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»

А В Т О Р Е Ф Е Р А Т
диссертации на соискание учёной степени кандидата технических наук

Москва — 2022

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет гражданской авиации» (МГТУ ГА).

Научный руководитель: кандидат технических наук, доцент, декан факультета авиационных систем и комплексов (ФАСК)
Петров Виктор Иванович

Официальные оппоненты: доктор технических наук,
профессор кафедры "Телекоммуникационные системы" филиала Военной академии РВСН им. Петра Великого (г. Серпухов),
Марюхненко Виктор Сергеевич

кандидат технических наук,
генеральный директор НППФ "Спектр",
Завалишин Олег Иванович

Ведущая организация: Федеральное государственное унитарное предприятие «Государственный научно-исследовательский институт гражданской авиации» (ФГУП ГосНИИ ГА), г. Москва.

Защита состоится 1 июня 2022 г. в 14:00 на заседании диссертационного совета Д 223.011.01 в Московском государственном техническом университете гражданской авиации по адресу: 125493, г. Москва, Кронштадтский бульвар, д. 20.

С диссертацией можно ознакомиться в библиотеке университета и на сайте www.mstuca.ru.

Автореферат разослан ____ _____ 2022 года.

Ученый секретарь
диссертационного совета
Д 223.011.01, доктор технических наук, профессор

Самойленко
Василий Михайлович

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, 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, 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 области информационной безопасности, указывают на то, что использование данной системы без каких либо дополнительных проверок определения достоверности данных, может являться непредусмотрительным решением. Исследования 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 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 Фальков Э.Я., Быбин С.С., 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., Лаврентьев О.Ю., Косьянчук В.В., Сельвесюк Н.И., 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» . Также в работе Калинцева А. С. и Рубцова Е. А. «Методика выявления ложных преднамеренно формируемых сигналов АЗН-В» 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 алго-

ритмов 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 5 (29 с.), 2 (21 с.) из которых были опубликованы в изданиях (по транспорту), рекомендованных ВАК при Минобрнауки РФ.

Также имеются тезисы участия в международных научно-технических конференциях и всероссийских совещаниях:

– «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, МГТУ ГА, 2016.
– «АЗН-В как новый тип аэронавигационного наблюдения. Проблемы безопасности и пути снижения угроз посредством измерения физических характеристик системы», XIII Всероссийское совещание-семинар «Инженерно-физические проблемы новой техники», Сборник докладов МГТУ им. Н.Э. Баумана, 2018.
– «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, МГТУ ГА, 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, четырех глав, заключения и приложения. Полный объем диссертации составляет 171 страницу с 55 рисунками и 5 таблицами. Список литературы содержит 67 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** дается обоснование актуальности темы диссертации, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, сформулированы научная новизна и практическая значимость представляемой работы.

В первой главе произведен анализ критичных элементов инфраструктуры автоматизированной системы управления воздушным движения с позиции безопасности полетов. Дана оценка влияния угроз несанкционированного вмешательства на отдельные компоненты автоматизированной системы управления воздушным движением, в частности на систему АЗН-В. Определяются наиболее "узкие"места системы АЗН-В, как компонента АС УВД. Схема информационного взаимодействия представлена на Рис. 1,

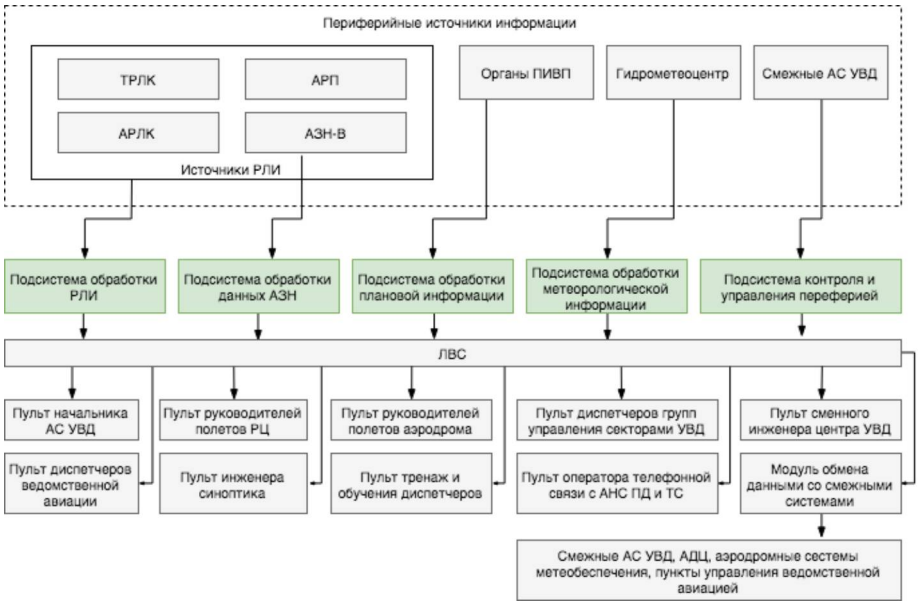


Рис. 1 — Схема информационного взаимодействия ПО АС УВД с периферийными источниками полетных данных и смежными системами

Исходя из схемы становится ясно, что при наличии только одного источника радиолокационной информации - системы АЗН-В, ситуация введения диспетчерской службы в заблуждение теоретически может наступить, при этом применение технологии АЗН-В становится небезопасным.

