



**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА  
(РОСАВИАЦИЯ)**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ  
ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ  
АВИАЦИИ» (МГТУ ГА)**

**ФАКУЛЬТЕТ** Авиационных Систем и Комплексов

**КАФЕДРА** Основ радиотехники и защиты информации

**Направление подготовки** 25.06.01 Аэронавигация и эксплуатация  
(код и наименование направления подготовки)  
авиационной и ракетно-космической техники

**Направленность** 05.22.13 Навигация и управление воздушным движением  
(наименование направленности)

**НАУЧНО-КВАЛИФИКАЦИОННАЯ РАБОТА**

**Тема** Методы и алгоритмы обнаружения несанкционированного  
вмешательства в сетях передачи данных систем управления воздушным  
движением

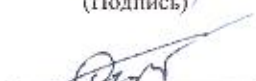
**Обучающийся:**

Ганичев А.А.  
(Ф.И.О.)

  
(Подпись)


**Научный руководитель:**

к.т.н., доцент, Окулесский В.А.  
(уч. степень, уч. звание, Ф.И.О.)

  
(Подпись)

**Рецензенты:**

д.т.н., профессор Болелов Э.А.  
(уч. степень, уч. звание, Ф.И.О.)

  
(Подпись)


д.т.н., профессор, Кузнецов С.В.  
(уч. степень, уч. звание, Ф.И.О.)

  
(Подпись)

**Работа допущена к защите:**

**Заведующий кафедрой**

к.т.н., доцент, Петров В.И.  
(уч. степень, уч. звание, Ф.И.О.)

  
(Подпись)

**МОСКВА 2025**

## ВВЕДЕНИЕ

**Актуальность темы исследования.** Авиационная отрасль характеризуется высокой степенью сложности, поскольку состоит из множества взаимодействующих компонентов, таких как управление воздушным движением (УВД) с различными системами связи, навигации и наблюдения. Системы связи обычно содержат устройства, которые облегчают обмен информацией (например, командами, голосом и другой информацией данных) между устройствами, системами и пользователями (например, диспетчерской службой УВД и пилотом). Проблема обеспечения защиты от несанкционированного вмешательства (НСВ) в авиации усугубляется большим трафиком воздушного движения, отчего она становится все более важной, поскольку все больше устройств и систем переводятся в цифровую форму и подключаются ко многим службам и коммуникациям, осуществляемым по беспроводной сети.

Посредством постоянного совершенствования сетевой инфраструктуры, новые технологии, такие как облачные вычисления, большие данные и искусственный интеллект, постоянно применяются в различных информационных системах УВД.

Учитывая значительный рост количества рейсов за последнее десятилетие, традиционные системы организации воздушного движения (ОрВД) испытывают трудности с предоставлением актуальной и достоверной информации о состоянии воздушного судна. В результате авиационное сообщество активно предпринимает шаги по повышению безопасности, пропускной способности и гибкости полетов, а также по снижению зависимости от устаревшей инфраструктуры путем изучения и совершенствования национальных систем воздушного пространства. Вместе с тем, в последние годы исследования указывают на недостатки в проектировании и внедрении бортовых систем и продемонстрировали, как некоторые основные бортовые системы можно взломать, просто используя готовое коммерческое оборудование и программное обеспечение (ПО).

Современные воздушные суда и наземные сегменты управления активно переходят на цифровые каналы связи и стандартные сетевые технологии. Уровень зависимости авиационной инфраструктуры от стабильной и надёжной работы сетей передачи данных постоянно растёт. На этом фоне усиливаются риски несанкционированного вмешательства в работу систем, обеспечивающих передачу критических сообщений и управление воздушным движением.

Европейский регламент EASA 2023/203 напрямую связывает такие воздействия с угрозами безопасности полётов. Документ устанавливает обязательные требования к обнаружению событий, которые могут привести к опасным отклонениям в функционировании технических средств. Это подчёркивает необходимость разработки решений, способных выявлять признаки внешнего вмешательства в телекоммуникационной среде авиационного назначения.

Задача усложняется особенностями авиационных сетей: высокой критичностью ошибок, ограниченными вычислительными ресурсами, спецификой используемых протоколов, ограничением доступа к тестовым данным. Эти факторы требуют создания специализированных подходов, адаптированных к условиям отрасли.

