT(t))/r1(t))-((BS2(1)-XRT(t))/r2(t));
g12(t) = ((BS1(1)-YRT(t))/r1(t))-((BS2(1)-YRT(t))/r2(t));

g21(t) = ((BS1(1)-XRT(t))/r1(t))-((BS3(1)-XRT(t))/r3(t));
g22(t) = ((BS1(1)-YRT(t))/r1(t))-((BS3(1)-YRT(t))/r3(t));

g31(t) = ((BS1(1)-XRT(t))/r1(t))-((BS4(1)-XRT(t))/r4(t));
g32(t) = ((BS1(1)-YRT(t))/r1(t))-((BS4(1)-YRT(t))/r4(t));

g41(t) = ((BS1(1)-XRT(t))/r1(t))-((BS5(1)-XRT(t))/r5(t));
g42(t) = ((BS1(1)-YRT(t))/r1(t))-((BS5(1)-YRT(t))/r5(t));

g51(t) = ((BS1(1)-XRT(t))/r1(t))-((BS6(1)-XRT(t))/r6(t));
g52(t) = ((BS1(1)-YRT(t))/r1(t))-((BS6(1)-YRT(t))/r6(t));

g61(t) = ((BS1(1)-XRT(t))/r1(t))-((BS7(1)-XRT(t))/r7(t));
g62(t) = ((BS1(1)-YRT(t))/r1(t))-((BS7(1)-YRT(t))/r7(t));

g71(t) = ((BS1(1)-XRT(t))/r1(t))-((BS8(1)-XRT(t))/r8(t));
g72(t) = ((BS1(1)-YRT(t))/r1(t))-((BS8(1)-YRT(t))/r8(t));
```

Листинг А.21

Определение местоположения цели методом МНК

```
A{t}=[x21 y21 r21(t); x31 y31 r31(t); x41 y41 r41(t); x51 y51 r51(t); x61 y61
b{t}= [(x21^2)+(y21^2)-(r21(t)^2);(x31^2)+(y31^2)-(r31(t)^2);(x41^2)+(y41^2)-
xe{t}=((A{:,t}.'*A{:,t}))\A{:,t}.'*b{:,t};
SX(t)=(xe{t}(1)+BS1(1));
SY(t)=(xe{t}(2)+BS1(2));
SRX(t)= SX(t).';
SRY(t)= SY(t).';
h{t} = [(r21(t)-(r2(t)-r1(t)));(r31(t)-(r3(t)-r1(t)));(r41(t)-(r4(t)-r1(t)));
G{t} = [g11(t) g12(t);g21(t) g22(t);g31(t) g32(t);g41(t) g42(t);g51(t) g52(t)
TLR1{t} = (G{:,t}.'/Q)*G{:,t};
TLR2{t} = (G{:,t}.'/Q)*h{:,t};


TDELTA{t} = TLR1{:,t}\TLR2{:,t};
XRT(t+1) = (TDELTA{t}(1)-XRT(t));
YRT(t+1) = (TDELTA{t}(2)-YRT(t));
```

Листинг А.22

Определение местоположения цели методом МНК

```
X_diff(t) = X(t)-SRX(t);
Y_diff(t) = Y(t)-SRY(t);
fun(t)=(SRX(t)-X(t))^2;
E(t)=sqrt(((X(t)-SRX(t))^2)+((Y(t)-SRY(t))^2));
```

Листинг А.23

Построение поверхности ошибок

```
disp('X');
disp(X(5));
disp('Y');
disp(Y(5));
disp('R1(5)');
disp(R1(5));
disp('tau21(5)');
disp(tau21(5));
disp('tau2(5)');
disp(tau2(5));
disp('tau1(5)');
disp(tau1(5));

disp('xs Xreal');
disp (xe{1}(1));
disp (X(1)-BS1(1));
disp('ys Yreal');
disp (xe{1}(2));
disp (Y(1)-BS1(2));

disp('A1');
disp (A{1}(1,3));



disp(X_diff(20));
disp(Y_diff(20));
```

Листинг А.24

Построение поверхности ошибок

```
figure(1);
subplot(2,1,1), plot(X_diff);
grid on; xlabel('time'); ylabel('Fluctuation'); title('Xfluct');

subplot(2,1,2),plot(Y_diff);
grid on; xlabel('time'); ylabel('Fluctuation'); title('Yfluct');

figure(3);
subplot(2,1,1),plot(E);
grid on; xlabel('time'); ylabel('MALEs'); title('MALE');


figure(2);
plot(SRX,SRY,'b-',X,Y,'--red',BS2(1),BS2(2),'*',BS1(1),BS1(2),'*',BS3(1),BS3(2),'*',BS


figure(4);
plot(XRT,YRT,'b-',X,Y,'--red',BS2(1),BS2(2),'*',BS1(1),BS1(2),'*',BS3(1),BS3(2),'*',BS
```

# Приложение Б

## Примеры кода определения точного времени прихода сигнала

Код демодуляции сообщения [28] с частотой отсчетов 2,4МГц представлен на листинге Б.1.

Листинг Б.1

Демодуляция с частотой сэмпплирования 2,4 МГц

```
// Part of dump1090, a Mode S message decoder for RTLSDR devices.