Для оценки угроз несанкционированного вмешательства на систему АЗН-В необходимо разработать модель угроз, поскольку существующая модель угроз ФСТЭК не позволяет описать взаимодействие участников воздушного движения и возможные угрозы. Для классификации типов несанкционированного вмешательства на систему АЗН-В, используется базовая модель угроз безопасности персональных данных (УБПДн). Для адаптации данной модели в качестве персональных данных принимаются сообщения АЗН-В. Общая схема модели угроз АЗН-В приводится на Рис. 2

Существуют следующие виды возможных угроз несанкционированного вмешательства: анализ радиотрафика, зашумление канала, ложное информирование ВС, скрытие ВС, виртуальное изменение траектории ВС. Наибольшую опасность представляют два вида угроз - несанкционированное вмешательство посредством ложного информирования воздушного судна и наземной станции, а также зашумление канала связи (в таблице угроза указана как DOS АЗН). Учитывая тот факт, что определение местоположения генератора пространственного зашумления не представляет сложности, а такие атаки как

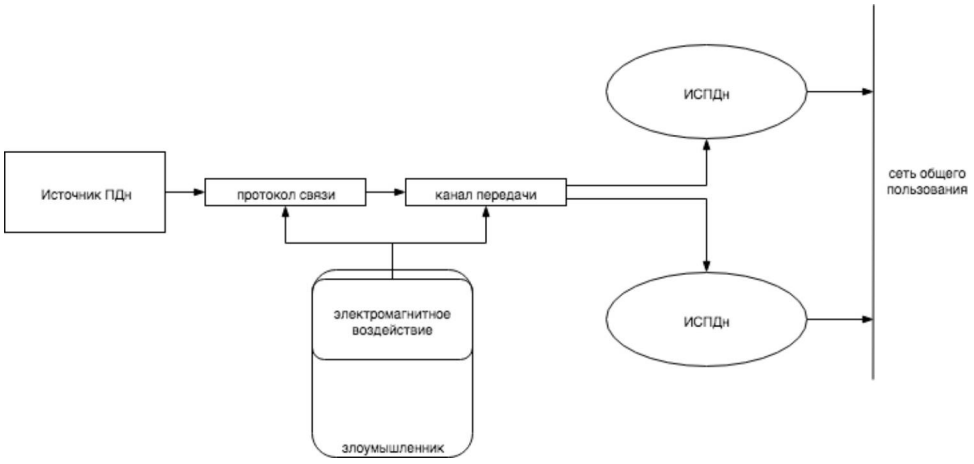


Рис. 2 — Общая схема модели угроз АЗН-В

виртуальный угон и скрытие ВС являются сложными в исполнении, наибольший научный интерес представляет атака ложного информирование ВС/НС. В работе рассмотрено несанкционированное вмешательство в работу наземной станции АЗН с использованием атаки ложной цели.

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.

Вторая глава диссертации посвящена оценке существующих методов и алгоритмов валидации сообщений системы АЗН и разработке новых методов, позволяющих решить задачу определения истинности сообщений в условиях несанкционированного вмешательства.

Необходимые условия обеспечения сетевой безопасности АЗН-В заключаются в: необходимости обеспечения целостности передаваемых данных, целостности и подлинности источника, своевременном обнаружении инцидентов несанкционированного вмешательства, обеспечении защиты от атак направленных на полный отказ системы АЗН, масштабируемости системы защиты АЗН.

Произведем классификацию существующих методов противодействия угрозам на систему АЗН-В.

Как показано на схеме (Рис. 3), существует два подхода к обеспечению безопасности АЗН-В: широковещательная аутентификация и верификация местоположения. 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.

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.

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, таких как зоны навигационного