Однако, методических материалов по защите СПД систем УВД от НСВ недостаточно. Сильная зависимость от ИТ-средств для поддержания качества услуг привела к более высокому уровню подверженности НСВ на авиационные сети передачи данных. Существует острая необходимость в обеспечении высокого уровня защиты авиационных сетей передачи данных от НСВ из-за роста объемов воздушного движения и увеличения числа цифровых систем, что определяет **противоречие практического характера**. Существующие методы и средства защиты часто оказываются недостаточными или неэффективными в условиях быстро развивающихся методов НСВ, что в свою очередь определяет **противоречие научного характера**. Возникает противоречие между необходимостью использования передовых технологий (таких как искусственный

интеллект и машинное обучение) и недостаточной изученностью их применения в авиационных системах. Сказанное определяет **актуальность работы**, посвященной разработке эффективной и не требующей значительных финансовых вложений методики по обеспечению безопасности авиационных сетей передачи данных. Для разрешения сформулированных противоречий практического и научного характера в диссертации решается актуальная **научно-техническая задача** противодействия несанкционированному вмешательству в функционирование информационных сетей передачи данных систем управления воздушным движением, требующая разработки на основе единого научно-методического аппарата методов и алгоритмов повышения уровня безопасности сетей передачи данных на воздушном транспорте.

**Объект исследований** – Подсистема телекоммуникаций АС УВД.

**Предмет исследований** – Методы и алгоритмы обнаружения несанкционированного вмешательства в информационно-вычислительных процессах подсистемы телекоммуникаций АС УВД.

**Проблема и её актуальность.** Проблема заключается в острой необходимости в обеспечении высокого уровня защиты авиационных сетей передачи данных ТКС АС УВД от НСВ из-за роста объемов воздушного движения и увеличения числа цифровых систем, что определяет **противоречие практического характера**. Существующие методы и средства защиты часто оказываются недостаточными или неэффективными в условиях быстро развивающихся методов НСВ, что в свою очередь определяет **противоречие научного характера**. Возникает противоречие между необходимостью использования передовых технологий (таких как искусственный интеллект и машинное обучение) и недостаточной изученностью их применения в авиационных системах.

**Гипотеза.** Предполагается, что разработка адаптированных для ТКС АС УВД методов и алгоритмов будет способствовать повышению уровня безопасности полетов.

**Целью** диссертационного исследования является решение научной задачи повышения уровня безопасности полетов за счёт разработки методов и алгоритмов обнаружения несанкционированного вмешательства в телекоммуникационной подсистеме АС УВД, имеющих существенное значение для развития авиационной отрасли.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Проанализировать состояние и актуальные проблемы защиты телекоммуникационной подсистемы автоматизированной системы управления воздушным движением от несанкционированного вмешательства и выявить направления, требующие разработки новых методов обнаружения;

2. Исследовать применимость существующих методов и моделей защиты, выявить ограничения традиционных подходов и обосновать необходимость использования интеллектуальных методов анализа информационного обмена с учётом специфики авиационной инфраструктуры;

3. Разработать методы и алгоритмы обнаружения НСВ в телекоммуникационной подсистеме АС УВД на основе анализа признаков информационного обмена, компактного представления данных и корреляции взаимосвязанных событий;

#### **Научная новизна работы.**

1. Предложен метод выявления признаков НСВ на основе анализа частых наборов признаков информационного обмена в телекоммуникационной подсистеме АС УВД.

2. Предложен метод компактного хранения и обработки больших объёмов данных о процессе информационного обмена в телекоммуникационной подсистеме АС УВД.

3. Предложены алгоритмы анализа и корреляции взаимосвязанных событий НСВ в телекоммуникационной подсистеме АС УВД.

**Теоретическая и практическая значимость.** При выполнении работы получены теоретические положения и алгоритмы, которые легли в основу конкретных методов, формирующих базу для дальнейших исследований в области

защиты от НСВ воздушного транспорта. Полученные результаты имеют потенциал для внедрения в реальных условиях, что позволит совершенствовать меры по защите объектов ВТ от НСВ в авиационную деятельность.

#### **Положения, выносимые на защиту:**

1. Метод выявления признаков несанкционированного вмешательства на основе анализа частых наборов признаков сетевого трафика телекоммуникационной подсистемы АС УВД.
2. Метод компактного хранения и обработки больших объёмов данных о сетевом трафике телекоммуникационной подсистемы АС УВД.
3. Алгоритмы анализа и корреляции событий несанкционированного вмешательства в телекоммуникационной подсистеме АС УВД.