#include "dump1090.h"
#include "hp-toa/manager.h"


void demodulate2400AC(struct mag_buf *mag)



        if (!(m[f1_sample-1] < m[f1_sample+0]))
            continue;      // not a rising edge

        if (m[f1_sample+2] > m[f1_sample+0] || m[f1_sample+2] > m[f1_sample+1])
            continue;      // quiet part of bit wasn't sufficiently quiet

        unsigned f1_noise = (m[f1_sample-1] + m[f1_sample+2]) / 2;
        unsigned f1_signal = (m[f1_sample+0] + m[f1_sample+1]) / 2;

        if (f1_noise * 4 > f1_signal) {
            // require 12dB SNR
            continue;
        }
```

Код расчета местоположния согласно данным с разных точек приема представлен на листинге Б.2.

Листинг Б.2

Определение местоположения на стороне ЦОД гиперболическим методом

```
def solve(measurements, altitude, altitude_error, initial_guess):

    if len(measurements) + (0 if altitude is None else 1) < 4:
        raise ValueError('Not enough measurements available')

    base_timestamp = measurements[0][1]
    pseudorange_data = [(receiver.position,
                         (timestamp - base_timestamp) * constants.Cair,
                         math.sqrt(variance) * constants.Cair)
                        for receiver, timestamp, variance in measurements]
    x_guess = [initial_guess[0], initial_guess[1], initial_guess[2], 0.0]
    x_est, cov_x, infodict, mesg, ier = scipy.optimize.leastsq(
        _residuals,
        x_guess,
        args=(pseudorange_data, altitude, altitude_error),
        full_output=True,
        maxfev=config.SOLVER_MAXFEV)
```

Листинг Б.3

Определение местоположения на стороне ЦОД гиперболическим методом

```
if ler in (1, 2, 3, 4):
    #glogger.info("solver success: {0} {1}".format(ler, mesg))

    # Solver found a result. Validate that it makes
    # some sort of physical sense.
    (*position_est, offset_est) = x_est

    if offset_est < 0 or offset_est > config.MAX_RANGE:
        #glogger.info("solver: bad offset: {0}".formaT(offset_est))
        # implausible range offset to closest receiver
        return None

    for receiver, timestamp, variance in measurements:
        d = geodesy.ecef_distance(receiver.position, position_est)
        if d > config.MAX_RANGE:
            # too far from this receiver
            #glogger.info("solver: bad range: {0}".format(d))
            return None

    if cov_x is None:
        return position_est, None
    else:
        return position_est, cov_x[0:3, 0:3]

else:
    # Solver failed
    #glogger.info("solver: failed: {0} {1}".format(ler, mesg))
    return None
```

Код вывода сообщений, отфильтрованных компаратором представлен на листинге Б.4.

Листинг Б.4

Определение используемых библиотек и определение формата вывода (CSV)

```
    import asyncio
import logging
import time
import math
import functools
import socket
import numpy

from mlat import constants, geodesy
from mlat.server import util, net

"""
Various output methods for multilateration results.
"""


def format_time(timestamp):
    return time.strftime("%H:%M:%S", time.gmtime(timestamp)) + ".{0:03.0f}".format(mat


def format_date(timestamp):
    return time.strftime("%Y/%m/%d", time.gmtime(timestamp))


def csv_quote(s):
    if s is None:
        return ''
    if s.find('\n') == -1 and s.find('"') == -1 and s.find(',') == -1:
        return s
    else:
        return '"' + s.replace('"', '""') + '"'
```

Листинг Б.5

Определение функции вывода сообщений

```
def write_result(self, receive_timestamp, address, ecef, ecef_cov, receivers, distinct
        try:
            if self.use_kalman_data:
                if not kalman_data.valid or kalman_data.last_update < receive_timestar
                    return

                lat, lon, alt = kalman_data.position_llh
                speed = int(round(kalman_data.ground_speed * constants.MS_TO_KTS))
                heading = int(round(kalman_data.heading))
                vrate = int(round(kalman_data.vertical_speed * constants.MS_TO_FPM))
            else:
                lat, lon, alt = geodesy.ecef2llh(ecef)
                speed = ''
                heading = ''
                vrate = ''

            ac = self.coordinator.tracker.aircraft[address]
            callsign = ac.callsign
            squawk = ac.squawk
            altitude = int(round(alt * constants.MTOF))
            send_timestamp = time.time()
```

Листинг Б.6

Определение формата вывода сообщений

```
line = self.TEMPLATE.format(mtype=3,
                                        addr=address,
                                        rcv_date=format_date(receive_timestamp),
                                        rcv_time=format_time(receive_timestamp),
                                        now_date=format_date(send_timestamp),
                                        now_time=format_time(send_timestamp),
                                        callsign=csv_quote(callsign),
                                        squawk=csv_quote(squawk),
                                        lat=round(lat, 4),
                                        lon=round(lon, 4),
                                        altitude=altitude,
                                        speed=speed,
                                        heading=heading,
                                        vrate=vrate,
                                        fs='',
                                        emerg='',
                                        ident='',
                                        aog='')
            self.writer.write(line.encode('ascii'))
            self.last_output = time.monotonic()

        except Exception:
            self.logger.exception("Failed to write result")
            # swallow the exception so we don't affect our caller
```