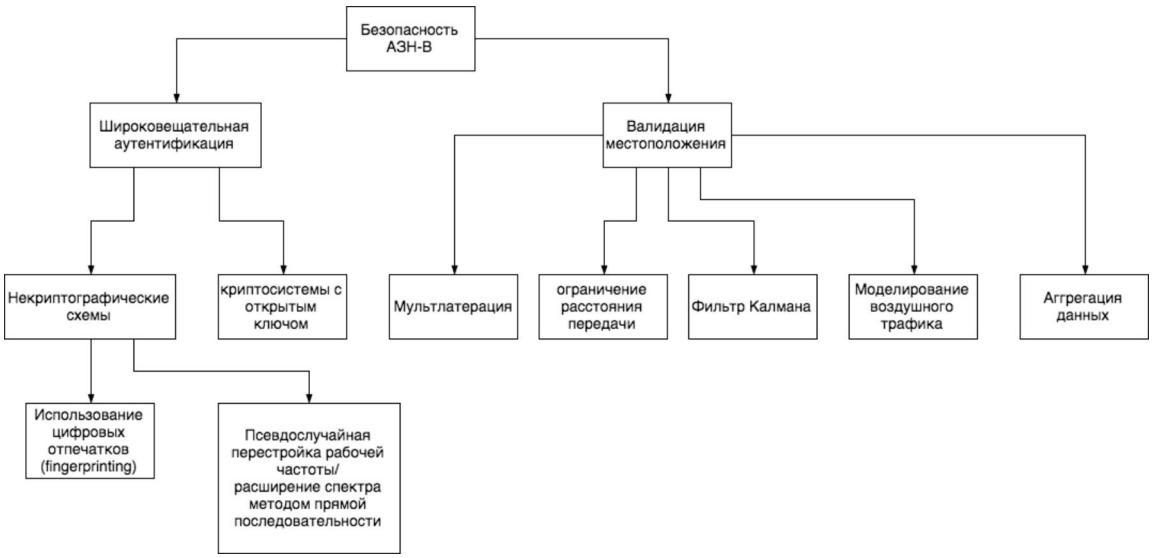


Рис. 3 — Структурная схема методов защиты системы АЗН-В от потенциальных угроз

обеспечения на маршрутах полета и зоны захода на посадку. Мультилатерационная система состоит из наземных станций (НС), принимающих сообщения АЗН-В от воздушных судов, и центральный узел обработки данных для вычислсния 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).

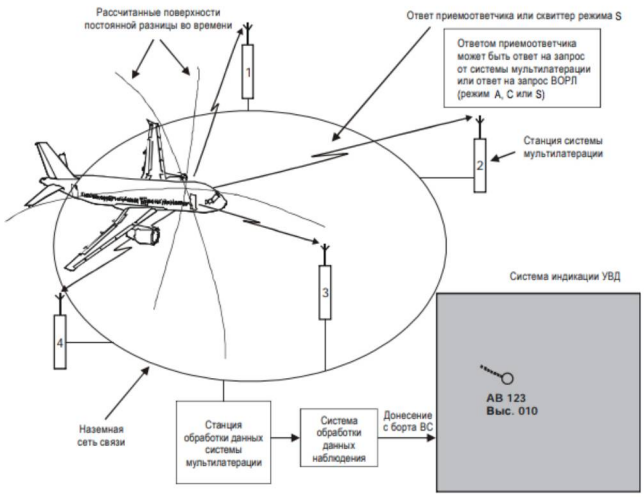


Рис. 4 — Типичная архитектура системы MLAT для наблюдения в целях УВД

Основной идеей использования данного метода в задаче валидации сообщений АЗН-В является сравнение информации полученной в сообщении АЗН с информацией полученной методом мультилатерации. Далее производится оценка истинности сообщений АЗН-В исходя из расстояния между транслируемым местоположением и расчетным. Для оценки были разработаны критерии истинности основанные на руководящих документах ИКАО и требованиям к системам ГНСС - так, если в полученном сообщении от АЗН-В передатчика указано положение для ВС, расстояние до которого от расчетного не превы-

шает величины двукратной ошибки АЗН-В (370 м), то информация о координатах объекта оценивается как достоверная.

Проанализированы технологии синхронизации времени наземных станций приема и дана оценка точности математических моделей, используемых при мультилатерации: метода наименьших квадратов (МНК) и метода рядов Тейлора - использование данных моделей необходимо при оценки местоположения ВС в условиях избыточного количества станций.

В случае с методом наименьших квадратов определение местоположения источника производится в соответствии с формулой 9. Элемепты вектора $\hat{X}$ - (x,y) являются координатами источника излучения, а (xi, yi) - заранее известные координаты базовой станции, где i = 1,2,3,..,M. M – конечное число наземных (базовых) станций (БС), принимающих участие в местонахождении источника излучения. Разности расстояний между базовыми станциями и источником сигнала определяются как:

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

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

$$D_1^2 - D_i^2 = 2D_1^2 d_{1i} - d_{1i}^2 \tag{3}$$

где c - скорость распространения электромагнитной волны, $d_{i,1}$ - TDOA (разность времени прихода) между i–ой базовой станцией и опорной. Выражение 3 можно переписать как

$$(x - x_1)(x_i - x_1) + (y - y_1)(y_i - y_1) + d_{1i}D_i = \frac{1}{2}\left[(x_i - x_1)^2 + (y_i - y_1)^2 - d_{1i}^2\right] \tag{4}$$

В матричной форме система уравнений выглядит следующим образом:

$$AX = b \tag{5}$$

Решением системы будет нахождение матрицы X, исходя из выражений 7 и 5:

$$A = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 & d_{21} \\ x_3 - x_1 & y_3 - y_1 & d_{31} \\ & \vdots & \\ x_m - x_1 & y_M - y_1 & d_{M1} \end{bmatrix} \tag{6}$$

$$X = \begin{bmatrix} x_s - x_1 & y_s - y_1 & D_1 \end{bmatrix}^T \tag{7}$$

$$b = \frac{1}{2}\begin{bmatrix} (x_2 - x_1)^2 + (y_2 - y_1)^2 - d_{21}^2 \\ (x_3 - x_1)^2 + (y_3 - y_1)^2 - d_{31}^2 \\ \vdots \\ (x_M - x_1)^2 + (y_M - y_1)^2 - d_{M1}^2 \end{bmatrix} \tag{8}$$

Производя линсйную аппроксимацию мстодом наимсньших квадратов получаем решение:

$$\hat{X} = arg\ \min_X (AX - b)^T (AX - b) = \left(A^T A\right)^{-1} A^T b = A^+ b \tag{9}$$