Научно-квалификационная работа состоит из введения, четырех глав и заключения.

В первом разделе рассматривается проблема перехода авиационных систем от аналоговой голосовой связи к цифровым технологиям передачи данных. Современное развитие информационных технологий оказывает значительное влияние на трансформацию авиационной связи, направленную на решение актуальных проблем голосовой радиосвязи и совершенствование системы УВД, известной также как Air Traffic Management (ATM) и Air Traffic Control (ATC). Программа «LINK 2000+», запущенная Европейской организацией по безопасности аэронавигации (EUROCONTROL) в 2001 году, представляет собой комплекс стандартов для интеграции технологий передачи данных в воздушном пространстве Европы, что указывает на стремление к стандартизации и повышению эффективности цифровой инфраструктуры в авиации. Прогнозируемые изменения в системе связи предполагают увеличение объёмов передаваемых данных и числа подключений, что увеличивает потенциальные векторы атак и требует разработки новых подходов к обнаружению НСВ. На рисунке 1.1 представлены ключевые аспекты прогнозируемой структуры авиационной связи [33-35].

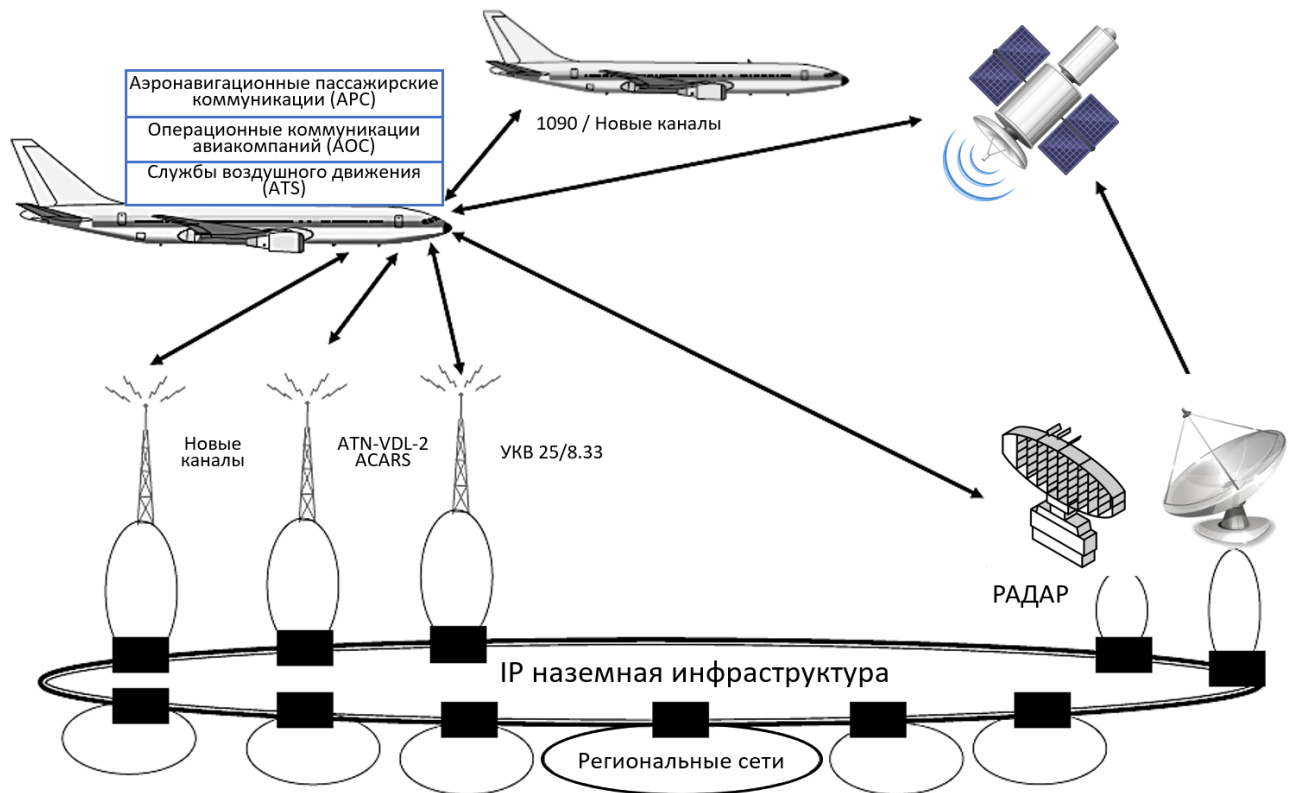


Рисунок 1.1. – Прогнозируемая структура авиационной связи

Проводится анализ современных стандартов авиационной связи, включая ACARS, ATN, SATCOM, а также программных и аппаратных решений (COTS-продукты, IP-сети).