В случае метода рядов Тейлора происходит итеративное определение местоположения исходя из начального условия. Обладая множеством накопленных данных о разностях времен прихода, данный метод подразумевает использование начального приближения и вычисляет отклонение оценки определения местоположения. Выражение 2 может

быть переписано как функция

$$f_i(x,y) = \sqrt{(x - X_{i+1})^2 + (y - Y_{i+1})^2} - \sqrt{(x - X_1)^2 + (y - Y_1)^2} \tag{10}$$

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

$$f_i(x,y) = d_{i+1,1} + \epsilon_{i+1,1} \tag{11}$$

где

$$d_{i+1,1} = c \cdot (t_{i+1} - t_1) \tag{12}$$

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

$$x = x_0 + \delta_x; y = y_0 + \delta_y \tag{13}$$

Разложив выражение 10 в ряд Тейлора, получаем:

$$f_{i,0} + a_{i,1}\delta_x + a_{i,1}\delta_y \approx d_{i+1,1} + \epsilon_{i+1,1} \tag{14}$$

$$\begin{cases} f_{i,0} = f_i \cdot (x_0,y_0) \\ a_{i,1} = \left.\dfrac{\partial f_i}{\partial x}\right|_{x_0,y_0} = \frac{X_1 - x_0}{d_1} - \frac{X_{i+1} - x_0}{d_{i+1}} \\ \widehat{d_i} = \sqrt{(x_0 - X_i)^2 + (y_0 - Y_i)^2} \\ a_{i,2} = \left.\dfrac{\partial f_i}{\partial x}\right|_{x_0,y_0} = \frac{Y_1 - y_0}{d_1} - \frac{Y_{i+1} - y_0}{d_{i+1}} \end{cases} \tag{15}$$

Соотношение 14 может быть переписано в матричном виде:

$$A\delta = D + \epsilon \tag{16}$$

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \\ \vdots & \vdots \\ a_{N-1,1} & a_{N-1,2} \end{bmatrix};\ \delta = \begin{bmatrix} \delta_x \\ \delta_y \end{bmatrix};\ D = \begin{bmatrix} \widehat{d_{2,1}} - f_{1,0} \\ \widehat{d_{3,1}} - f_{2,0} \\ \vdots \\ \widehat{d_{N,1}} - f_{N-1,0} \end{bmatrix};\ \epsilon = \begin{bmatrix} \epsilon_{2,1} \\ \epsilon_{3,1} \\ \vdots \\ \epsilon_{N,1} \end{bmatrix}. \tag{17}$$

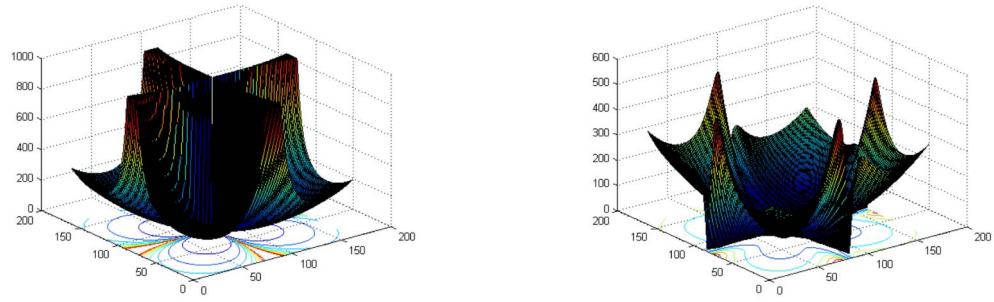
$$\delta = [A^T R^{-1} A]^{-1} \cdot A^T R^{-1} D \tag{18}$$

где R - ковариационная матрица ошибок, определяемая как

$$R = M(\epsilon) \cdot \begin{bmatrix} 1 & \cdots & 0.5 \\ \vdots & \ddots & \vdots \\ 0.5 & \cdots & 1 \end{bmatrix} \tag{19}$$

Итерации продолжаются до тех пор, пока девиация x и y не станет пренебрежительно малой.

Так по результатам проведенного имитационного моделирования, при условии равноудаленности наземных станций друг от друга, было определено что при 4-х НС ошибки МНК в несколько порядков превышают аналогичные ошибки при определении МП методом рядов Тейлора (Рис. 5).



а) б)

Рис. 5 — Поверхность ошибок (СКО, м) при 4-х БС для МНК (а) и метода рядов Тейлора (б)

Общие выводы по различным методам мультилатерации приведены в заключении.

Методы машинного обучения, а именно классификационные алгоритмы, позволяют отделить ложные сообщения, сгенерированные в рамках несанкционированного вмешательства, от истинных сообщений.

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 диссертационной работе будет именоваться **монолатерацией**. Основная идея монолатерации заключается в том, чтобы на основе большого массива данных отнести каждое поступающее сообщение к одному из двух классов: «ложь» либо «истина». При этом на вход системы поступает вектор признаков сообщения АЗН, такой как мощность сигнала, координаты, высота и т.д. Задача алгоритмов отнести набор признаков к одному из классов. Всего рассматривалось четыре популярных метода машинного обучения – адаптивный бустинг (AdaBoost), градиентный бустинг (LightGBM), метод K-ближайших соседей и наивный байесовский классификатор.

Современные алгоритмы машинного обучения зачастую представлены в виде ансамблей, содержащих базовые модели классификации, такие как решающие деревья. 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, отнесящимся к данному листу. 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, предсказывающая функция дерева определяется так:

$$f(x) = \sum_{m=1}^{M} c_m I(x, R_m) \tag{20}$$

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.

Принцип металгоритма бустинга представлен на рисунке 6.

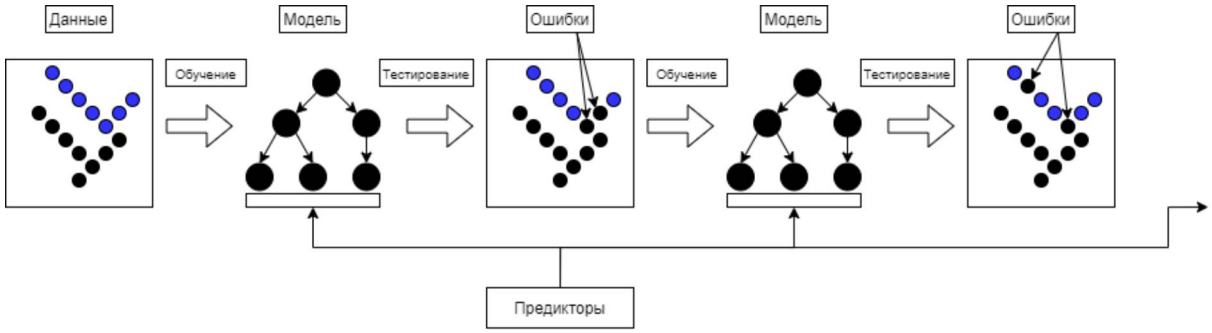


Рис. 6 — Принцип работы алгоритма бустинга

Для определения эффективного алгоритма машинного обучения по выявлению несанкционированных сообщений АЗН в данной работе использовалась следующая последовательность: получение обучающей выборки, разбиение обучающей выборки на несколько частей, отбор полезных признаков с использованием алгоритмов решающих деревьев, настройка параметров модели обучения (глубина деревьев, количество итераций), оценка модели на тестовой выборке с использованием различных метрик - Accuracy, precision, recall и AUC-ROC.

Рис. 7 — Схема процесса определения оптимального алгоритма машинного обучения

Третья глава посвящена практическому применению методов и алгоритмов валидации сообщений системы АЗН-В.

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. Приведем гибридный алгоритм валидации сообщений на Рис. 8

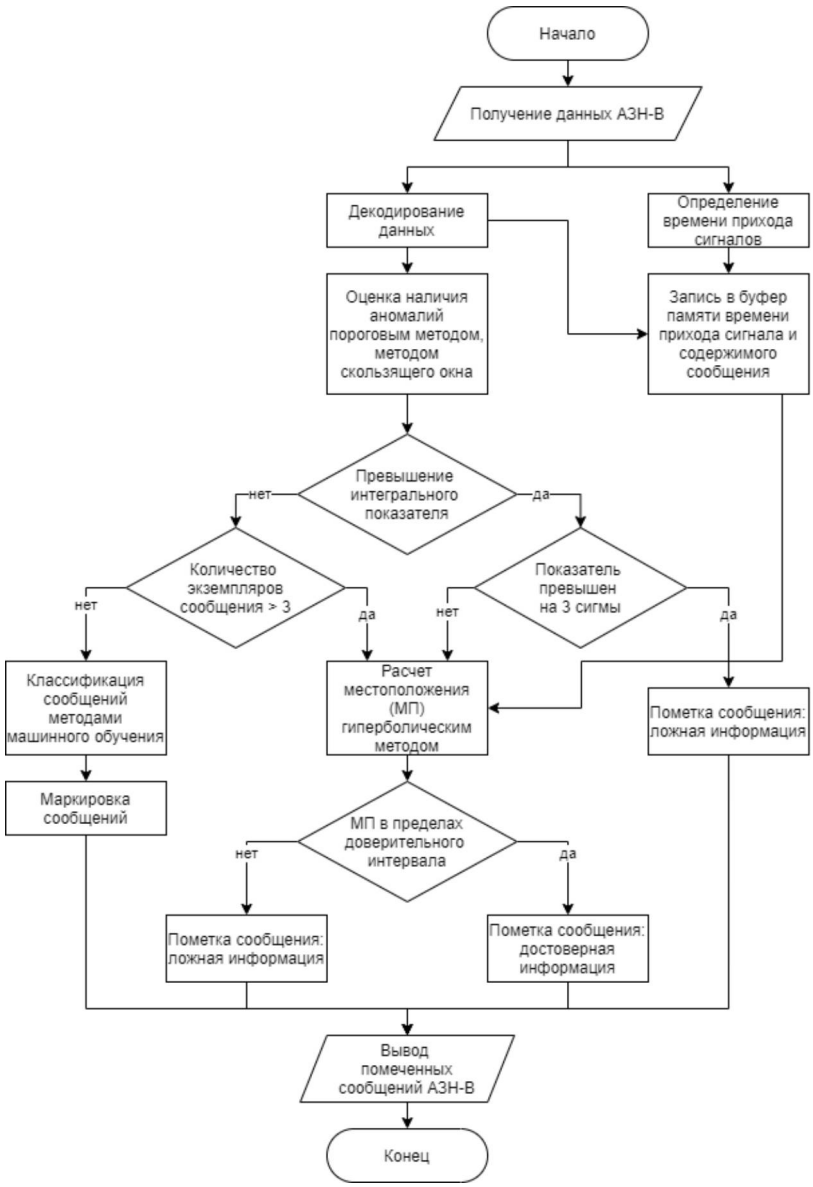


Рис. 8 — Гибридный алгоритм определения местоположения судна в условиях несанкционированного вмешательства