Проведен анализ ключевых вызовов, связанных с увеличением объёма трафика, перегрузкой радиочастотного спектра и внедрением новых сервисов (например, In-Flight Connectivity).

Рассмотрены архитектурные особенности телекоммуникационной подсистемы АС УВД. АС УВД выполняет автоматизированную обработку следующих информационных потоков, обеспечивая выполнение её ключевых функций в интересах управления воздушным движением:

1. приём, агрегирование и отображение координатных и идентификационных данных о воздушной обстановке, поступающих от радиолокационных систем и средств автоматического зависимого наблюдения;

2. обработка и распределение плановой информации о траекториях полётов на основе сопряжения с каналами автоматизированной фиксированной электросвязи;

3. сбор и ретрансляция метеорологических данных с наземных и бортовых источников в интересах сопровождения воздушных судов;

4. анализ текущей и прогнозной обстановки для обеспечения эшелонирования, выделения безопасных маршрутов и разрешения потенциально конфликтных ситуаций;

5. интеграция информации о текущем положении и прогнозах траекторий для выявления нарушений норм эшелонирования и возможных отклонений от допустимых параметров полёта;

6. автоматизированное взаимодействие с другими сегментами АС УВД и смежными автоматизированными системами (в том числе системами ведомственной авиации);

7. обеспечение документирования событий, формирование архивов и воспроизведение последовательности обмена в целях последующего анализа или расследования инцидентов;

8. поддержка учебно-тренировочного режима функционирования в интересах подготовки и проверки квалификации диспетчерского состава.

Рассмотрены случайные и преднамеренные воздействия в информационно-вычислительный процесс АС УВД. Рассмотрены основные составляющие факторы информационной безопасности АС УВД.

Предложена классификация атак на информационно-вычислительные процессы АС УВД. Предлагаемая классификация [91], показанная на рисунке 1.6, использует четыре различных показателя:

1. Возникновение;
2. Характер нападения;
3. Цель;
4. Атрибуты безопасности «Затронутые»



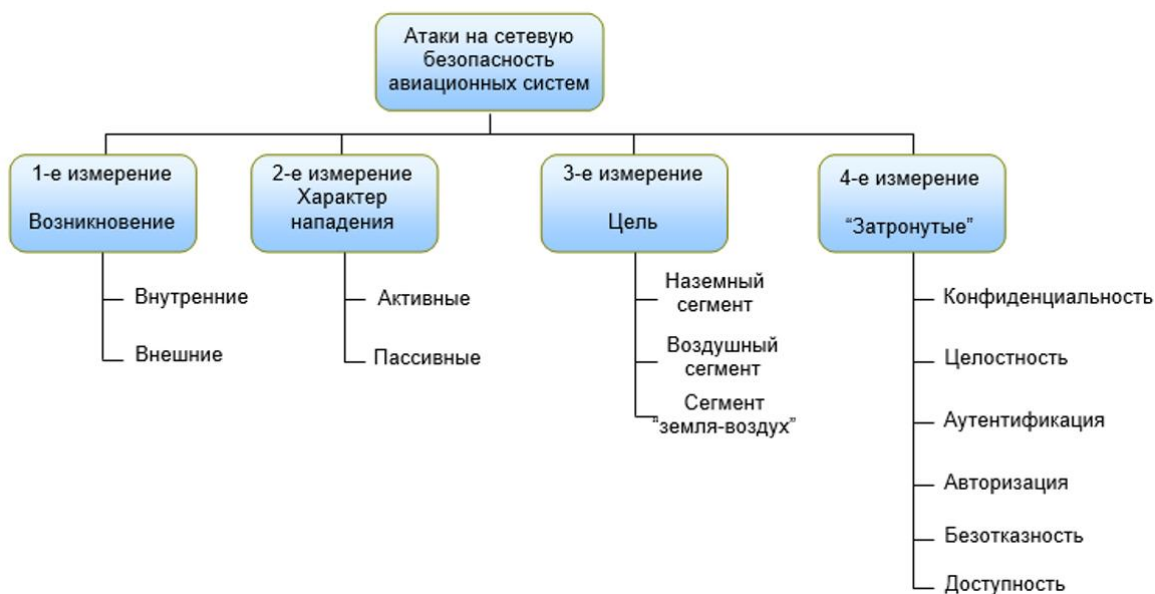


Рисунок 1.6. – Классификация атак на сетевую безопасность в авиационных СПД.