Полученный алгоритм может быть использован при построении 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 масштабирования ресурсов микросервисов.

Рис. 9 — Облик системы анализа и фильтрации сообщений АЗН-В при использовании одной станции приема

Разрабатываемая система может быть реализована согласно Рис. 10.

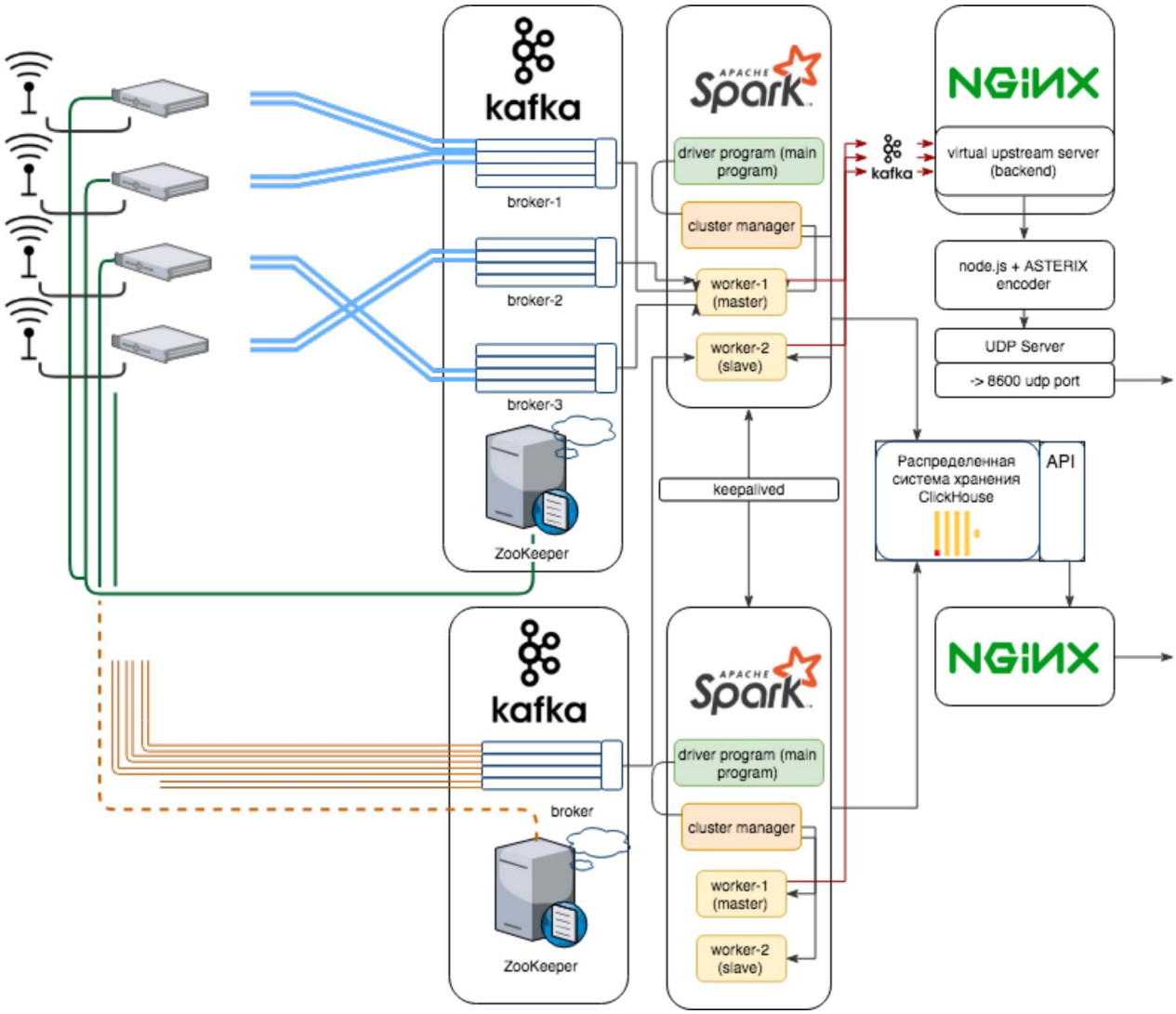


Рис. 10 — Схема прохождения информационных потоков через ключевые микросервисы системы

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. 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. 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).

В **четвертой главе** была апробирована система анализа и фильтрации сообщений АЗН-В, реализован натурный эксперимент несанкционированного вмешательства, направленный на оценку эффективности предложенных методов валидации.