Представлена сравнительная таблица атак на ТКС АС УВД.

Во втором разделе осуществляется анализ моделей защиты ТКС АС УВД, основанные на разграничении доступа и криптографических средствах. Разработана математическая модель угроз АС УВД в условиях несанкционированного вмешательства. Модель позволяет описать вероятностные характеристики отказов компонентов и целенаправленных атак, а также количественно оценить их влияние на связность сети. Предложенный подход дает возможность выявить критичные узлы и каналы (наиболее уязвимые с точки зрения потери связности) и учесть эффективность их мониторинга – показано, что повышение вероятности обнаружения атак при одновременном снижении ложных срабатываний существенно уменьшает общий риск нарушения работы сети. Модель является основой для обоснованного выбора и оптимального распределения средств защиты: она позволяет ранжировать угрозы по степени влияния и сконцентрировать защитные меры на наиболее значимых элементах сети, минимизируя вероятность успешных атак.

Рассмотрены основные методы и алгоритмы машинного обучения в задаче обнаружения НСВ на сети АС УВД. Установлено, что ни традиционные методы

классификации и кластеризации, ни прямое применение подходов поиска паттернов не обеспечивает полной эффективности решения задачи обнаружения НСВ в условиях авиационной СПД. Это объясняется как жёсткими требованиями реального времени и надёжности, так и непредсказуемостью возможных сценариев атак.

В третьем разделе произведена разработка методов и алгоритмов обнаружения НСВ в СПД АС УВД. Зафиксированные события описываются в виде векторов признаков:

$$x_i = \{a_1^{(i)}, a_2^{(i)}, \dots, a_m^{(i)}\}, i = 1, 2, \dots, N \quad (1)$$

На выходе получается нормализованная последовательность, пригодная для анализа:

$$\tilde{X} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N\} \quad (2)$$

Формально структура данных представляется как дерево (см. п. 2.2) На основе построенного дерева выделяется множество частых многомерных шаблонов:

$$P = \{p_j \subseteq \tilde{x}_i \mid \text{support}(p_j) \geq \theta_S\} \quad (3.4)$$

где  $\theta_S$  — минимальный порог поддержки. Эти шаблоны отражают устойчивые сочетания признаков, характерные для НСВ в СПД.

Каждому паттерну  $p_j$  из множества  $P$  сопоставляется ассоциативное правило вида  $A \Rightarrow B$ , для которого рассчитываются метрики эффективности:

- поддержка:  $\text{support}(A \Rightarrow B)$
- достоверность (confidence):  $\text{conf}(A \Rightarrow B) = \frac{\text{count}(A \cup B)}{\text{count}(A)}$
- оценка степени интереса методом измерения степени нормы:

$$\text{Lift}(A \Rightarrow B) = \frac{\text{support}(A \cup B)}{\text{support}(A) \cdot \text{support}(B)} \quad (3.5)$$

Разработка реализует последовательную обработку сетевого трафика для выявления устойчивых сочетаний признаков с последующей генерацией

ассоциативных правил. Таким образом, предложены алгоритмы анализа и корреляции взаимосвязанных событий НСВ в СПД телекоммуникационной подсистемы АС УВД, отличающиеся от существующих за счёт использования устойчивых сочетаний признаков, выявленных методом многомерного анализа, и совокупной обработки частотных и временных характеристик сетевых событий.

В четвертом разделе реализована система обнаружения НСВ в информационно-вычислительных процессах АС УВД на основе предложенных методов и алгоритмов. Проведена апробация разработанной системы и сравнительный анализ эффективности с современными методами машинного обучения, доказана эффективность предлагаемых методов и алгоритмов.

Основные результаты научно-квалификационной работы сводятся к следующему:

В работе проведен анализ проблем обеспечения защиты информационно-вычислительных процессов АС УВД от несанкционированного вмешательства.

Исследованы современные методы машинного обучения в задаче обнаружения НСВ в АС УВД, показавшие необходимость разработки новых методов и алгоритмов.

Предложены оригинальные методы и алгоритмы обнаружения НСВ в АС УВД. Показана эффективность предложенных методов и алгоритмов.