Для моделирования ситуации несанкционированного вмешательства были рассмотрены два сценария проведения атаки - с использованием реальных данных АЗН-В и при генерации сообщений АЗН. Для проведения эксперимента было осуществлено: получение реальных данн АЗН-В, подмешивание ложных данных, оценка эффективности валидации. Диаграмма процесса моделирования представлена на рисунке 11

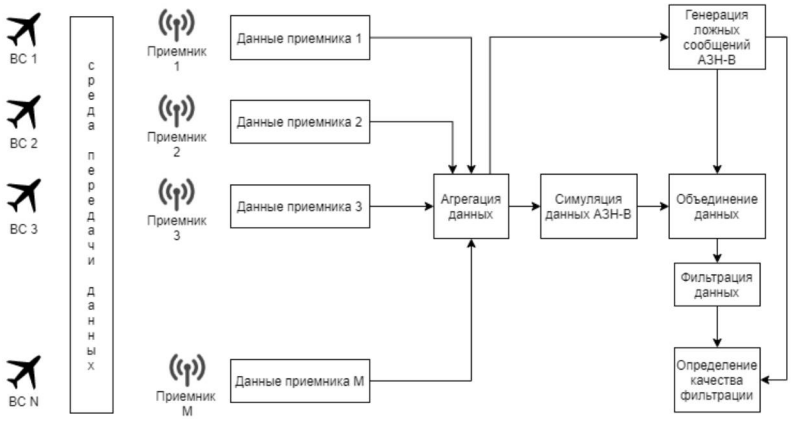


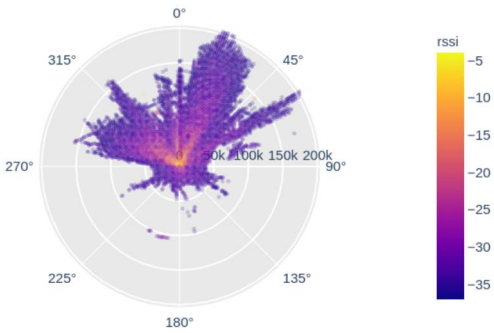
Рис. 11 — Моделирование несанкционированного вмешательства с использованием реальных полетных данных

Для реализации задачи сбора информации на основе программно-определяемой радиосистемы (SDR) на базе чипов RTL2832U+R820T2 за период с 2020.11.05 по 2020.11.28 было собрано 20 млн. сообщений АЗН-В.

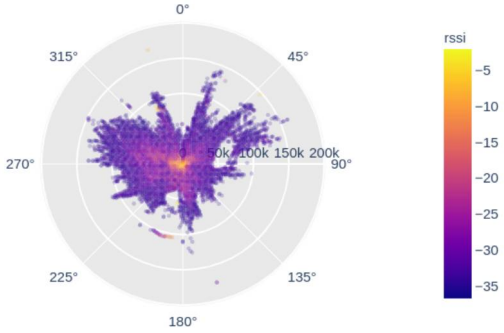
На Рис. 12 представлены полярные диаграммы приема сигналов АЗН-В. Данные диаграммы отражают общую картину мощности принимаемого сигнала за месяц наблюдений – по координатам полученных сообщений рассчитывался пеленг и дальность, для полученной точки на диаграмме рассчитывался усредненный уровень принимаемого сигнала (rssi).

Затем, для реализации задачи обучения, производилось «подмешивание» ложных данных к истинным и их маркировка. При проведении несанкционированного вмешательства использовалась программно-управляемая система HackRF One (Рис. 13а) расположенная в непосредственной близости от приемника (Рис. 13б). Мощность передатчика HackRF One составляет 20мВт, КПД используемой штырьковой антенны - 1%, что, учитывая чувствительность действующих станций в -95дБм не представляет угрозы для УВД - по расчетам МСЭ-R P.525 испускаемый сигнал не может быть детектирован действующими станциями на растоянии более 490 метров.

Атака производилась двух типов: генерация ложных данных исходя из модели движения ВС (моделируемые параметры) и полное повторение сигналов (дублирование реальных данных), полученных с другой станции приема (Рис. 14).



а) Внутри помещения



б) Вне помещения

Рис. 12 — Диаграммы уровня принимаемого сигнала для приемных устройств, размещенных в различных условиях. Период наблюдений - 2021.01.04 - 2021.01.24

а) Оборудование для передачи ложных сообщений АЗН-В

б) Оборудование для получения сообщений АЗН-В

Рис. 13 — Оборудование приема и передачи сообщений АЗН-В

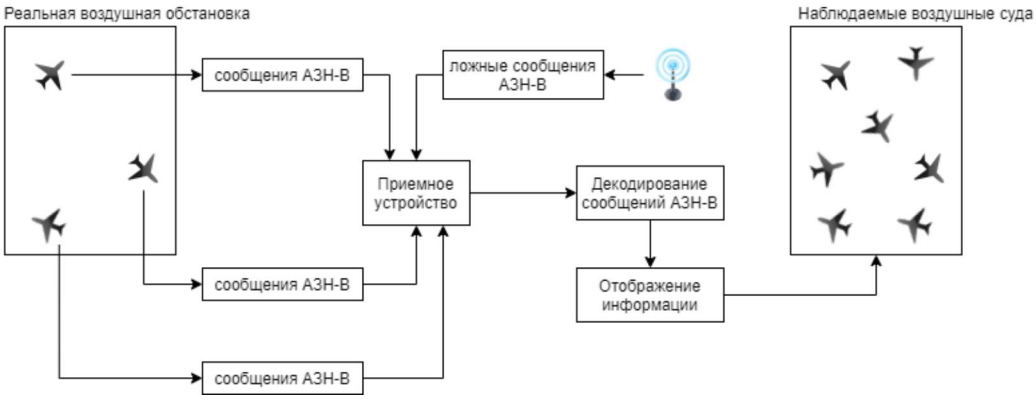


Рис. 14 — Схема постановки эксперимента атаки повторения сигналов АЗН-В

Для упрощения, для реализации атаки второго типа, сообщения «подмешивались» в конечную базу данных без их передачи в эфир. На основе проведенного эксперимента удалось установить наиболее весомые признаки сообщения АЗН-В, результаты представлены на Рис. 15

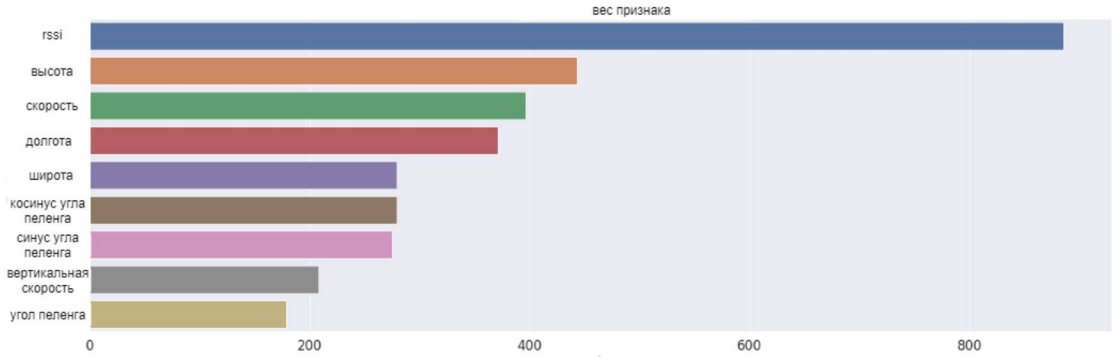


Рис. 15 — Вклад признаков при классификации сообщений АЗН-В

Результаты проведенного эксперимента по классификации сообщений АЗН при несанкционированном вмешательстве позволили составить сравнительную характеристику точности классификации различных алгоритмов по разным типам атак. Для атаки с моделируемыми параметрами (злоумышленник пытается повторить физические показатели распространения сигнала) результаты эксперимента выглядят следующим образом:

Метод	Ошибка I рода	Ошибка II рода	Точность, %
Мстод К-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

Таблица 1

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

Для атаки с полным «воспроизведением» уровня принимаемого сигнала результаты следующие:

Метод	Ошибка I рода	Ошибка II рода	Точность, %
Метод К-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

Таблица 2

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

Наиболее точными классификационными алгоритмами машинного обучения, согласно поставленному эксперименту, являются метод К-ближайших соседей и градиентный бустинг. Ожидаемо подтвердилась высокая эффективность метода монолатерации при несанкционированном вмешательстве с моделируемыми параметрами вероятность

корректной классификации составила (P=0.995), но что неожиданно, при атаке с повторением сигналов АЗН-В, метод монолатерации также показал сопоставимо высокие результаты при использовании метода К-ближайших соседей (P=0.9165).

В **заключении** приведены основные результаты работы, которые состоят 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 К-ближайших соседей, градиентный бустинг (LightGBM), адаптивный бустинг (AdaBoost) и на-

ивный 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 работ, опубликованных автором по теме диссертации

В рецензируемых научных изданиях, рекомендуемых ВАК РФ (по транспорту):

1. Машошин А. О. Вопросы избыточности в задаче определения местоположения воздушного судна разностно-временным методом // Научный Вестник МГТУ ГА. — 2016. — No 224. — С. 147—157.
2. 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. — No 37. — С. 136—145.

***В материалах тезисов докладов**, сделанных на международных и всероссийских научно технических и научно практических конференциях:*

1. Машошин А.О., «Актуальные угрозы АЗН-В и методы противодействия» / Гражданская авиация на современном этапе развития науки, техники и общества / Международная научно-техническая конференция, посвященная 45-летию Университета. Сборник тезисов докладов. -Москва., -2016.
2. Машошин А.О., «АЗН-В как новый тип аэронавигационного наблюдения. Проблемы безопасности и пути снижения угроз посредством измерения физических характеристик системы» / XIII Всероссийское совещание -семинар «Инженерно-физические проблемы новой техники МГТУ им. Н.Э. Баумана. Сборник докладов. - Москва., -2018.
3. Петров В.И., Машошин А.О., Машошин Н.О., «Практическое применение методов машинного обучения в задаче определения истинности сообщений системы автоматического зависимого наблюдения» / Гражданская авиация на современном этапе развития науки, техники и общества» / Международная научно-техническая конференция, посвященная 50-летию Университета. Сборник тезисов докладов. -Москва., -2021.

Соискатель: