ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

На правах рукописи

Ганичев Александр Александрович

МЕТОДЫ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОГО ВМЕШАТЕЛЬСТВА В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ СИСТЕМ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

Специальность: 2.9.6. Аэронавигация и эксплуатация авиационной техники

Диссертация

на соискание ученой степени

кандидата технических наук

Научный руководитель

Кандидат технических наук, доцент,
Петров Виктор Иванович

Москва - 2026

Содержание

Введение

Актуальность темы исследования. Авиационная отрасль представляет собой сложную систему, в которой взаимодействуют средства связи, навигации и наблюдения, объединённые в системе управления воздушным движением (УВД). Функционирование основано на информационном обмене между воздушным судном (ВС) и наземными системами УВД, обеспечивающем согласованное взаимодействие элементов в рамках единой среды управления.

Процессы УВД связаны с передачей значительных объёмов служебных данных, необходимых для обеспечения безопасного и эффективного выполнения полётов. Рост интенсивности полётов приводит к увеличению нагрузки на системы связи и обработки информации, а также повышает требования к достоверности и доступности передаваемых данных.

Развитие авиационной инфраструктуры сопровождается переходом на цифровые каналы связи и внедрение сетей передачи данных (СПД). Это приводит к тому, что передача служебных сообщений и команд между диспетчером УВД и экипажем ВС осуществляется в цифровой форме вместо традиционной голосовой радиосвязи, а функционирование систем УВД становится зависимым от устойчивости каналов связи и корректности сетевого информационного обмена.

В этих условиях возможны нарушения информационного обмена, связанные с несанкционированным вмешательством (НСВ). Такие воздействия могут проявляться как на уровне отдельных компонентов, так и на уровне их взаимодействия, что приводит к искажению или задержке передаваемых данных и влияет на процессы УВД.

Международные нормативы напрямую связывают информационное воздействие с безопасностью полётов. Так, европейский регламент EASA 2023/203 устанавливает обязательные требования по обнаружению событий, способных привести к опасным отклонениям в работе авиационных систем, подчёркивая

необходимость разработки решений для выявления признаков НСВ в телекоммуникационной среде авиации.

На национальном уровне вопросам защиты авиационных коммуникаций также уделяется серьезное внимание. К объектам, подлежащим защите от НСВ, отнесены технические средства связи и каналы передачи данных, задействованные в работе воздушного транспорта. Кроме того, Постановление Правительства РФ № 1701 прямо регламентирует оснащение беспилотных авиационных систем (БАС) и пилотируемых ВС линиями управления, каналами связи и средствами криптографической защиты; эти линии управления функционируют через наземные пункты управления и станции контроля; для пилотируемых ВС устанавливается требование наличия бортовых систем связи и навигации, согласованных с наземными системами ОрВД.

Среди факторов, влияющих на возможность реализации НСВ в авиационную деятельность, следует отметить зависимость систем УВД от сетевого взаимодействия, использование стандартных протоколов передачи данных и ограниченные возможности изменения существующей инфраструктуры. Указанные особенности затрудняют применение общих методов информационной безопасности. Следовательно, противодействие НСВ в контуре УВД является актуальной проблемой, имеющей важное практическое значение для авиационной отрасли.

Таким образом, современный контур УВД охватывает как воздушный, так и наземный сегменты и предъявляет новые требования к безопасности каналов «воздух–земля». В рамках настоящего исследования под контуром УВД понимается система взаимодействия наземных автоматизированных систем управления воздушным движением (АС УВД), ВС и каналов цифрового информационного обмена, подверженная угрозам НСВ. Ранее системы УВД не рассматривались в виде единого контура, объединяющего наземные и бортовые компоненты, с точки зрения защиты от НСВ – данный подход реализуется впервые.

Степень разработанности темы.

Большой вклад в решение широкого круга теоретических и прикладных вопросов защиты объектов воздушного транспорта от НСВ в авиационную деятельность внесли Е.Ю. Зыбин, С.Ю. Желтов, В.В. Косьянчук, Н.И. Сельвесюк, Р.Н. Акиншин, В.И. Петров, А.О. Машошин, Э.Я. Фальков, С.С. Быбин, А.В. Никитин, А.М. Аршинов, Е.Л. Дружинин, Д.Г. Булатов, В.А. Педанов, В.В. Минин, М.С. Савельев, Д.С. Коптев, И.Е. Мухин, С.С. Карпенко, А.С. Овсянникова.

Тематика противодействия НСВ в авиационную деятельность так же широко освещена в работах зарубежных авторов R. Sampigethaya, E. Ukwandu, H. Whitworth, M. Wrana, R. Akram, L. Basora, P. Corretjer, G. Dave, T. Dubot, T. Pollard, A. Rahim.

Однако, несмотря на обширные исследования в области обнаружения и противодействия НСВ в авиационную деятельность, специализированных методических решений по защите контура УВД от НСВ, учитывающих специфику его цифровых каналов передачи данных, недостаточно. В настоящее время задача разработки методов и алгоритмов обнаружения НСВ в СПД контура УВД в целом не решена. Не решены в полном объёме, в частности, задачи разработки алгоритмов анализа частых признаков транзакций информационного обмена на предмет наличия НСВ. В ряде работ излагаются подходы, позволяющие эффективно решать отдельные частные задачи анализа отдельных сегментов СПД. Однако, эти подходы не обладают свойством системности и не адаптированы к изучению процессов функционирования контура УВД в условиях НСВ. Практически не существует решений, ориентированных на комплексное обнаружение НСВ в контуре УВД. Таким образом, вопросы разработки методов и алгоритмов обнаружения НСВ в контур УВД нуждаются в дальнейшем развитии.

Таким образом, формируется **противоречие практического характера**, связанное с необходимостью обеспечения устойчивого функционирования контура УВД в условиях возрастающей интенсивности полётов и внедрения цифровых каналов в системах УВД.

Существующие технологии искусственного интеллекта, применяемые для выявления признаков НСВ в реальном времени, как правило, не учитывают специфику функционирования контура УВД и ориентированы на использование предварительно размеченных наборов данных на этапе обучения. Это, в свою очередь, определяет **противоречие научного характера**, заключающееся в несоответствии между необходимостью внедрения методов обнаружения НСВ на основе технологий искусственного интеллекта и ограниченностью теоретической и практической базы их адаптации к условиям функционирования в контуре УВД.

Для разрешения сформулированных противоречий практического и научного характера в настоящем исследовании решается **актуальная научно-техническая задача** разработки методов и алгоритмов обнаружения НСВ в СПД систем УВД на основе технологий искусственного интеллекта.

Объект исследований – Контур УВД как система взаимодействия наземных систем АС УВД, ВС и каналов цифрового информационного обмена, подверженная угрозам НСВ.

Предмет исследований – Методы и алгоритмы обнаружения НСВ в контуре УВД.

Целью диссертационной работы является решение научной задачи разработки методов и алгоритмов обнаружения НСВ в сетях передачи данных систем УВД на основе технологий искусственного интеллекта, имеющей существенное значение для развития авиационной отрасли.

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

1. проанализировать состояние и актуальные проблемы обнаружения НСВ в контуре УВД, провести классификацию угроз и определить направления совершенствования;

2. на основе проведенного анализа разработать математические модели СПД в контуре УВД в условиях НСВ, описывающие структуру сети и характер вмешательства;

3. разработать методы и алгоритмы обнаружения НСВ в контуре УВД на основе разработанных математических моделей и технологий искусственного интеллекта, реализующих выявление вмешательства без этапа обучения;

4. произвести апробацию разработанных методов и алгоритмов и оценить их эффективность путём экспериментального исследования на моделируемых сценариях вмешательства, выполнить сравнительный анализ полученных результатов с известными решениями, предложить рекомендации по внедрению.

Научная новизна работы состоит получении следующих новых научных результатов.

1. Разработан метод многомерного анализа частых наборов признаков транзакций информационного обмена на основе технологий искусственного интеллекта, позволяющий сохранять структуру многомерных данных и выявлять устойчивые комбинации признаков информационного обмена, характерные для НСВ в контуре УВД.

2. Разработан метод формирования компактного представления транзакций информационного обмена в контуре УВД, что позволяет сократить объём памяти и вычислительных затрат при обработке больших массивов транзакций информационного обмена.

3. Разработаны алгоритмы классификации транзакций информационного обмена в контуре УВД, основанные на выявлении частых сочетаний признаков транзакций, позволяющие сформировать ассоциативные правила и выявлять шаблоны НСВ без этапа предварительного обучения.

4. Исследована эффективность методов и алгоритмов обнаружения НСВ в контуре УВД на основе технологий искусственного интеллекта, предложены рекомендации по внедрению в наземный и бортовой сегмент УВД.

Теоретическая и практическая значимость. Полученные научные результаты позволяют сформировать направления совершенствования существующих и разработки перспективных систем защиты от НСВ в телекоммуникационной инфраструктуре воздушного транспорта.

Методы исследования. При решении поставленных задач используются методы системного подхода, методы сравнительного и теоретико-аналитического анализа, технологии искусственного интеллекта, методы машинного обучения, методы интеллектуального анализа данных, методы выявления НСВ, методы корреляционного и статистического анализа, а также методы извлечения частых шаблонов в потоке информационного обмена.

Положения, выносимые на защиту:

1. Метод многомерного анализа частых наборов признаков транзакций информационного обмена в контуре УВД.

2. Метод формирования компактного представления транзакций информационного обмена в контуре УВД для последующего анализа НСВ.

3. Алгоритмы классификации транзакций информационного обмена в контуре УВД при НСВ.

4. Исследование эффективности методов и алгоритмов обнаружения НСВ в контуре УВД, рекомендации по внедрению в наземный и бортовой контур УВД.

Достоверность и обоснованность результатов, представленных в диссертации, подтверждается сравнением со статистическими данными, непротиворечивостью с ранее полученными результатами других авторов, а также соответствием практике противодействия несанкционированному вмешательству в контуре управления воздушным движением, апробацией полученных результатов в научных публикациях и докладах на конференциях.

Апробация работы. Основные результаты диссертационной работы обсуждались и были одобрены на следующих научных конференциях и семинарах:

1. Международной научно-технической конференции, посвященной 50-летию МГТУ ГА. Москва, 2021 г.

2. V Межвузовская конференция аспирантов, соискателей и молодых ученых (Москва, 18–19 апреля 2023 г.)

3. XXI Научно-техническая конференция «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского» 2024 г.

4. XXII Научно-техническая конференция «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского» 2025 г.

5. Международная научно-практическая конференция аспирантов и молодых ученых «Гражданская авиация в условиях глобальных изменений: наука и практика» 2025 г.

6. XXIII Научно-техническая конференция «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского» 2026 г.

Публикации. Список публикаций автора по теме диссертации включает 9 печатных изданий, 4 из которых (42 с.) в рецензируемых научных журналах из перечня ВАК при Минобрнауки, из них без соавторов – 1 статья; 1 (10 с.) научная статья в журнале, рецензируемом Scopus; 3 (22 с.) научных статей и тезисов, опубликованных в других изданиях и материалах конференций. Получено свидетельство о государственной регистрации программы для ЭВМ № 2025665933 от 25.07.2025.

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

– разработан метод многомерного анализа частых наборов признаков транзакций информационного обмена в контуре УВД на основе технологий искусственного интеллекта;

– разработан метод формирования компактного представления транзакций информационного обмена в контуре УВД для анализа НСВ;

– разработаны алгоритмы классификации транзакций информационного обмена в контуре УВД при НСВ;

– исследована эффективность методов и алгоритмов обнаружения НСВ в контуре УВД на основе технологий искусственного интеллекта, предложены рекомендации по внедрению в наземный и бортовой контур УВД.

Объём и структура диссертации. Диссертация изложена на 150 страницах, состоит из введения, четырёх разделов, заключения и содержит 36 рисунков и 9 таблиц. Список литературы содержит 105 источников.

Глава 1. Анализ состояния вопроса обеспечения защиты сетей передачи данных в контуре управления воздушным движением от несанкционированного вмешательства и постановка задачи исследования

1.1. Анализ технологий и сетей передачи данных в контуре управления воздушным движением

Контур УВД представляет собой совокупность каналов цифрового обмена между ВС, в том числе БАС, объектами наземной инфраструктуры воздушного транспорта и системами УВД, формируемую в рамках информационного взаимодействия в доменах аэронавигационного и оперативного контроля [1]. К числу объектов, подлежащих защите от НСВ, отнесены технические средства связи и каналы передачи данных, задействованные в работе воздушного транспорта [2]. В связи с активной интеграцией БАС в единое цифровое воздушное пространство, нормативные документы требуют оснащения пилотируемых ВС и БАС линиями управления и каналами связи. Эти линии функционируют через наземные пункты управления и должны обеспечивать надёжную связь с органами УВД. Таким образом, современный контур УВД предъявляет новые требования к безопасности каналов «воздух–земля» [3].

Современное развитие информационных технологий приводит к трансформации авиационной связи, направленной на решение актуальных проблем голосовой радиосвязи и совершенствование систем УВД. Программа «LINK 2000+», запущенная Европейской организацией по безопасности аэронавигации (EUROCONTROL) в 2001 году, представляет собой комплекс стандартов, обеспечивающих внедрение технологий передачи данных в воздушном пространстве Европы и направленных на повышение эффективности цифровой

инфраструктуры в авиации [4]. Прогнозируемые изменения в системе связи предполагают увеличение объёмов передаваемых данных, что увеличивает потенциальные векторы атак и требует разработки новых подходов к обнаружению НСВ в контуре УВД. На рисунке 1.1 представлена схема информационного взаимодействия в контуре УВД [5-6].

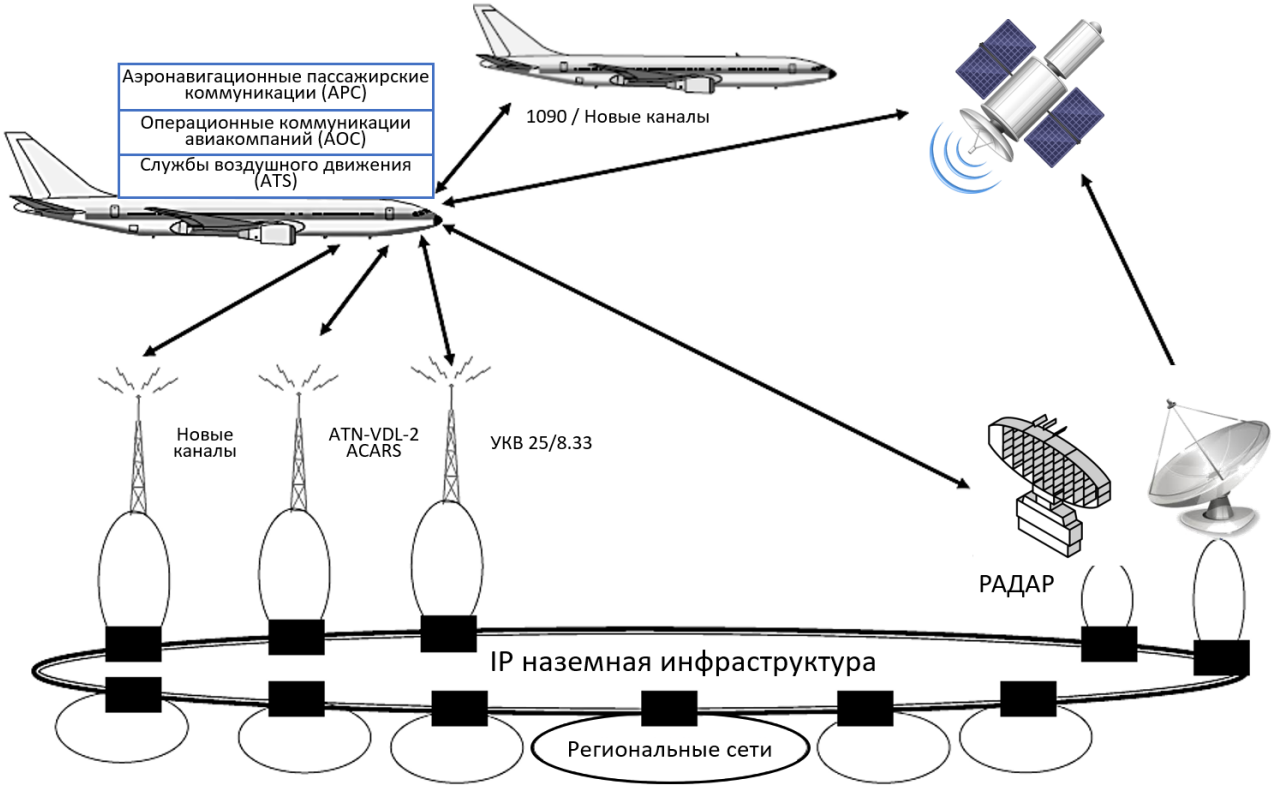

Рисунок 1.1 – Схема информационного взаимодействия в контуре УВД

Для анализа безопасности в контуре УВД требуется рассматривать три сегмента: каналы «воздух–земля», каналы «земля–земля» и механизмы взаимодействия с бортовым оборудованием ВС. Рост интенсивности полётов усиливает нагрузку на радиочастотный спектр 108–137 МГц, традиционно используемый для голосовой связи. В условиях перегруженности спектра возникают задержки и временная недоступность каналов связи между экипажем и диспетчером. ИКАО отмечает необходимость расширения доступного спектра для перспективных цифровых линий передачи данных «воздух–земля» [7]. Исторически предпринимались меры по снижению нагрузки, включая расширение полосы частот и уменьшение разнесения каналов до 8,33 кГц в рамках инициативы

EUROCONTROL 1994 года [8]. Однако данные меры не решают фундаментальных ограничений аналоговой связи и не обеспечивают устойчивого обмена данными в условиях растущей информационной нагрузки.

Переход к цифровому обмену связан с разработкой концепции CNS/ATM Комитетом FANS (1983 г.). CNS/ATM предусматривает использование цифровых каналов и спутниковых технологий, что повышает пропускную способность каналов «воздух–земля» и обеспечивает устойчивый обмен данными в интересах УВД. В рамках данной архитектуры применяются три основных среды передачи: VHF Data Link Mode 2 (VDL-2), спутниковая связь (SATCOM) и HF Data Link.

Наиболее широко применяемым каналом передачи данных в контуре УВД является VDL-2, функционирующий в диапазоне частот 118.000–136.975 МГц. Теоретическая пропускная способность канала составляет порядка 31,5 кбит/с [9].

Вместе с тем эксплуатационные данные свидетельствуют о существенном расхождении между номинальными и фактическими характеристиками. По материалам EUROCONTROL, в условиях высокой плотности воздушного движения, эффективная скорость передачи данных в условиях реальной нагрузки, как правило, не превышает 8 кбит/с, при этом в отдельных сценариях эксплуатации наблюдается её снижение до 4 кбит/с [10-13]. Указанные ограничения обусловлены влиянием совокупности факторов, включая высокую плотность трафика, особенности множественного доступа и служебные накладные расходы протоколов.

Результаты исследований подтверждают эффективность применения VDL-2: согласно данным [14], использование голосовой радиосвязи сократилось на 84% для ВС, оснащённых системой Controller to Pilot Data Link Communication (CPDLC). Полученный результат указывает на переход к цифровым решениям в авиационной связи в задачах УВД и оперативной связи авиакомпаний, что повышает надёжность и эффективность коммуникации.

Интеграция цифровых каналов связи в состав бортовой авионики осуществляется через блок управления связью (Communications Management Unit, CMU). Данный блок обеспечивает маршрутизацию сообщений адресно-отчётной

системы авиационной связи (ACARS) и CPDLC между радиосредствами, системой управления полётом (Flight Management System, FMS) и экипажем ВС. Современные модули, такие как CMU-900, поддерживают функции CPDLC, соответствуют европейским требованиям к передаче данных и позволяют настраивать таблицы маршрутизации для оптимизации использования каналов связи в зависимости от эксплуатационной конфигурации. Расширение перечня цифровых интерфейсов, функционирующих на борту ВС, увеличивает число входных точек, через которые возможна реализация НСВ, что показано на рисунке 1.2 [15].

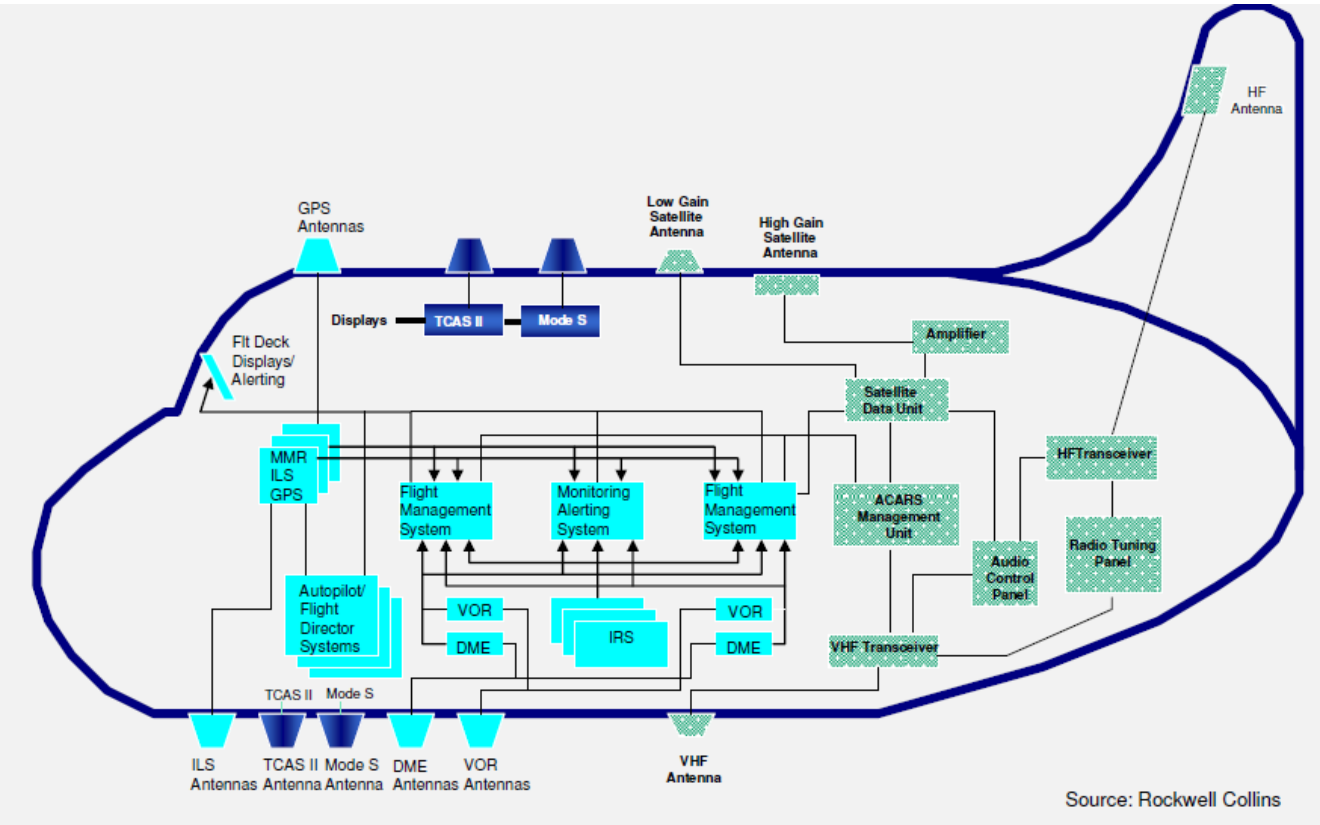

Рисунок 1.2 – Современные радиосистемы авионики

Существующие подходы к обеспечению информационной безопасности бортового оборудования ВС ориентированы на архитектурную перестройку информационно-вычислительной среды, включая разделение на домены доверия, внедрение защищённых шлюзов и специализированных серверов обработки данных [16-17]. Реализация указанных решений требует глубокой модификации бортового оборудования и протоколов информационного взаимодействия, что в

условиях эксплуатации действующего авиационного парка сопряжено со значительными техническими, экономическими и регуляторными ограничениями и, как следствие, практически невыполнимо в краткосрочной перспективе [18-20]. При этом применение криптографических алгоритмов требует не только переоборудования бортового оборудования ВС, но и модернизации наземной инфраструктуры, что предполагает синхронное обновление всех элементов контура УВД, сопровождаемое значительными затратами, длительной сертификацией и ограничениями совместимости.

Дополнительно следует учитывать, что существующие методы анализа безопасности бортового оборудования ВС также предполагают доступ к исходным текстам и проведение их статического и динамического анализа, что на практике затруднено вследствие ограничений на доступ к программному обеспечению и отсутствия нормативно-правовой базы его контроля [21-22].

В дополнение к анализу каналов «воздух–земля» необходимо рассмотреть наземную телекоммуникационную инфраструктуру АС УВД как ключевой компонент контура УВД, обеспечивающий обработку, маршрутизацию и формирование сообщений, передаваемых по каналам цифровой связи. Именно сочетание воздушного сегмента, каналов передачи данных и наземных подсистем управления формирует единое цифровое воздушное пространство, в пределах которого возможны риски НСВ.

В условиях растущей интенсивности воздушного движения возрастают объемы динамических данных АС УВД, требуемых для эффективного управления. Эти данные характеризуются большим объемом, вариативностью во времени и неоднородностью источников. АС УВД, обрабатывающие и передающие эти данные в режиме реального времени, выполняют критически важные функции: анализ авиационных рисков, координацию операций, обнаружение возможных конфликтов полётов и поддержку принятия решений в ситуациях высокой нагрузки и потенциальных угроз [23–24].

В качестве прикладного примера наземной информационно-телекоммуникационной инфраструктуры в авиационной отрасли целесообразно

рассматривать АС УВД Российской Федерации. Для решения задач обеспечения безопасности, экономичности и регулярности воздушного движения в филиале «Московском Центре АУВД» процесс ОрВД был переведен на новую АС ОрВД «Синтез-АР4», являющуюся крупнейшей в России и одной из самых крупных в мире. В условиях высокой интенсивности воздушного движения новая система АС ОрВД «Синтез-АР4» полностью обеспечивает диспетчерский персонал всей необходимой информацией для целей УВД. Уже сейчас в АС ОрВД «Синтез-АР4» внедрены такие современные технологии как CPDLC.

Архитектура АС УВД опирается на распределённую обработку данных, организацию защищённого обмена информацией между разнородными компонентами и интеграцию с объектами аэронавигационного обеспечения. Структура типовой телекоммуникационной подсистемы АС УВД представлена на рисунке 1.3 [25].

Телеметрические, радиолокационные и плановые данные циркулируют в пределах многоуровневой сети, включающей наземные центры управления, пульты диспетчерских служб, интерфейсы автоматического наблюдения, каналы фиксированной электросвязи и каналы радиосвязи. Для обеспечения непрерывности функционирования телекоммуникационной подсистемы применяются цифровые линии передачи данных, резервируемые по маршрутам и по типу носителей (наземные и радиоканалы). Связь осуществляется как в реальном времени (при управлении воздушной обстановкой), так и в периодической форме (при передаче метеорологического обеспечения и плановой информации о полёте ВС).

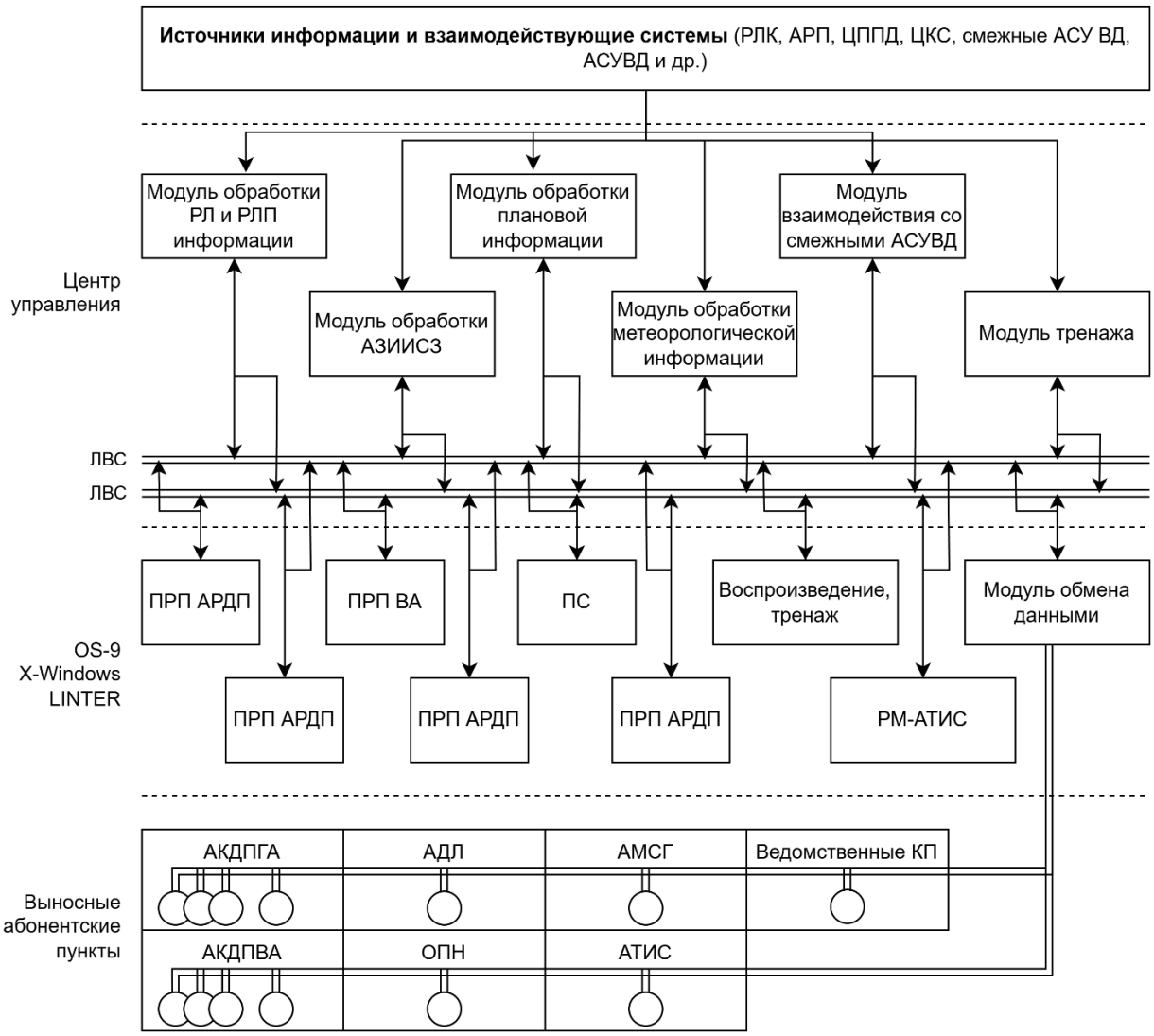

Рисунок 1.3 – Структура АС УВД

АС УВД выполняет автоматизированную обработку следующих информационных потоков, обеспечивая выполнение её ключевых функций в интересах УВД:

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.

При наличии межсетевых связей и интеграции с внешними системами, АС УВД остаётся уязвимой к НСВ, направленному на манипулирование информационными потоками. Компрометация узлов наземной инфраструктуры потенциально позволяет злоумышленнику воздействовать и на каналы «воздух–земля» — в частности, формировать или модифицировать сообщения ACARS и CPDLC, передаваемые на борт ВС.

Перспективное развитие систем передачи данных в контуре УВД определяется переходом к цифровым технологиям, обеспечивающим повышение эффективности, расширение функциональности каналов «воздух–земля» и рост степени автоматизации процессов ОрВД. Одним из ключевых факторов такой трансформации является использование коммерческих программно-аппаратных решений [26]. Их применение упрощает интеграцию сетевых компонентов, снижает затраты на сопровождение и обеспечивает совместимость с существующей наземной телекоммуникационной инфраструктурой. Однако, такое

распространение коммерческих решений в критически важных авиационных системах приводит к появлению унаследованных уязвимостей и увеличивает риски НСВ, включая вмешательство в процессы обмена данными между бортовыми и наземными средствами связи [27]. Итоговая структура цифровых каналов передачи данных на воздушном транспорте представлена на рисунке 1.4.

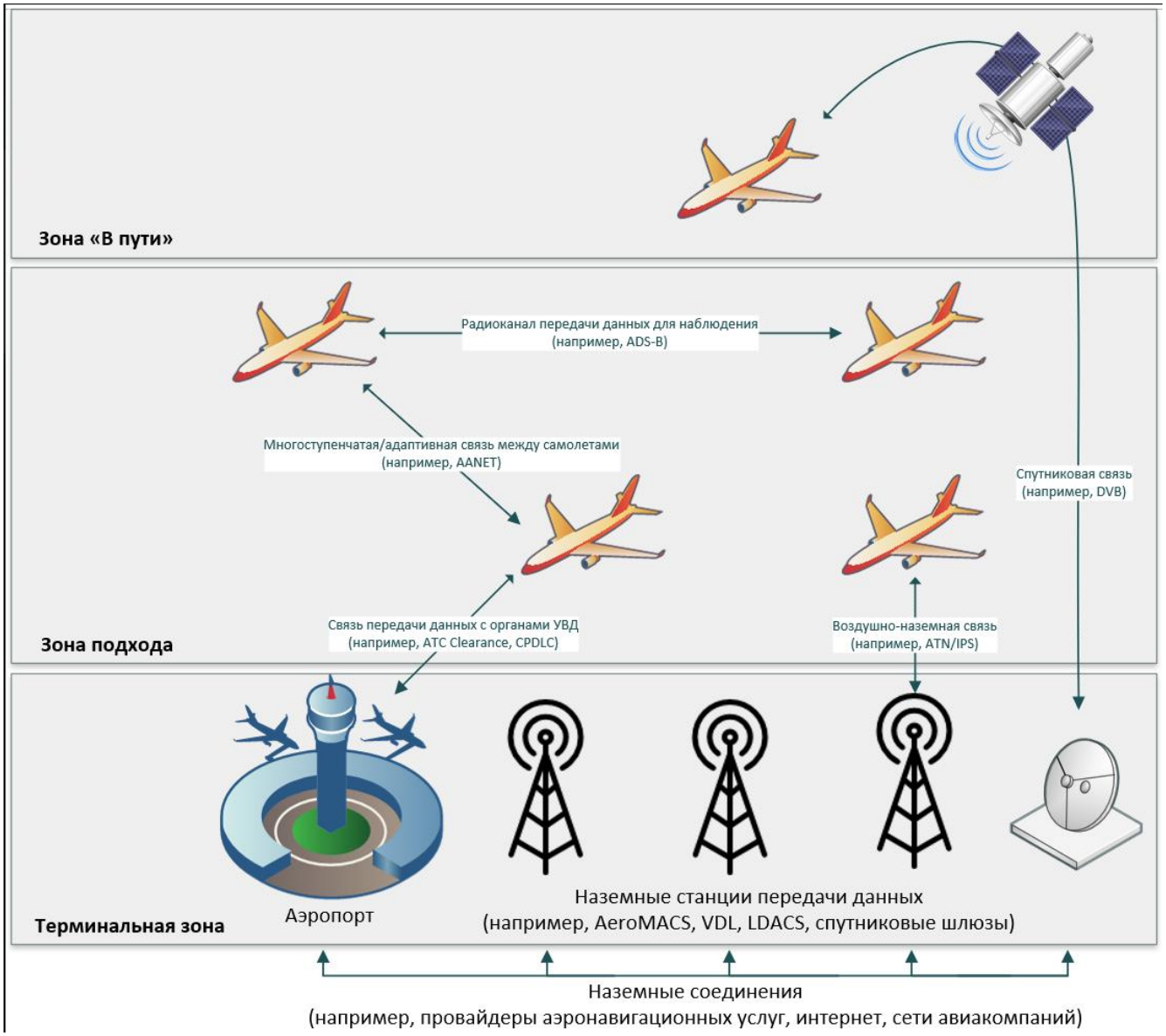

Рисунок 1.4 – Связь по каналам передачи данных на воздушном транспорте

Стратегическое направление модернизации авиационной телекоммуникационной сети связано с внедрением архитектуры ATN/IPS, разработанной ИКАО для унификации цифровых средств связи «воздух–земля» и «земля–земля» [28-29]. Стек ATN/IPS обеспечивает поддержку взаимодействия

различных коммуникационных технологий и ориентирован на эксплуатацию в условиях неоднородных сетей с различиями в задержке, пропускной способности и уровне ошибок. Переход от ATN/OSI к ATN/IPS означает, что передача сообщений CPDLC и эксплуатационных данных ACARS будет осуществляться по IP-сегментам, что позволяет интегрировать эти сервисы в общую сетевую инфраструктуру, но одновременно делает каналы обмена подверженными угрозам, характерным для IP-среды: подмене маршрутов и источников, манипуляции пакетами, блокированию передачи и искажению параметров сетевых событий.

Таким образом, современный контур УВД представляет собой разнородную цифровую среду, включающую каналы «воздух–земля», каналы «земля–земля», элементы бортовой авионики и наземные АС УВД. Расширение спектра используемых технологий сопровождалось ростом объёмов передаваемых данных, увеличением числа коммуникационных интерфейсов и усложнением архитектуры обмена. Интеграция этих средств в состав бортовых и наземных подсистем приводит к появлению новых точек взаимодействия и, как следствие, потенциальных каналов реализации НСВ, направленного на искажение, блокирование или подмену цифровой информации, циркулирующей в контуре УВД. Для выработки эффективных мер защиты необходимо провести анализ НСВ в контуре УВД.

1.2. Анализ несанкционированного вмешательства в контуре управления воздушным движением

Анализ угроз для систем передачи данных в контуре УВД должен учитывать не только технические особенности архитектуры связи, описанные ранее, но и

нормативные требования, определяющие границы допустимых рисков для объектов воздушного транспорта. В соответствии с положениями Федерального закона от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» воздушный транспорт отнесён к числу объектов, в отношении которых предусмотрены меры противодействия актам незаконного вмешательства, нарушающим функционирование информационных и технических систем, при этом подход к обеспечению безопасности в авиации должен основываться на международных стандартах, установленных ИКАО [30]. В соответствии с Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [31], авиационные системы связи и УВД входят в число критически важных объектов. Их защита предполагает предотвращение незаконного доступа, пресечение попыток нарушения устойчивости связи, а также контроль целостности передаваемых данных. На международном уровне соответствующие направления закреплены в Глобальном плане обеспечения авиационной безопасности, утверждённом по итогам 42-й сессии Ассамблеи ИКАО. В актуальной редакции документа подчёркивается значимость учёта угроз, связанных с воздействием на сетевую инфраструктуру авиационного транспорта, при модернизации систем и реализации новых технологических решений [32]. НСВ в контуре УВД, рассматривается как один из возможных векторов реализации подобных угроз.

Вся цепочка обмена данными между ВС и наземными сегментами в контуре УВД представляет собой совокупность потенциальных точек входа для проведения НСВ. К таким точкам относятся каналы передачи «воздух–земля» (VHF, VDL-2, HFDL, SATCOM), серверы органов ОрВД, маршрутизирующие узлы АС УВД, а также подсистемы, обеспечивающие доставку сообщений экипажу ВС. Отсутствие встроенных криптографических механизмов в ряде технологий (ACARS, CPDLC) приводит к тому, что результаты преднамеренного воздействия могут проявляться на уровне операционной деятельности так же, как и последствия технического сбоя [33].

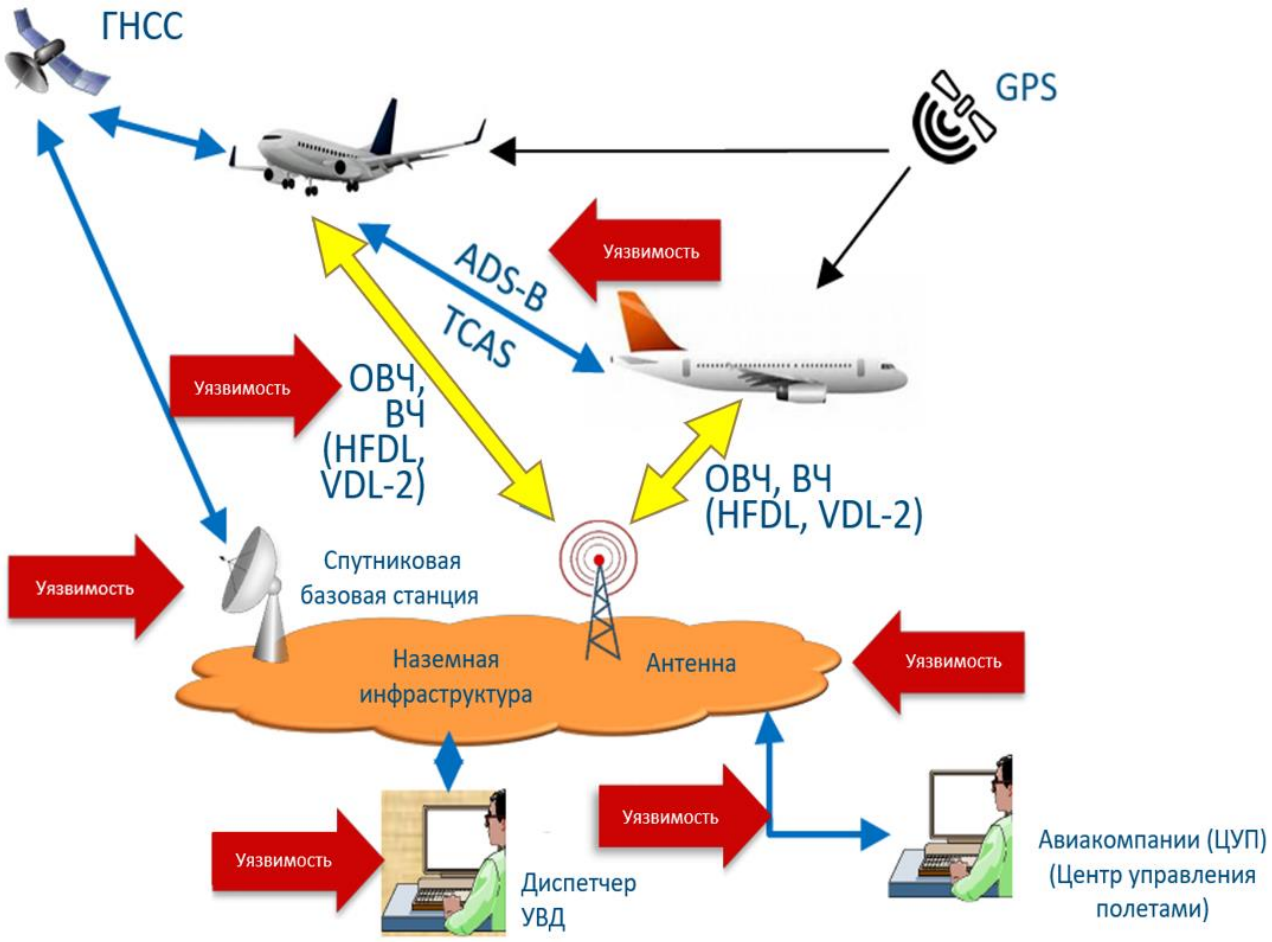

Рисунок 1.5 – Структура контура УВД в условиях НСВ

В рамках данной архитектуры критически следует учитывать, что проявления НСВ в контуре УВД могут быть неотличимы от стандартных отказов, тогда как системы УВД не обладают средствами различения причин нарушения. Анализ инцидентов показывает, что нарушения работы наземных компонентов АС УВД приводят к отклонению траекторий ВС и нарушению графиков полётов, включая этапы захода и посадки, с зарегистрированными отклонениями более чем на 20% от планового маршрута [34]. При НСВ аналогичные эффекты могут возникать вследствие преднамеренного искажения данных, задержки передачи команд диспетчера УВД или манипулирования служебными сообщениями, что делает последствия НСВ неотличимыми от технического отказа.

Результаты моделирования в среде MACS показывают, что нарушение передачи данных увеличивает рабочую нагрузку диспетчера (рост NASA-TLX с 53 до 73 баллов), увеличивает время передачи управления (с 39 до 53 секунд) и

снижает точность ситуационной осведомлённости (с 80 % до 62 %) [35]. Отмечены случаи, когда диспетчеры продолжали использовать фактически неработающие средства связи вследствие отсутствия своевременного уведомления об отказе [36]. В условиях НСВ аналогичная ситуация проявляется как скрытый отказ: вмешательство маскируется под техническую неисправность, а отсутствие механизмов анализа сетевых признаков создаёт риск неправильной интерпретации поступающих данных в контуре УВД.

Далее необходимо рассмотреть НСВ в каналах «воздух-земля» и воздействие на бортовое оборудование ВС. Архитектура обмена данными «воздух-земля» представлена на рисунке 1.6 [37].

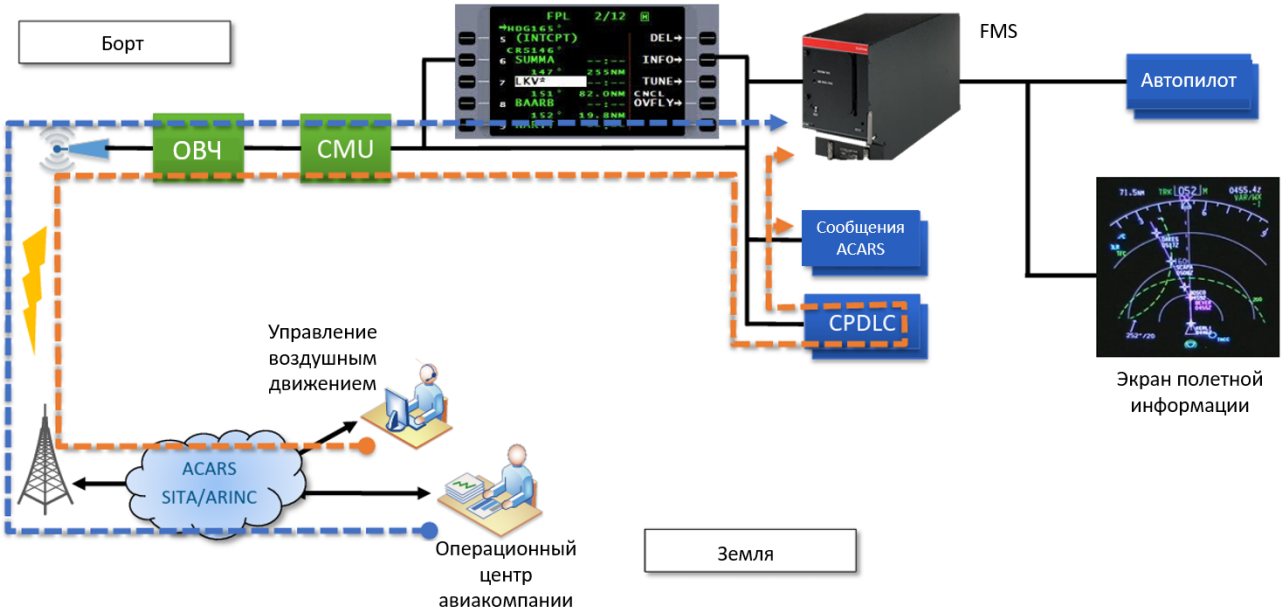

Рисунок 1.6 – Архитектура обмена данными «воздух-земля»

Она демонстрирует прохождение управляющих сообщений от наземных систем в сторону ВС: данные, поступающие по каналам VHF, VDL-2 или SATCOM, принимаются блоком управления связью CMU, после чего маршрутизируются в сторону FMS и связанных подсистем, включая автопилот и средства отображения. В цепочку входят как сообщения ACARS, так и сообщения CPDLC, причём в распространённой реализации FANS-1/A, по данным ИКАО, передача CPDLC осуществляется поверх ACARS и наследует отсутствие проверки целостности и криптографической аутентификации источника [38]. Контроль целостности в

CPDLC ограничивается обнаружением искажений, но не защищает от умышленной подмены сообщения.

В такой архитектуре НСВ в канал связи на этапе передачи «воздух–земля» может приводить к загрузке в FMS некорректных параметров полёта: высоты, маршрута, эшелона, скорости. Канал CMU → FMS функционирует автоматически, и внесённые изменённые значения могут отразиться на расчёте траектории до того, как экипаж обратит внимание на недостоверность данных. Это превращает НСВ в каналах передачи данных в прямой фактор нарушения аэронавигационного обеспечения полётов.

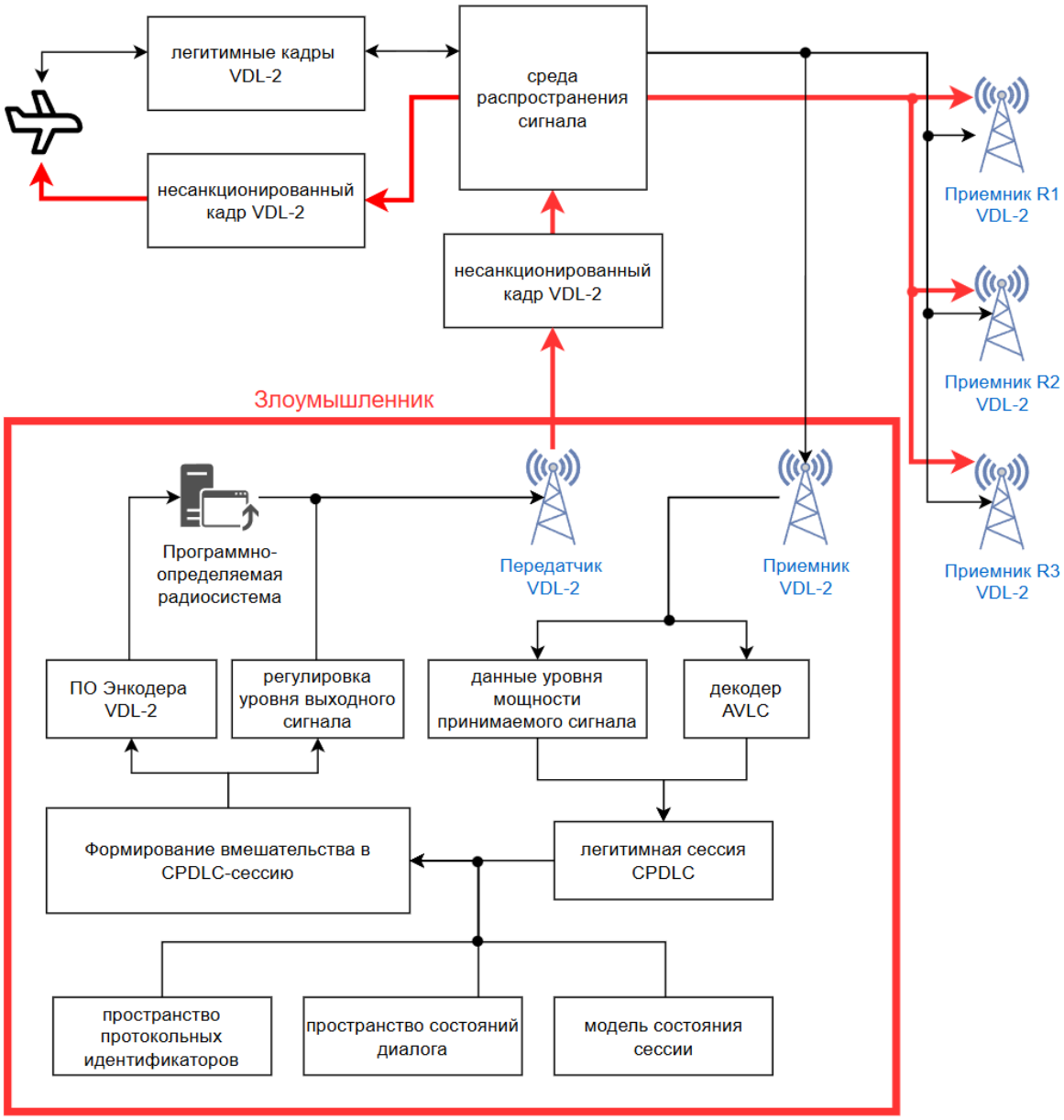

Рисунок 1.7 – Модель несанкционированного вмешательства

Модель НСВ показана на рисунке 1.7. Данная модель показывает возможность злоумышленника использовать среду распространения сигнала для получения информации о состоянии канала VDL-2, декодировать содержание сообщений, устанавливать контекст легитимного информационного обмена для последующего вмешательства, направленных на снижение доступности или доверия к цифровому каналу.

Практическая осуществимость подобных воздействий подтверждается исследованиями, демонстрирующими возможность перехвата сообщений CPDLC при наличии прямой видимости в диапазоне ОВЧ [39-40]. Использование высоколетящего БАС увеличивает радиопокрытие и обеспечивает злоумышленнику возможность воздействия на ВС. В этих условиях злоумышленник способен формировать поддельные ACARS- и CPDLC-сообщения, которые могут быть восприняты CMU как корректные и переданы далее в FMS.

Исследования в области защиты каналов передачи данных «воздух–земля» и сетевых компонентов СПД в контуре УВД [41-42] указывают на наличие широкого спектра уязвимостей, реализация которых позволяет злоумышленнику воздействовать как на наземные элементы АС УВД, так и на бортовые системы ВС. Наиболее уязвимыми оказываются системы ACARS и CPDLC, поскольку обе технологии функционируют в радиоканале, используют команды диспетчера УВД. Основываясь на результатах анализа указанных работ, ниже приводится классификация воздействий, начиная с наиболее простых и заканчивая сложными сценариями преднамеренного НСВ.

Наиболее простой формой НСВ является перехват незашифрованного радиотрафика. Сообщения ACARS и CPDLC могут приниматься с помощью SDR в диапазоне 118–137 МГц без нарушения работы систем УВД [43-44]. Злоумышленник пассивно принимает и анализирует незашифрованные ACARS- и CPDLC-сообщения, восстанавливая структуру маршрута, текущие параметры полёта, особенности работы конкретных авиакомпаний и органов УВД [45]. По классификатору ФСТЭК такое воздействие соответствует УБИ.1 «Угроза утечки

информации» и напрямую не нарушает функционирование системы, однако создаёт основу для последующих активных атак, поскольку позволяет сформировать сценарий НСВ в контуре УВД.

Следующей по сложности группой являются атаки обрыва связи на стороне НС/ВС. Можно выделить генерацию избыточных легитимных сообщений в канале VDL-2, создающих перегрузку для канала VDL-2 [46] или наземных шлюзов. Для реализации такого НСВ злоумышленнику достаточно генерировать сигнал достаточной мощности в рабочем диапазоне и имитировать структуру легитимного протокола. Последствием становится потеря или значительная задержка получения управляющих сообщений и служебной информации экипажем, что в свою очередь приводит к увеличению использования голосовой радиосвязи и увеличению нагрузки на диспетчера. Подобные сценарии относятся к УБИ.140 «Угроза приведения системы в состояние отказа в обслуживании». Данная атака представляет наибольший научный интерес.

Более сложной по воздействию является группа атак ложного информирования экипажа ВС, которое может привести к виртуальному угону, так как информационное воздействие может привести к изменению параметров полёта без физического захвата ВС. Злоумышленник может формировать поддельные ACARS/CPDLC-сообщения, внешне соответствующие протоколу, и доставлять их в цепочку «орган УВД — VDL-2 — CMU — FMS» [47-49]. Изменение данных о массе и центровке (weight&balance update) приводит к некорректным расчётам взлётных режимов (передаваемые по ACARS), а сообщения типа PROCEED DIRECT TO — к выполнению манёвров, не соответствующих исходному заданию. В таком случае экипаж формально остаётся у штурвала, но часть решений фактически принимается на основе подменённых данных, что позволяет рассматривать подобные сценарии как виртуальный угон. В терминах ФСТЭК описанные воздействия соответствуют УБИ.027 «Угроза искажения вводимой и выводимой на периферийные устройства информации» и УБИ.033 «Угроза использования слабостей кодирования входных данных», поскольку приводят к дезинформированию экипажа ВС через модифицированные входные данные.

Близкой по характеру, но более узкой по цели является атака виртуального изменения траектории ВС. Последовательное внедрение поддельного плана полётов по ACARS или поддельных команд изменения эшелона по каналу CPDLC способно привести к значимому отклонению траектории от расчётной. Возможен сценарий, при котором команда CLIMB TO/DESCEND TO, модифицированная в канале передачи, приводит к сближению с другим ВС при отсутствии визуального конфликта на стороне диспетчера. Такая атака технологически неотличима от совокупности ошибок экипажа ВС и диспетчера, хотя её источником является преднамеренное НСВ на уровне сообщений ACARS/CPDLC.

Анализ НСВ в контуре УВД показывает, что наиболее актуальной и реальной является атака обрыва связи для экипажа ВС и наземной АС УВД, так как злоумышленник имеет данные по установленной сессии, может привести к множественной повторной установке сессии CPDLC, что приводит соответственно к обрыву связи по цифровому каналу, увеличению нагрузки на голосовую радиочастоту, увеличению нагрузки на диспетчера, что может вызвать потенциально-конфликтную ситуацию в зоне аэропорта.

Таблица 1.1. Сравнительная таблица атак в контуре УВД

Тип атаки	Уровень	Метод	Воздействие	Сложность
Разведка	Прикладной	Анализ незашифрованного радиотрафика	Слабое	Низкая
Обрыв связи для ВС	Канальный	Перегрузка каналов ACARS/CPDLC	Среднее	Низкая
Обрыв связи для наземной инфраструктуры	Транспортный	Перегрузка каналов ACARS/CPDLC	Среднее	Средняя
Ложное информирование ВС	Прикладной	Спуфинг	Среднее	Низкая
Ложное информирование диспетчера УВД	Прикладной	Спуфинг	Среднее	Среднее
Виртуальный угон ВС	Прикладной	Модификация сообщений ACARS/CPDLC	Сильное	Среднее
Виртуальное изменение траектории ВС	Прикладной	Модификация сообщений ACARS/CPDLC	Сильное	Среднее

Таким образом, можно систематизировать существующие и потенциальные угрозы в контуре УВД. Таксономия атак представляет собой схему, которая помогает классифицировать атаки, облегчая их анализ и повторное использование информации для обеспечения безопасности. Предлагаемая классификация [50], показанная на рисунке 1.8, использует четыре различных показателя.

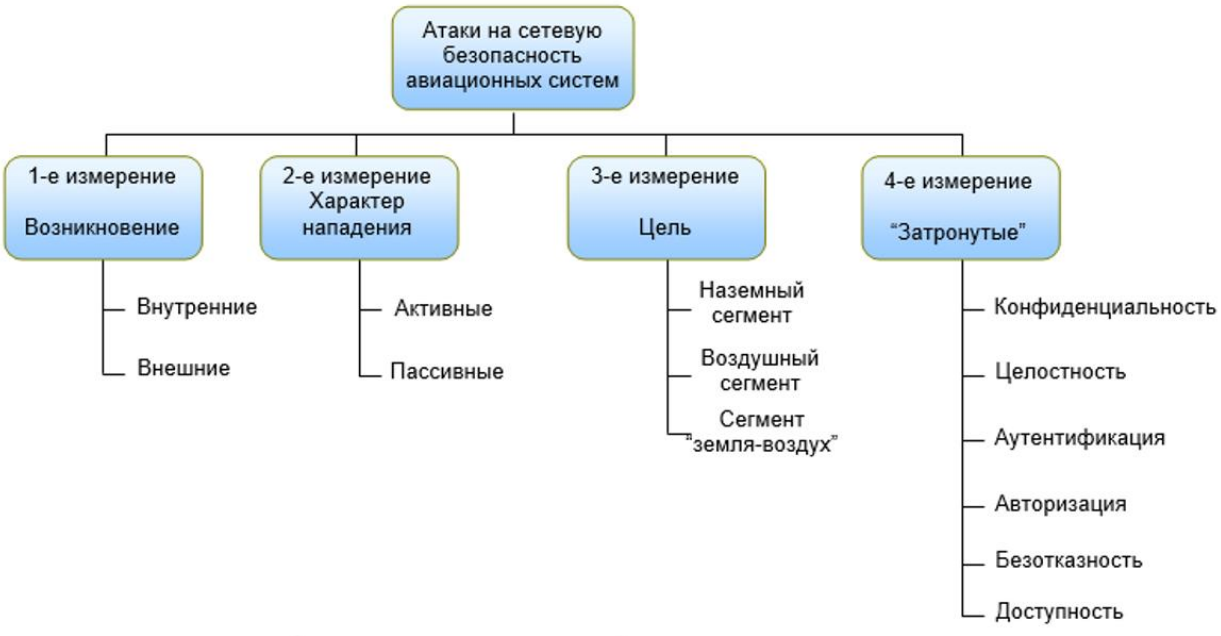

Рисунок 1.8 – Классификация атак на СПД в контуре УВД

1. Возникновение - используется для классификации атак в зависимости от того, являются ли они внутренними или внешними:

• *Внутренние атаки* обычно инициируются доверенным лицом (например, диспетчером УВД или техническим специалистом аэропорта);

• *Внешние атаки* инициируются объектом, который не принадлежит логической сети или не признан легитимным субъектом системы. Внешние атаки чаще происходят в контуре УВД.

2. Характер нападения - учитывает цель нападения, оно может быть активным или пассивным:

• *Активные атаки* напрямую взаимодействуют с целью или системой (например, внедрение сообщений, атаки с повторным воспроизведением);

• *Пассивные атаки* обычно проводятся путем перехвата информации, которая может быть использована позже для начала активной атаки. Из-за беспроводного характера средств связи «воздух-земля» среда ОрВД подвержена таким атакам.

3. Целью - является один из сегментов ОрВД, а именно:

• *воздушный сегмент* – бортовая система;

• *сегмент «воздух – земля»*, соответствующий средству связи (например, спутниковая линия связи);

• *наземный сегмент*, который касается наземных сетей.

Особенно критична устойчивость каналов «воздух–земля», характерных для контура УВД, полностью зависящих от качества и защищённости линии управления. Любое НСВ на такой канал может непосредственно повлиять на безопасность полётов.

4. Атрибуты безопасности «Затронутые» - соответствуют службам безопасности, первоначально запрошенным целью, но ставшими недействительными в случае успешной атаки.

Таким образом, проведён анализ НСВ в контуре УВД. Выделены векторы воздействия на АС УВД, бортовые компоненты ВС и каналы «воздух–земля», установлены характерные направления реализации атак и их влияние на устойчивость информационного обмена.

1.3. Анализ технологий искусственного интеллекта в задаче обнаружения несанкционированного вмешательства в контур управления воздушным движением

Цифровые СПД обеспечивают возможность накопления параметров трафика, отражающих состояние информационного обмена в контуре УВД (как наземными службами, так и бортовыми системами). Традиционные системы обнаружения вторжений, основанные на сигнатурах или анализе сетевых протоколов, демонстрируют ограниченную эффективность при столкновении с новыми типами атак, такими как распределенный отказ в обслуживании, использующих нестандартные схемы передачи данных [51]. Для СПД это особенно критично: применение жёстко заданных правил не позволяет своевременно реагировать на неизвестные угрозы (или угрозы нулевого дня), а ложные срабатывания могут привести к сбоям в работе бортовых и наземных систем [52].

Анализ противодействия деградации цифрового канала связан с несколькими направлениями. Первое – криптографическая защита и целостность. На сегодняшний известны решения по криптографической защите прикладных сообщений ACARS и CPDLC, разработанные ARINC [53-54] и рассмотренные в трудах [55], однако, эта защита не охватывает протокольный стек. Проверка целостности так же не защищает от деградации канала и возможной подмене сообщений [56-57].

Второе – доступность. Радиопеленгация злоумышленника невозможна, так как он может послать короткое сообщение, недостаточное по мощности и продолжительности для определения местоположения сигнала с помощью радиопеленгации VDF. Резервным вариантом является переход на голосовую связь, что может привести далее к её деградации (см. п. 1.2).

Таким образом, актуальным направлением развития является моделирование информационного обмена в контуре УВД и дальнейшее обнаружение признаков вмешательства на основе машинного обучения.

Рисунок 1.9 – Методы обеспечения устойчивости канала VDL-2

Это создаёт условия для применения технологий искусственного интеллекта, а именно методов машинного обучения в задаче обнаружения НСВ [58-59] Такие методы классифицируются на три основные группы: алгоритмы классификации, кластеризации и регрессионного анализа. Классификация направлена на отнесение события к одному из заранее определённых классов. Кластеризация применяется в условиях отсутствия априорной информации о структуре данных и позволяет выделять группы на основе внутренней схожести. Регрессионные методы используются для восстановления функциональных зависимостей между признаками сетевого трафика.

НСВ в контур УВД проявляется в виде отклонений параметров телеметрии от штатных режимов функционирования системы. В наблюдаемых

информационно-вычислительных процессах в контуре УВД регистрируются наборы параметров (векторов) $\bar{x}$, отражающие текущее состояние различных подсистем и сетевого трафика. В отсутствие внешнего вмешательства такие векторы признаков остаются в пределах, соответствующих штатной работе. Появление же аномальных комбинаций или последовательностей значений, не характерных для нормальной эксплуатации, служит индикатором возможного НСВ. Цель обнаружения НСВ заключается в автоматическом выделении таких событий (аномалий), потенциально связанных с внешним вмешательством, на основе анализа структуры и параметров телеметрических данных.

Формально задачу обнаружения НСВ в контуре УВД можно рассматривать как частный случай классификации. Пусть $\bar{x} = (x_1, x_2, \dots, x_n)$ — вектор характеристик (признаков), описывающих состояние системы на некотором интервале времени, и $y \in \{0; 1\}$ — бинарная переменная, принимающая значение $y = 1$ при наличии НСВ и $y = 0$ в нормальном режиме. Тогда алгоритм обнаружения задаётся отображением $a : X \to Y$, ставящим в соответствие каждому наблюдению $x \in X$ решение $y \in \{0; 1\}$ о наличии либо отсутствии внешнего вмешательства.

С учётом того, что результатом НСВ в контур УВД чаще всего становится отклонение от эталонного состояния, наиболее целесообразным является использование классификационных алгоритмов. Такие алгоритмы позволяют автоматически отличать допустимые сетевые взаимодействия от потенциально нарушающих норму, что делает их применимыми для выявления признаков внешнего воздействия на процессы передачи данных на ВТ.

Наиболее популярными классификационными алгоритмами, применяемыми в задачах обнаружения НСВ, являются:

– метод опорных векторов;

– байесовский классификатор;

– метод построения решающих деревьев;

– многослойные нейронные сети;

– метод K-средних.

Обучение классификационных алгоритмов направлено на минимизацию эмпирического риска, то есть снижение средней ошибки на обучающей выборке. Для оценки качества работы модели применяются функции потерь, аргументами которых являются прогнозируемое значение и истинное значение из размеченной выборки.

В процессе обучения используется кросс-валидация, при которой обучающая выборка делится на несколько частей, а затем модель обучается на одной из них и тестируется на остальных. Такой подход позволяет получить объективную оценку точности алгоритма.

Для выбора наиболее эффективного метода машинного обучения в задаче обнаружения НСВ применяется следующая последовательность:

1. формирование обучающей выборки;

2. предварительная обработка данных: очистка, нормализация, кодирование категориальных признаков (если есть);

3. отбор значимых признаков с использованием нескольких методов оценки важности;

4. разбиение данных на обучающую и тестовую части;

5. обучение моделей и настройка параметров;

6. оценка эффективности моделей по метрикам: доля правильных классификаций (accuracy), точность (precision), полнота (recall), F1-мера (см. п. 3.4);

В задаче обнаружения НСВ информационный обмен в контуре УВД описывается по различным характеристикам, таким как:

– время поступления пакета;

– тип передаваемого пакета;

– задержка передачи данных;

– протокол транспортного уровня;

– порядковый номер сообщения;

– размер передаваемого сообщения.

Приведем основные алгоритмы машинного обучения, которые могут быть использованы для решения задачи выявления НСВ в контуре УВД.

Алгоритм дерева решений используется для классификации информационного обмена при обнаружении НСВ. Модель формируется на основе обучающей выборки путём разбиения множества по признакам, минимизирующим энтропию. В качестве критерия выбора признака используется прирост информации, определяемый как разность энтропии исходного множества транзакций и взвешенной суммы энтропий подмножеств, полученных при разбиении по признаку A:

$$\Delta H(A) = H(T) - \sum \frac{|T_i|}{|T|} \cdot H(T_i)\,, \tag{1.1}$$

где: T – исходная выборка,

T_i – подмножества, полученные при разбиении.

Энтропия множества определяется как:

$$H(T) = \sum p_j \cdot \log_2(p_j)\,, \tag{1.2}$$

где p_j – доля объектов класса j.

Метод характеризуется высокой интерпретируемостью, низкой вычислительной сложностью и пригоден для анализа телеметрических потоков информационного обмена в авиационной инфраструктуре. Он позволяет обрабатывать данные в реальном времени при ограниченных вычислительных ресурсах.

При использовании двенадцати признаков и интервала анализа в две секунды достигается точность 97,5 % при обнаружении атак типа отказ в обслуживании [60]. Обнаружение ранее неизвестных воздействий не обеспечивается, однако чувствительность повышается при построении адаптивных деревьев по прикладным протоколам [61] и расширении пространства признаков [62]. Комбинированные модели с разметкой на известные и неизвестные атаки позволяют реализовать поэтапную оптимизацию по критерию информационного выигрыша [63].

Несмотря на простоту алгоритма, при обработке выборок с большим числом признаков и значительным объёмом данных построение дерева решений

сопровождается увеличением вычислительной сложности. Без ограничения глубины дерево склонно к переобучению, формируя разветвлённую структуру с большим числом узлов. Это увеличивает вычислительные затраты как на этапе построения, так и при последующем использовании модели. Также алгоритмы дерева решений требуют наличия размеченного набора данных и не позволяют выявлять сложные взаимосвязанные атаки, что ограничивает их применение в контуре УВД.

В связи с указанными ограничениями при анализе данных применяются более гибкие модели, в частности, нейронные сети. Их работа основана на последовательной обработке входных данных через слои искусственных нейронов. Каждый слой выполняет преобразование входного сигнала с учётом весов связей и выбранной функции активации.

В задачах классификации часто оказывается достаточным использование одного скрытого слоя. Однако при наличии нелинейных зависимостей между признаками применяются многослойные архитектуры. Это позволяет учитывать внутреннюю структуру данных и выявлять скрытые закономерности без использования заранее заданных сигнатур.

Модели искусственных нейронных сетей обладают рядом свойств, важных для анализа телекоммуникационного трафика: устойчивостью к единичным сбоям, распределённым характером обработки информации и адаптивностью структуры. Это делает возможным их применение в условиях высокой динамики сетевого взаимодействия в контуре УВД. В ряде работ показана эффективность резонансных архитектур и самоорганизующихся карт при распознавании как известных, так и аномальных паттернов поведения [64–65]. Использование иерархических структур обеспечивает обработку данных в распределённой среде [66]. Сравнение эмпирических характеристик сетевого взаимодействия с эталонными профилями позволяет выявлять отклонения при анализе нетипичного трафика [67].

Высокая чувствительность к структуре данных определяет возможность применения таких моделей для обнаружения ранее неизвестных форм несанкционированного вмешательства. В то же время значительная

вычислительная нагрузка, склонность к переобучению и зависимость от объёмов размеченных данных ограничивают их использование в условиях авиационных СПД, где критичны устойчивость, ресурсная эффективность и интерпретируемость решений.

Метод опорных векторов представляет собой алгоритм бинарной классификации, направленный на построение гиперплоскости, максимизирующей зазор между классами. Обучение осуществляется путём решения задачи выпуклой квадратичной оптимизации, что обеспечивает достижение глобального минимума и устойчивость результата. При линейной неразделимости классов используется ядровая функция, позволяющая проецировать данные в пространство большей размерности, где возможно линейное разделение при сохранении вычислительной эффективности.

В отличие от моделей на основе нейронных сетей, метод опорных векторов демонстрирует высокую устойчивость к переобучению, работает при ограниченном объёме размеченных данных и не зависит от начальных условий. Эти свойства делают его применимым для задач обнаружения НСВ в телекоммуникационных системах, в том числе в авиационной сфере, где объёмы трафика велики, а характер атак подвержен изменениям [68].

Для повышения эффективности классификации предложены различные модификации. В частности, использование нечеткой дискриминации повышает точность идентификации аномалий [69], а интеграция с теорией грубых множеств позволяет сократить размерность признакового пространства и повысить устойчивость к шуму [70-71]. Применение вейвлет-преобразования направлено на удаление избыточных признаков и ускорение обучения [72], тогда как метод наименьших квадратов упрощает оптимизационную процедуру при сохранении требуемой точности [73]. Генетические алгоритмы используются для автоматического подбора параметров и повышения устойчивости модели [74], а объединение с методами муравьиной колонии улучшает точность обнаружения атак [75].

Несмотря на указанные преимущества, метод опорных векторов имеет ряд ограничений. Модель чувствительна к пропущенным и аномальным значениям, а её эффективность снижается при наличии перекрытия классов или несбалансированного распределения, характерных для контура УВД. Кроме того, рост размерности признаков и увеличение объёма выборки приводят к значительным затратам ресурсов на этапе обучения, что ограничивает применимость метода в условиях реального времени, характерных для авиационных СПД.

Байесовская классификация относится к числу вероятностных методов, основанных на применении теоремы Байеса, позволяющей оценивать апостериорную вероятность принадлежности объекта к тому или иному классу. Наиболее известной реализацией является наивный байесовский классификатор, в основе которого лежит предположение об условной независимости признаков. Это допущение упрощает вычисления, обеспечивая высокую скорость работы, стабильность на малых выборках и устойчивость при частичных пропусках данных.

В задачах с более сложной структурой зависимостей применяются байесовские сети, представляющие собой ориентированные ациклические графы с таблицами условных вероятностей. Совместное распределение случайных величин в такой сети определяется по формуле:

$$P(x_i, x_2, \cdots, x_n) = \prod_{i-1}^{n} P\left(x_i \middle| Parents(x_i)\right), \tag{1.3}$$

где $Parents(x_i)$ — множество причинных признаков для переменной x_i.

Вероятностный подход используется в построении распределённых систем обнаружения, основанных на обмене статистическими оценками между узлами [76]. Байесовские методы применяются в задачах дискриминантной классификации [77], в архитектурах облачных сетей [78], а также в средах с ограниченными ресурсами, таких как беспроводные сенсорные сети [79]. Отдельные работы ориентированы на повышение точности классификации с

помощью вероятностных моделей, усреднения нескольких байесовских структур и отбора признаков [80-83].

Главным ограничением метода остаётся допущение условной независимости признаков, которое редко соблюдается при анализе телекоммуникационного трафика. Это снижает обобщающую способность модели и затрудняет её применение в задачах, где присутствуют скрытые корреляции между параметрами, как это характерно для авиационных СПД.

Метод кластеризации К-средних (K-means) представляет собой алгоритм неконтролируемого обучения, применяемый для разбиения данных на k кластеров на основе близости между объектами и центрами кластеров [84]. Он относится к числу базовых методов кластеризации, при котором объекты, обладающие схожими признаками, группируются в один кластер.

Алгоритм кластеризации К-средних имеет вид [85]:

1. случайным образом выбрать *k* объектов в качестве начальных центров кластеризации (исходных точек);
2. рассчитать расстояние между каждой точкой и центральным объектом и повторно разделить соответствующие точки на основе минимального расстояния;
3. пересчёт центров как средних значений точек в каждом кластере;
4. повторять шаги (2, 3), пока каждый кластер не стабилизируется.

Метод k-средних применяется в задачах, не предполагающих наличие заранее размеченных данных. В отличие от алгоритмов классификации, основанных на обучении по меткам классов, он не требует предварительного присвоения объектов к известным категориям и позволяет выявлять структурные особенности выборки без предварительной информации. Это делает его полезным в задачах обнаружения аномалий в телекоммуникационном трафике, где тип нарушений заранее неизвестен [86]. Для авиационных сетей, характеризующихся высокой изменчивостью и отсутствием стабильных паттернов, такой подход позволяет зафиксировать отклонения от нормального поведения без предварительного обучения модели.

Применение самоорганизующихся карт Кохонена позволяет формировать устойчивые приближения центров кластеров, которые могут уточняться методом k-средних [87]. Использование оптимизации роя частиц снижает чувствительность алгоритма к начальному положению центров и повышает точность кластеризации [88], тогда как сочетание с критерием Колмогорова–Смирнова расширяет возможности выявления выбросов при анализе больших массивов телекоммуникационных данных [89]. Геометрическая переработка центров кластера направлена на повышение стабильности результатов при асимметричном распределении признаков [90], а применение многопоточной архитектуры ускоряет обработку данных [91]. Минимаксный подход уменьшает влияние исходной инициализации и улучшает качество кластеризации [92]. Использование генетических алгоритмов обеспечивает оптимизацию признаков и повышает эффективность модели в условиях высокой размерности [93].

Метод k-средних используется в составе комплексных схем обнаружения. Его комбинация с методом опорных векторов повышает устойчивость модели к аномальным данным [94-95]. Эффективность таких систем подтверждается результатами, полученными при построении многокомпонентных классификаторов [96-98]. В ряде решений реализовано объединение с нейронными сетями и компонентным анализом, что позволяет повысить точность идентификации и сократить объём обрабатываемых признаков [99-100].

Несмотря на вычислительную эффективность и простоту реализации, метод k-средних обладает рядом ограничений. Он чувствителен к выбору количества кластеров, подвержен влиянию выбросов и демонстрирует нестабильность при анализе данных с произвольной формой распределения. Эти особенности затрудняют его прямое применение в задачах анализа сложного и неустойчивого трафика авиационных СПД без соответствующей адаптации.

Таким образом, применение методов машинного обучения в системах обнаружения НСВ позволяет адаптировать процесс анализа сетевого трафика к изменяющимся условиям телекоммуникационной среды и снижает зависимость от предварительно заданных сигнатур. Каждый из методов, рассмотренных ранее,

обладает набором технических и прикладных особенностей, определяющих его применимость в конкретных задачах. В таблице 1.2 представлено обобщённое сравнение их ключевых преимуществ и ограничений.

Таблица 1.2. Сравнение алгоритмов машинного обучения по признакам применимости в задаче обнаружения НСВ

Метод	Преимущество	Недостаток
Дерево решений	Обработка больших данных, высокая точность обнаружения	Определяет, является ли отдельное событие атакой, но не связывает их в последовательности
Нейронная сеть	Самообучаемость, способность к обобщению неполных данных	Риск переобучения, сложность интерпретации
Метод опорных векторов	Высокая точность на малых выборках, устойчивость к переобучению	Ограниченность при работе с нелинейными структурами и пропущенными данными
Байесовский метод	Устойчивость к неполноте данных, эффективность при дискретных признаках	Зависимость от корректной априорной оценки и предположения независимости
Метод k-средних	Быстрое выполнение, простота реализации, устойчивость при чистых данных	Чувствительность к выбросам, необходимость ручного выбора числа кластеров

Однако в общем случае обнаружение НСВ не сводится к простой бинарной классификации. Многие виды внешнего вмешательства заранее неизвестны, и отсутствуют размеченные данные для обучения алгоритма на все возможные сценарии атак. Кроме того, характеристики воздействия могут со временем меняться: появляются новые типы аномальных паттернов, ранее не наблюдавшиеся в системе. Таким образом, необходимы решения, способные работать с

неразмеченными данными и выявлять нетипичные, ранее не встречавшиеся паттерны в потоках информационного обмена контура УВД без опоры исключительно на предварительное обучение.

Классические методы классификации демонстрируют ряд ограничений при применении к задаче обнаружения НСВ в контуре УВД. Во-первых, для построения классификатора требуется репрезентативный набор размеченных данных, охватывающий все значимые типы внешнего вмешательства, что на практике практически недостижимо. Если в обучающей выборке отсутствует какой-либо сценарий атаки, алгоритм классификации с высокой вероятностью не распознает его в реальном потоке. Во-вторых, даже при наличии обученных моделей их жёсткая привязка к известным шаблонам поведения может приводить к повышенному числу ложных срабатываний при столкновении с необычными, но легитимными ситуациями, не учтёнными в тренировочных данных.

Методы кластеризации, в свою очередь, также обладают существенными недостатками применительно к рассматриваемой задаче. Хотя для их использования не требуется предварительная разметка, результаты кластеризации трудно интерпретировать напрямую в терминах «атака» или «норма». Алгоритмы кластеризации стремятся разбить наблюдения на группы по сходству, однако редкие аномальные события могут не формировать отдельного кластера и остаться незамеченными среди нормальных данных. Кроме того, многие алгоритмы кластеризации плохо масштабируются в условиях потоковой обработки данных, характерной для телеметрии в контуре УВД.

В качестве альтернативы стандартным подходам можно рассмотреть методы поиска структурных паттернов (*pattern mining*), позволяющие выявлять скрытые закономерности и аномальные последовательности событий без предварительной разметки. Такие методы анализируют внутреннюю структуру данных (например, последовательности пакетов или взаимосвязи между различными параметрами) и способны обнаруживать шаблоны, отличающие нормальное функционирование системы от потенциально вредоносных отклонений. Однако традиционные алгоритмы обнаружения паттернов, как правило, ориентированы на офлайн-анализ

статических данных и недостаточно приспособлены для работы с непрерывной, распределённой телеметрической информацией. Их прямое применение в реальном времени приводит к генерации чрезмерного числа паттернов, что, в свою очередь, требует дополнительных этапов фильтрации и обобщения результатов. Более того, при анализе распределённых данных следует учитывать, что значимый сценарий НСВ может охватывать события, происходящие одновременно на нескольких узлах сети.

Таким образом, ни традиционные методы классификации и кластеризации, ни прямое применение подходов поиска паттернов не обеспечивает полной эффективности решения задачи обнаружения НСВ в контуре УВД. Это объясняется как жёсткими требованиями реального времени, так и непредсказуемостью возможных сценариев атак. Следовательно, требуется разработка методов и алгоритмов, учитывающих структурные зависимости между признаками, способных обрабатывать неполные (неразмеченные) наборы данных без потери качества классификации, а также обеспечивающих допустимое время обработки при анализе большого объема сетевого трафика.

В связи со сказанным, можно сформулировать постановку задачи исследований.

1.4. Постановка задачи исследований

Задача обнаружения НСВ в СПД контура УВД рассматривается в условиях неполноты априорной информации о возможных сценариях НСВ и изменчивости характеристик информационного обмена. Множество потенциальных воздействий на каналы «воздух–земля» и наземные сегменты заранее не задано, а

репрезентативная разметка данных по всем значимым типам атак отсутствует. Это не позволяет опираться на строго фиксированную классификационную структуру и требует формализации задачи обнаружения как задачи выявления отклонений от нормального функционирования по совокупности наблюдаемых признаков информационного обмена.

Пусть $X_{\text{норма}} \subset X$ – подмножество пространства наблюдений, соответствующее допустимому функционированию сетей передачи данных в контуре УВД. Тогда задача обнаружения формализуется как построение процедуры, определяющей принадлежность наблюдения $\bar{x} \in X$, множеству $X_{\text{норма}}$, что формально может быть записано в виде отображения:

$$a: X \to \{0,1\}, a(\bar{x}) = \begin{cases} 1, \text{если } \bar{x} \notin X_{\text{норма}} \\ 0, \text{если } \bar{x} \in X_{\text{норма}} \end{cases}. \quad (1.4)$$

При этом множество $X_{\text{норма}}$ не задано явно и должно быть приближённо определено по данным, доступным в процессе информационного обмена между ВС и наземными системами УВД. Такая формализация допускает реализацию через частотные, статистические или структурные признаки и не требует жёсткой фиксации классов заранее известных атак.

В целях решения поставленной научно-технической задачи обнаружения НСВ в контуре УВД требуется решить следующие задачи:

1. на основе проведенного анализа разработать математические модели СПД в контуре УВД в условиях НСВ, описывающие структуру сети и характер вмешательства;

2. разработать методы и алгоритмы обнаружения НСВ в контуре УВД на основе разработанных математических моделей и методов частотного анализа без этапа предварительного обучения;

3. произвести апробацию предложенных методов и алгоритмов и оценить их эффективность путём экспериментального исследования на моделируемых сценариях вмешательства в контур управления воздушным движением, выполнить сравнительный анализ полученных результатов с известными решениями, предложить рекомендации по внедрению.

Выводы по главе 1

В первой главе были получены следующие основные результаты и выводы:

1. проведён обзор текущего состояния сетей передачи данных в контуре УВД. Показано, что активное внедрение цифровых технологий и рост объёмов передаваемой информации приводят к увеличению количества потенциальных уязвимостей и появлению новых векторов атак в авиационной отрасли;

2. проведена классификация угроз НСВ, актуальных для авиационных сетей передачи данных, таких как ACARS/CPDLC. Установлено, что применяемые механизмы защиты зачастую не учитывают специфические требования и условия эксплуатации авиационных систем, что снижает их эффективность при противодействии НСВ;

3. показано, что традиционные сигнатурные методы обнаружения не обеспечивают своевременного выявления новых типов НСВ. Проведен анализ известных методов машинного обучения в рамках задачи обнаружения НСВ в контуре УВД;

4. сделан вывод о необходимости разработки новых методов и алгоритмов, учитывающих специфику контура УВД без потери качества классификации и обеспечивающих допустимое время обработки при анализе большого объема информационного обмена в условиях отсутствия обучающего набора данных;

5. сформулированы задачи диссертационного исследования, направленные на решение актуальной научно-технической задачи разработки методов и алгоритмов обнаружения НСВ в контуре УВД на основе машинного обучения, имеющей существенное значение для развития авиационной отрасли.

Глава 2. Разработка математических моделей сетей передачи данных в контуре управления воздушным движением в условиях несанкционированного вмешательства

2.1. Разработка модели информационного обмена в контуре управления воздушным движением

Математическая модель каналов информационного обмена и возможных угроз необходима для формализованного описания функционирования СПД в контуре УВД в условиях НСВ. Основной задачей является выявление взаимосвязей между легитимной сетевой активностью, характерной для АС УВД, и потенциальными сценариями НСВ, нарушающего структуру или параметры информационного обмена. Контур УВД рассматривается как логически связанная сетевая структура, уязвимая к деструктивным воздействиям, определенных в п. 1.2. При построении модели учитываются особенности архитектуры сети, топология взаимодействия между компонентами, а также возможность нарушения связности при реализации различных сценариев НСВ.

Формализация модели охватывает несколько ключевых направлений:

– описание СПД в виде графа, где узлы соответствуют компонентам системы, а рёбра представляют каналы связи;

– вероятностная модель отказов узлов и каналов связи;

– определение угроз, связанных с НСВ в работу авиационных систем;

– оценка вероятности обнаружения НСВ.;

– расчёт вероятности нарушения связности сети и потери критически важной информации;

– разработка стратегий защиты, направленных на предотвращение вмешательства в работу авиационных систем;

Для начала необходимо формализовать структуру авиационной сети передачи данных. Естественным образом сеть представляется в виде графа G:

$$G = (V, E), \tag{2.1}$$

где: $V = \{v_1, v_2, \dots, v_n\}$ – множество узлов (вершин),

$E = \{e_1, e_2, \dots, e_m\}$ – множество соединений (рёбер) между ними.

Узлами графа могут выступать бортовые компьютеры ВС, наземные центры управления (в том числе пункты дистанционного управления БАС), ретрансляторы и прочие компоненты в контуре УВД. Рёбра графа отображают каналы передачи данных (радиолинии, спутниковые каналы и т.п.), обеспечивающие связь между узлами. Будем считать, что граф неизменен структурно во времени, то есть состав узлов и наличие каналов задано исходно.

Каждый компонент сети обладает определённой надёжностью и, соответственно, ненулевой вероятностью отказа. Введём следующие обозначения: пусть p_i – вероятность безотказной работы узла i в рассматриваемый период:

$$q_i = 1 - p_i\ , \tag{2.2}$$

где: q_i – вероятность отказа этого узла по техническим причинам.

Аналогично, для каждого канала связи (рёбра) $e \in E$ обозначим через p_e вероятность его исправного функционирования:

$$q_e = 1 - p_e\ , \tag{2.3}$$

где q_e – вероятность отказа канала. Предполагается, что отказы отдельных узлов и каналов являются случайными событиями, которые с заданными вероятностями могут происходить независимо друг от друга (данное допущение упрощает анализ, хотя в реальности могут иметь место коррелированные сбои).

Для оценки работоспособности всей сети вводится понятие связности графа. Сеть считается связной и функционирующей, если для любой пары критически важных узлов (например, «борт – центр УВД» для пилотируемого ВС или «БАС – центр управления» для беспилотной системы) существует хотя бы один путь в графе, соединяющий их посредством исправных узлов и каналов. Соответственно, событие нарушения связности означает, что найдётся хотя бы одна пара узлов, между которыми не осталось работоспособного маршрута передачи данных. Вероятность сохранения связности сети можно рассматривать как показатель её общей надёжности. Вычисление этой вероятности эквивалентно задаче оценки надежности графа с заданными надёжностями элементов.

В общем случае точное вычисление вероятности связности для произвольного графа представляет значительные трудности, так как требует учета всех возможных комбинаций отказов. Однако для некоторых типовых конфигураций сети можно записать аналитические выражения. Рассмотрим случай, когда важные узлы соединены последовательной цепочкой из N каналов. В этом случае сеть остаётся связной только при работоспособности каждого из каналов. Тогда вероятность связности R_{conn} определяется выражением

$$R_{conn} = \prod_{e=1}^{N} p_e \, . \tag{2.4}$$

При наличии параллельного резервирования каналов надёжность сети возрастает. Для случая двух параллельных каналов между одними и теми же узлами вероятность полной потери связи равна произведению вероятностей отказа каждого канала. Следовательно, вероятность сохранения связи через хотя бы один из каналов определяется выражением

$$R_{conn} = 1 - (1 - p_1)(1 - p_2) \, . \tag{2.5}$$

Приведённые примеры демонстрируют влияние топологии сети на её надёжность: наличие альтернативных маршрутов (дублирующих узлов или каналов) снижает вероятность полного отказа связи. В контуре УВД структура СПД является сложной, включает множество узлов и пересекающихся маршрутов. Для общей модели введём множество:

$$C = \{C_1, C_2, \dots, C_K\}, \tag{2.6}$$

где C – множество минимальных разрезов графа, то есть критических наборов компонентов, отказ которых приводит к нарушению связности сети. Иными словами, каждый $C_K \subseteq V \cup E$ представляет собой минимальное множество узлов и/или рёбер, при одновременном выходе из строя которых граф G распадается на несвязные части.

Контур УВД, помимо случайных сбоев, подвержен и целенаправленным воздействиям (см. п. 1.2). Для количественного анализа угроз необходимо ввести вероятностную модель подобных воздействий.

Предположим, что для каждого элемента сети можно оценить вероятность успешной атаки в рассматриваемый период. Обозначим через P_i^{attack} вероятность того, что узел $i \in V$ будет скомпрометирован злоумышленником (атакован с нарушением его функционирования). Аналогично, для канала $e \in E$ введём вероятность P_e^{attack}, отражающую вероятность того, что по каналу будет проведена успешная атака. Как правило, значения P_i^{attack} невелики, но ненулевые, что указывает на возможность успешного проведения атаки при определённых условиях.

НСВ по своей сути приводит к выходу из строя узла или канала аналогично техническому отказу, но имеет иную природу. Поэтому целесообразно рассматривать атаку как дополнительный случай отказа компонента. Можно объединить две причины нарушения работы – случайный отказ и успешную атаку – в единой вероятностной модели элемента сети. Если считать эти причины статистически независимыми, то итоговая вероятность того, что компонент j выйдет из строя (либо из-за отказа, либо из-за атаки), определяется следующим образом:

$$q_j^{total} = 1 - \left(1 - q_j\right)\left(1 - P_j^{attack}\right), \quad (2.7)$$

где: q_j - вероятность технического отказа компонента (узла или канала) j,

q_j^{total} - суммарная вероятность того, что компонент j окажется неработоспособным в результате либо отказа, либо атаки.

Формула (2.7) показывает, что компонент выходит из строя, если происходит хотя бы одно из двух событий: внутренний сбой или успешное внешнее воздействие. Эквивалентно вероятность безотказной работы с учётом атак можно записать в виде:

$$p_j^{total} = \left(1 - q_j\right)\left(1 - P_j^{attack}\right), \quad (2.8)$$

то есть компонент продолжит функционировать только при условии отсутствия отказа и успешной атаки.

Вероятности P_j^{attack} отражают уязвимость элементов сети. Злоумышленник, как правило, стремится атаковать наиболее критичные узлы и связи, вывод из строя которых приводит к максимальному нарушению работы сети. В терминах ранее введённых минимальных разрезов C_K целенаправленная атака может быть нацелена на выведение из строя всех компонентов некоторого разреза C_K, что гарантированно нарушит связность сети. Однако возможность реализации подобной комплексной атаки зависит от ресурсов нарушителя и может быть маловероятной, если разрез включает значительное число элементов.

Математическая модель должна учитывать различные сценарии атак: от одиночных воздействий на отдельные узлы или каналы до комбинированных атак, нацеленных на несколько элементов сети одновременно. Для каждого сценария можно задать соответствующие вероятности реализации угрозы.

Важным фактором, снижающим влияние угроз, является система обнаружения НСВ. Предположим, что в контуре УВД внедрены средства мониторинга и диагностики, позволяющие выявлять аномалии в передаче данных. К таким средствам относятся системы обнаружения вторжений, анализаторы трафика, механизмы контроля целостности сообщений и другие методы

мониторинга. Их основная задача – выявление атак или аномальных событий с высокой вероятностью и минимальным числом ложных срабатываний.

Моделирование процесса выявления атак можно выполнить в вероятностной постановке. Введём два ключевых показателя эффективности системы обнаружения:

1. p_d - вероятность правильного обнаружения атаки (чувствительность системы);

2. p_{fa} - вероятность ложного срабатывания системы, то есть формирования инцидента при отсутствии реальной угрозы.

Если в сети происходит атака, то с вероятностью p_d она будет зафиксирована средствами мониторинга, а с вероятностью $1 - p_d$ атака останется незамеченной. Значение p_d, близкое к 1, означает эффективное обнаружение почти всех атак, тогда как его снижение указывает на вероятность пропуска угроз. Показатель p_{fa} характеризует избирательность системы: при отсутствии атак ложные срабатывания возникают с вероятностью p_{fa}. Желательно, чтобы этот параметр был минимальным, чтобы избежать избыточной нагрузки на операторов и системы обработки инцидентов.

Следовательно, вероятность успешной атаки, которая не была выявлена средствами мониторинга, уменьшается на фактор p_d. Формально введём эффективную вероятность успешной атаки с учётом системы обнаружения:

$$\tilde{P}_j^{attack} = P_j^{attack}(1 - p_d), \tag{2.9}$$

Подставляя $\tilde{P}_j^{attack}$ вместо P_j^{attack} в ранее полученное выражение для вероятности отказа компонента (2.7), можно пересчитать итоговую вероятность его неработоспособности с учётом мониторинга. Таким образом, повышение эффективности обнаружения (увеличение p_d) снижает вероятность отказа сети в результате атак.

Объединив вышеописанные элементы — надёжность компонентов, вероятность атак и вероятность их обнаружения — можно оценить совокупный риск для СПД в контуре УВД. Под риском нарушения работы сети будем понимать

вероятность события F, при котором сеть теряет связность, то есть становится невозможным обмен данными между определёнными узлами. Эта вероятность определяется комбинацией отказов и не обнаруженных атак, затрагивающих узлы и каналы. Событие F эквивалентно ситуации, при которой выходят из строя все компоненты по крайней мере одного из минимальных разрезов $C_K \in C$ графа сети. Для оценки риска необходимо учесть вероятность каждого такого неблагоприятного исхода.

Обозначим через $\tilde{q}_i$ эффективную вероятность отказа компонента j с учётом атак и их возможного обнаружения. В соответствии с предыдущими разделами, для любого узла или канала j выполняется:

$$\tilde{q}_i = 1 - (1 - q_j)(1 - \tilde{P}_j^{attack}), \tag{2.10}$$

где: q_j - вероятность технического отказа узла или канала j;

$\tilde{P}_j^{attack}$ - вероятность успешной необнаруженной атаки на компонент j.

Произведение $\prod_{j \in C_K} \tilde{q}_i$ соответствует вероятности того, что все элементы разреза C_K одновременно выйдут из строя. Соответственно, вероятность нарушения связности сети можно оценить как сумму вероятностей отказа таких критических наборов. Используя объединение событий по всем минимальным разрезам, получаем приближённую оценку риска:

$$P(F) = \sum_{k=1}^{K} \prod_{j \in C_K} \tilde{q}_i . \tag{2.11}$$

В данной формуле учитываются все возможные критические разрезы сети. Однако сумма вероятностей несколько завышает истинное значение $P(F)$, поскольку различные разрезы могут иметь общие компоненты, что делает события их отказов зависимыми. Для более точного расчёта следовало бы использовать принцип включений-исключений или другие методы теории надёжности. Тем не менее, выражение (2.11) даёт полезное приближение риска и позволяет сравнивать различные конфигурации сети и меры защиты.

Если какой-либо разрез сети имеет существенно более высокую вероятность отказа, чем остальные, то риск $P(F)$ определяется в первую очередь этим разрезом. Например, если в сети существует единственный критически важный узел, через который проходят все данные, то вероятность полного отказа сети приближённо равна $\tilde{q}_i$ — эффективной вероятности выхода из строя данного узла. В более сбалансированных сетях, где отказ отдельного элемента не приводит к немедленному разрыву связи, в расчёте риска участвует несколько слагаемых.

После количественной оценки риска следующим этапом является разработка мер по его минимизации. Оптимизация стратегии защиты СПД в контуре УВД направлена на снижение вероятности успешных атак и отказов, наиболее существенно влияющих на связность сети. В рамках разработанной математической модели это означает уменьшение значений $\tilde{q}_i$ для элементов, внесших наибольший вклад в суммарный риск $P(F)$. Практически это может быть достигнуто двумя путями:

1. повышением надёжности компонентов (уменьшением q_j);

2. снижением вероятности реализации атак (уменьшением P_j^{attack} либо повышением p_d для этих атак, что увеличивает вероятность их обнаружения).

Формально задачу минимизации риска можно представить в виде оптимизационной задачи выбора защитных мер при ограниченных ресурсах. Пусть $X = \{x_1, x_2, \dots, x_n\}$ – набор бинарных переменных, каждая из которых соответствует определённой мере защиты для конкретного элемента сети (узла или канала). Значение $x_i = 1$ означает, что на компонент i выделены ресурсы защиты. Значение $x_i = 0$ означает, что дополнительных мер не применено.

Влияние защитных мер выражается в уменьшении вероятностей отказа и атаки на компонент. Если $x_i = 1$, то:

– надёжность компонента увеличивается (его вероятность отказа q_j уменьшается до $q_j{}'$);

– вероятность успешной атаки снижается (P_j^{attack} уменьшается до $P_j^{attack\prime}$).

Конкретные значения $q_j{}'$ и $P_j^{attack\prime}$ зависят от эффективности выбранной меры защиты. Оптимальное распределение ресурсов, минимизирующее риск, можно выразить следующим образом:

$$X^* = \arg\min_X P(F|X)\,, \tag{2.12}$$

где $P(F|X)$ – вероятность нарушения связности сети при заданном наборе реализованных мер защиты X. Ограничения на выбор защитных мер могут быть заданы в виде:

$$\sum_i c_i x_i \le C_{max}\,, \tag{2.13}$$

где: c_i – стоимость или трудоёмкость защиты i-го элемента сети;

C_{max} – общий доступный ресурс (например, бюджет или технические ограничения).

Соотношение (2.12) описывает задачу оптимального резервирования и защиты сети. Требуется определить такой набор X^*, при котором вероятность $P(F|X)$ минимальна. В общем случае решение является комбинаторным и характеризуется экспоненциальным числом вариантов, особенно при увеличении размера сети.

При этом структура графа существенно влияет на результат. Анализ минимальных разрезов позволяет выделить элементы, оказывающие наибольшее влияние на связность. Именно на этих узлах и каналах целесообразно сосредоточить защитные меры.

Разработанная математическая модель угроз СПД контура УВД в условиях НСВ позволяет оценивать вероятностные характеристики отказов и целенаправленных атак, а также их влияние на связность сети. На основе модели могут быть определены критичные узлы и каналы. Учитывается и эффективность мониторинга: увеличение вероятности обнаружения атак при снижении ложных срабатываний приводит к уменьшению общего риска нарушения работы сети.

Модель используется для выбора и распределения средств защиты. Она даёт возможность ранжировать угрозы по степени влияния и сосредоточить защитные меры на наиболее значимых элементах сети.

При этом вероятностная модель описывает состояние сети в статическом виде. Для анализа развития НСВ во времени необходимо учитывать динамику изменения состояний элементов контура УВД и переходы между ними.

Результаты данного параграфа были опубликованы в [101].

2.2. Разработка модели несанкционированного вмешательства в контуре управления воздушным движением

Для обоснования и оценки устойчивости элементов СПД в контуре УВД к НСВ необходимо формализовать последовательность действий нарушителя и возможные отклонения работы каналов обмена данными. Моделирование таких процессов позволяет наглядно проследить, при каких условиях возникает переход системы из штатного режима в состояние, связанное с нарушением управления или потери целостности информации.

Для формализованного описания процессов, связанных с реализацией угроз НСВ, в работе использован аппарат сетей Петри. Такой выбор обусловлен следующими преимуществами сетей Петри: наличие графического представления моделируемой системы, возможность наглядного описания взаимодействия между процессами, развитый арсенал методов анализа, проверенная практика применения сетей Петри для моделирования мультипрограммных, асинхронных, распределённых, параллельных, недетерминированных и/или стохастических информационно-вычислительных систем и процессов обмена данными в них.

Свойство достижимости сети Петри означает, что произвольная маркировка M_n достижима из начальной маркировки M_0; то есть существует последовательность запусков переходов $\sigma = t_1, t_2 \dots t_n$, приводящая систему от M_0 к M_n.

Свойство активности сети Петри тесно связано с отсутствием возможности взаимной блокировки переходов в процессе функционирования системы. Сеть Петри считается активной, если независимо от достигнутой маркировки M для любого перехода существует последовательность состояний, приводящая к его запуску. Это означает, что для активной сети Петри при любой последовательности запусков полностью исключена возможность взаимной блокировки.

Задача моделирования угроз НСВ сформулирована следующим образом:

– дана сеть Петри PN, моделирующая нормальное функционирование элементов контура УВД (начальная маркировка сети — M_0; сеть обладает свойствами достижимости и активности);

– требуется дополнить исходную сеть Петри элементами, описывающими процесс НСВ, и определить достижимость во вновь полученной сети Петри состояния, соответствующего реализации цели вмешательства, или проверить активность переходов исходной сети с учётом влияния добавленных элементов.

Проведённый анализ показал, что для решения задач исследования временных характеристик моделируемых процессов целесообразно использовать расширение формализма сетей Петри, известное как *E*-сети. В отличие от классических сетей Петри, *E*-сети позволяют эффективно описывать не только динамику и взаимодействие параллельных процессов, но и управление перемещением маркеров с учётом состояния памяти сети, временные задержки на переходах, а также разнообразные преобразования данных, ассоциированных с перемещающимися маркерами в виде признаков (атрибутов) или глобальных параметров сети. Упрощенная Е-модель НСВ на контур УВД представлена на рисунке 2.1.

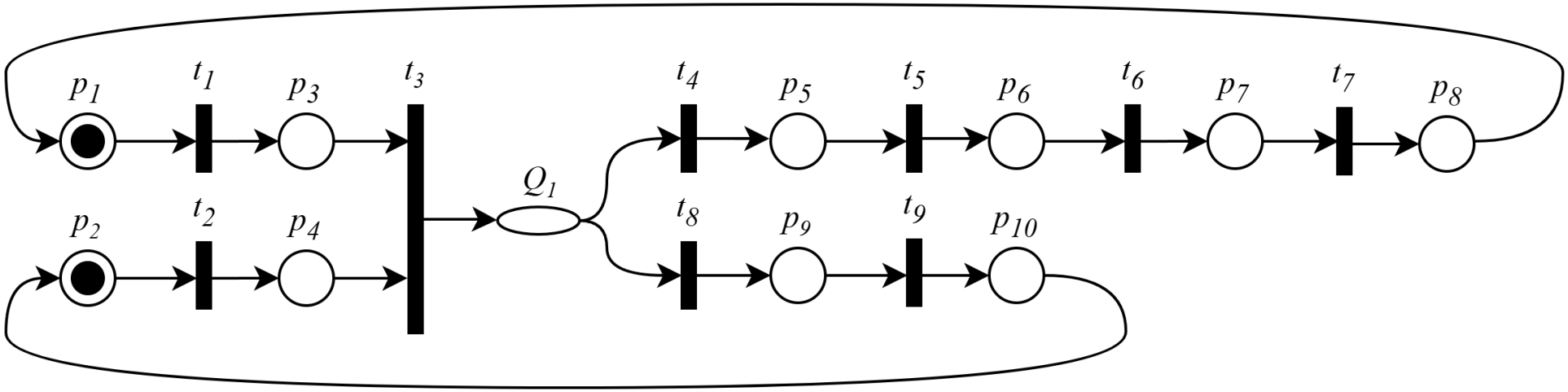

Рисунок 2.1 – Упрощенная Е-модель НСВ в контуре УВД

Описание позиций и переходов модели приведено в таблицах 2.1 и 2.2.

Таблица 2.1. Позиции Е-модели НСВ в контуре УВД

Позиция	Характеристики позиции (перехода)
p_1	Стадия генерации корректного управляющего или информационного запроса со стороны легитимного объекта в контуре УВД (например, пилотируемый ВС или наземная АС УВД)
p_2	Стадия генерации сетевого запроса, инициированного потенциальным нарушителем в контуре УВД
p_3	Корректный запрос после предварительной подготовки к постановке в очередь обработки
p_4	Запрос потенциального нарушителя после формирования и подготовки к постановке в очередь
Q_1	Логический буфер (очередь) обработки управляющих и информационных запросов в контуре УВД; модель очереди отражает ограниченную пропускную способность сегмента информационного взаимодействия
p_5	Стадия непосредственной обработки запроса в рамках наземного сегмента или бортовой подсистемы в контуре УВД
p_6	Стадия выделения и фиксации вычислительного ресурса, канала связи или полосы пропускания для выполнения обработки
p_7	Формирование и отправка отклика после завершения обработки
p_8	Освобождение занятого ресурса и завершение цикла обработки легитимного запроса
p_9	Фиксация состояния переполнения очереди (отражает исчерпание допустимой нагрузки на сегмент обработки)
p_{10}	Перевод в состояние отказа в обслуживании или сбоя вследствие переполнения очереди и некорректной обработки

Таблица 2.2 Переходы E-модели НСВ на контур УВД

Переход	Характеристики перехода
t_1	Формирование корректного запроса легитимным элементом контура УВД
t_2	Формирование запроса потенциальным нарушителем или вредоносным агентом
t_3	Постановка подготовленного запроса в очередь обработки (Q1) с учётом текущей загрузки сегмента
t_4	Выборка запроса из очереди для последующей штатной обработки при нормальных условиях эксплуатации
t_5	Выделение и закрепление необходимого вычислительного или канального ресурса для обработки запроса
t_6	Формирование и передача управляющего или информационного отклика после завершения обработки
t_7	Освобождение занятого ресурса и завершение цикла обработки
t_8	Обнаружение состояния переполнения очереди при превышении пороговых значений загрузки
t_9	Перевод контура УВД в состояние сбоя или отказа вследствие зафиксированного переполнения

Формально предложенная E-сетевая модель задается в виде (2.14):

$$E = \langle P, T, I, O, G \rangle , \tag{2.14}$$

где $P = \{p_1, p_2, p_3, p_4, Q_1, p_5, p_6, p_7, p_8, p_9, p_{10}\}$ – множество позиций,

$T = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9\}$ – множество переходов,

I и O – множества входных и выходных функций переходов,

$G = \langle k, F, counter \rangle$ - множество глобальных параметров (k — число узлов, подлежащих сканированию, $F = \{F_i\}$, $F_i = \langle N_a, N_p, N_s \rangle$ - характеристика i-го

целевого узла, *counter* — переменная, используемая в качестве счётчика текущего объекта сканирования).

Общий вид маркера модели можно представить в виде (2.15):

$$M = \langle N_a, N_p, Q \rangle , \tag{2.15}$$

где N_a — адрес целевого узла, N_p — порт назначения, Q — тип посылаемого запроса.

В начальном состоянии единичный маркер размещается в позиции p_1 и p_2, глобальные параметры G инициализируются заранее, переменная counter устанавливается в ноль.

Переход t_1 формирует легитимный запрос, выбирая атрибуты маркера из F по индексу counter. Переход t_2 формирует запрос потенциального нарушителя. Постановка в очередь выполняется переходом t_3, если выполняется условие $M(Q_1) < Cap$, где Cap — предельная ёмкость буфера, задаваемая в параметрах G. Выборка маркера из очереди для штатной обработки осуществляется через переходt_4; переполнение фиксируется через t_8, что переводит сеть в состояние отказа (через t_9). После штатной обработки маркер возвращается к генерации новых легитимных запросов, после фиксации переполнения — к повторной генерации атакующего запроса.

Таким образом, предложенная универсальная E-модель обеспечивает формализованное описание типовых сценариев НСВ в контур УВД. Представленная модель описывает развитие процесса во времени и позволяет формализовать переходы между состояниями элементов СПД в контуре УВД.

Полученная формализация информационного обмена и сценариев НСВ создаёт основу для разработки математической модели формирования нарушений информационного обмена в контуре УВД на основе изменения наблюдаемых параметров во времени.

2.3. Разработка модели формирования нарушений информационного обмена в контуре управления воздушным движением

Функционирование сетевого информационного обмена в контуре УВД рассматривается как случайный процесс, отражающий изменение параметров взаимодействия между бортовыми и наземными подсистемами во времени. В отличие от известных моделей надёжности, в данном случае объектом анализа является структура и динамика информационного обмена.

Для формализации вводится случайный процесс $Z_0(t)$, характеризующий состояние обмена в штатных условиях. Данный процесс отражает изменение параметров сетевого взаимодействия, включая интенсивность передачи сообщений, интервалы между кадрами, долю служебных сообщений и согласованность протокольных состояний.

В условиях НСВ на контур УВД воздействует внешний поток событий, приводящий к изменению параметров обмена. Пусть $N(t)$ — случайный процесс, определяющий число актов вмешательства на интервале времени $[0, t]$. Предполагается, что $N(t)$ является пуассоновским процессом с интенсивностью λ, что позволяет записать:

$$R(N(t) = n) = \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t}, n = 0, 1, 2, \ldots \quad (2.16)$$

Каждое воздействие приводит к изменению состояния системы. Обозначим через ξ_k вклад k-го воздействия в деградацию информационного обмена. Под деградацией информационного обмена понимается накопление отклонений параметров сетевого взаимодействия от штатных значений, приводящее к нарушению согласованности протокольных состояний и увеличению задержек передачи данных. Тогда суммарное влияние внешних воздействий определяется как

$$\Delta Z(t) = \sum_{k=1}^{N(t)} \xi_k \,, \tag{2.17}$$

При этом, если $N(t) = 0$, то и сумма (2.17) полагается равной нулю. Тогда совокупное состояние системы имеет вид:

$$Z(t) = Z_0(t) + \Delta Z(t) \,. \tag{2.18}$$

Данное представление отражает, что состояние обмена формируется как результат наложения штатной динамики и внешних воздействий. Предполагается статистическая независимость процесса $Z_0(t)$, случайных величин ξ_k и процесса $N(t)$.

Для анализа вероятностных характеристик состояния системы определяется функция распределения случайной величины $Z(t)$:

$$F_Z(z,t) = R(Z(t) < z) = R(Z_0(t) + \sum_{k=1}^{N(t)} \xi_k < z) \,. \tag{2.19}$$

Так как число воздействий является случайной величиной, применяется формула полной вероятности по $N(t)$:

$$F_Z(z,t) = \sum_{n=0}^{\infty} R\left(Z_0(t) + \sum_{k=1}^{n} \xi_k < z\right) R(N(t) = n) \,. \tag{2.20}$$

С учётом распределения Пуассона в выражении (2.16) получаем:

$$F_Z(z,t) = \sum_{n=0}^{\infty} R\left(Z_0(t) + \sum_{k=1}^{n} \xi_k < z\right) \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t} \,. \tag{2.21}$$

Пусть процесс $Z_0(t)$ имеет плотность распределения $f_{Z_0}(z,t)$, а случайные величины ξ_k независимы и одинаково распределены с плотностью $f_\xi(x)$. Тогда

сумма, определенная в формуле (2.17) имеет плотность $f_{\xi}^{*n}(u)$, равную n-кратной свёртке распределения $f_{\xi}(x)$. В этом случае условная вероятность может быть представлена в интегральной форме:

$$R\left(Z_0(t) + \sum_{k=1}^{n} \xi_k < z\right) = \int_0^z \int_0^{z-u} f_{Z_0}(v,t)\, f_{\xi}^{(*n)}(u)\, dv du, \tag{2.22}$$

при допущении, что $Z_0(t) \geq 0$ и $\xi_k \geq 0$. Подставляя это выражение, получаем окончательное представление функции распределения:

$$F_Z(z,t) = \sum_{n=0}^{\infty} \left[\int_0^z \int_0^{z-u} f_{Z_0}(v,t)\, f_{\xi}^{*n}(u)\, dv du\right] \cdot \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t}\,. \tag{2.23}$$

Работоспособность системы определяется ограничениями на допустимое состояние информационного обмена. Вводится порог H, при превышении которого функционирование считается нарушенным:

$$Z(t) > H. \tag{2.24}$$

Данный механизм соответствует накопленному нарушению и обусловлен суммарным влиянием множества воздействий. Помимо этого, учитывается возможность мгновенного нарушения функционирования вследствие отдельного воздействия. Пусть D_0 — критическое значение воздействия, тогда условие мгновенного нарушения имеет вид:

$$\xi_k > D_0. \tag{2.25}$$

Таким образом, реализуются два механизма нарушения: накопленный и мгновенный, а время потери работоспособности определяется как

$$T = \min(T_{\text{нак}}, T_{\text{мгн}}). \tag{2.26}$$

Вероятность отсутствия мгновенного нарушения при фиксированном числе воздействий n определяется как:

$$R(\xi_1 \leq D_0, \dots, \xi_n \leq D_0) = \left[F_{\xi}(D_0)\right]^n, \tag{2.27}$$

Где $F_\xi(x)$ – функция распределения случайной величины ξ_k. Тогда вероятность отсутствия мгновенного нарушения $R_{\text{мгн}}(t)$ на интервале $[0, t]$ равна

$$R_{\text{мгн}}(t) = \sum_{n=0}^{\infty} \left[F_\xi(D_0)\right]^n \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t}. \quad (2.28)$$

Используя разложение экспоненциального ряда, получаем замкнутую форму:

$$R_{\text{мгн}}(t) = e^{-\lambda t} \sum_{n=0}^{\infty} \frac{(\lambda \cdot t \cdot F_\xi(D_0))^n}{n!} = e^{-\lambda t(1-F_\xi(D_0))}. \quad (2.29)$$

Вероятность безотказного функционирования системы определяется как вероятность одновременного отсутствия накопленного и мгновенного нарушения для всех k-воздействий:

$$R(t) = R(Z(t) < H, \xi_k \le D_0 \forall k \le N(t)). \quad (2.30)$$

Раскладывая это выражение по числу воздействий, получаем:

$$R(t) = \sum_{n=0}^{\infty} R\left(Z_0(t) + \sum_{k=1}^{n} \xi_k < H, \xi_1 \le D_0, \dots, \xi_n \le D_0\right) \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t}. \quad (2.31)$$

Аналогично вводятся вероятности реализации каждого механизма нарушения. Вероятность накопленного нарушения при отсутствии мгновенного определяется как:

$$Q_{\text{нак}}(t) = \sum_{n=0}^{\infty} R\left(Z_0(t) + \sum_{k=1}^{n} \xi_k > H, \xi_1 \le D_0, \dots, \xi_n \le D_0\right) \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda t}, \quad (2.32)$$

а вероятность мгновенного нарушения может быть записана через дополнение к вероятности отсутствия критических воздействий:

$$Q_{\text{мгн}}(t) = 1 - e^{-\lambda t(1-F_{\xi}(D_0))}. \quad (2.33)$$

Таким образом, модель формирования нарушений в контуре УВД описывает влияние НСВ как внешнего стохастического процесса, изменяющего параметры сетевого информационного обмена. Полученные зависимости описывают изменение наблюдаемых параметров информационного обмена во времени, что позволяет рассматривать их в качестве признаков для последующего анализа с использованием методов частотного анализа.

Выводы по главе 2

Во второй главе были получены следующие основные результаты и выводы:

1. разработана математическая модель сетей передачи данных в контуре УВД в условиях НСВ, в которой структура сети представлена в виде графа, где вершины соответствуют элементам телекоммуникационной инфраструктуры, а рёбра — каналам связи между ними. Модель позволяет формализовать взаимодействие элементов СПД и анализировать влияние НСВ на функционирование контура УВД;

2. в рамках разработанной модели учтены вероятностные характеристики отказов узлов и каналов связи, что позволяет количественно оценивать риск нарушения связности сети и деградации информационного обмена при реализации сценариев НСВ;

3. разработана универсальная *E*-модель НСВ в контуре УВД, отражающая типовые сценарии атак и учитывающая особенности функционирования авиационной телекоммуникационной инфраструктуры;

4. предложенная *E*-модель обеспечивает формализованное описание развития НСВ во времени и позволяет моделировать переходы между состояниями

элементов СПД в контуре УВД, что создаёт основу для последующего анализа признаков НСВ в информационном обмене;

5. установлено, что влияние НСВ на информационный обмен в контуре УВД может быть формализовано в виде составного стохастического процесса, включающего базовую динамику легитимного обмена и случайный поток внешних воздействий;

6. показано, что нарушение функционирования описывается двумя конкурирующими механизмами — накопленным, обусловленным суммарной деградацией параметров обмена, и мгновенным, связанным с реализацией критического воздействия, что позволяет получить аналитические выражения для вероятности безотказного функционирования и вероятностей реализации каждого механизма нарушения;

7. полученная модель формирования нарушений отражает формирование наблюдаемых параметров информационного обмена в контуре УВД в условиях НСВ и тем самым создаёт предпосылки для их агрегирования в виде признаков транзакций и последующего применения методов частотного анализа.

Глава 3. Разработка и исследование методов и алгоритмов обнаружения несанкционированного вмешательства в контуре управления воздушным движением с использованием технологий искусственного интеллекта

3.1. Разработка и исследование метода многомерного анализа частых наборов признаков транзакций информационного обмена в контуре управления воздушным движением с использованием технологий искусственного интеллекта

Задача разработки методов и алгоритмов обнаружения НСВ в контуре УВД может быть решена на основе обработки телекоммуникационного трафика VDL-2 с применением методов частотного анализа. Это позволяет выделять устойчиво повторяющиеся наборы признаков, отражающие характерные проявления атак и аномальных состояний сети. Общая схема регистрации в сети УВД и прикладной обмен CPDLC-сообщениями показан на рис. 3.1.

Для выявления устойчиво повторяющихся комбинаций признаков в потоках сетевого трафика традиционно применяются алгоритмы ассоциативного анализа, такие как метод априори (Apriori) и метод роста частых шаблонов (Frequent Pattern Growth, FP-Growth). Метод Apriori последовательно строит и проверяет кандидаты частых наборов, используя принцип антимонотонности: если набор нечастый, то и все его надмножества нечасты. Такой подход хорошо подходит для небольших и плоских данных, но плохо масштабируется при большом числе атрибутов, поскольку требует многократного сканирования базы и генерации всех возможных комбинаций.

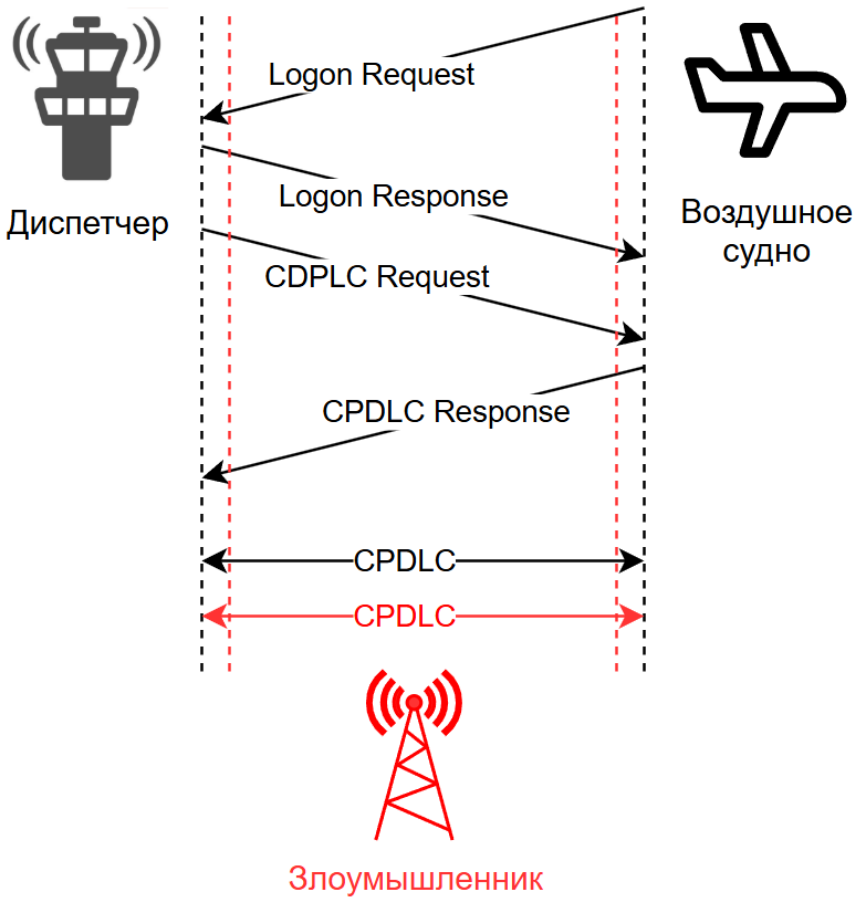

Рисунок 3.1 – Общая схема регистрации в сети УВД и прикладной обмен CPDLC-сообщениями

Более эффективный метод FP-Growth устраняет необходимость в генерации всех кандидатов. Он строит древовидную структуру (FP-дерево), где каждый путь соответствует уникальной последовательности значений признаков. Частые наборы извлекаются путём обхода дерева и анализа путей, заканчивающихся на целевой элемент. За счёт этого метод существенно ускоряет обработку, особенно при большом числе повторяющихся структур в данных.

Однако перед применением алгоритмов ассоциативного анализа необходимо определить, что именно рассматривается в качестве транзакции при анализе сетевого трафика в контуре УВД. В рамках настоящего исследования транзакция не отождествляется с отдельной протокольной единицей данных (кадром AVLC, блоком X.25, PDU CLNP или сегментом COTP). Транзакция представляет собой совокупность параметров протокольного обмена между ВС и наземной станцией за

определённый интервал времени. В неё включаются контекстные параметры соединения, характеристики потока сообщений, радиопараметры канала, а также признаки протоколов AVLC, X.25 и COTP. Такая структура позволяет применять методы анализа частых наборов признаков для выявления вмешательства в информационный обмен. Такой подход соответствует известной методике набора данных CICFlowID, где транзакции формируются на основе параметров сетевых потоков, а не из содержимого отдельных пакетов.

Для CPDLC, передаваемого по сетям ATN, исходным материалом является многоуровневый сетевой трафик, включающий заголовки протоколов AVLC, X.25, X.233 CLNP, X.224 COTP, X.225 Session SPDU и X.227 ACSE. Формирование потоков в этом случае осуществляется с использованием заголовков сетевого и транспортного уровней, функционально аналогичных использованию IP- и TCP-заголовков в наборе данных CICIDS. В частности, используются идентификаторы виртуального канала X.25 (group и channel), управляющие типы кадров X.25 (Data, Call Request, Receive Ready), заголовочные поля CLNP, а также идентификаторы транспортного соединения COTP (destination reference, признаки завершения передачи). Указанные поля применяются исключительно для разделения параллельных потоков и расчёта агрегированных характеристик трафика. Структура исходного трафика CPDLC и используемых заголовков показана на рис. 3.2 и 3.3, на которых изображены процессы регистрации в сети УВД и установление сессии CPDLC.

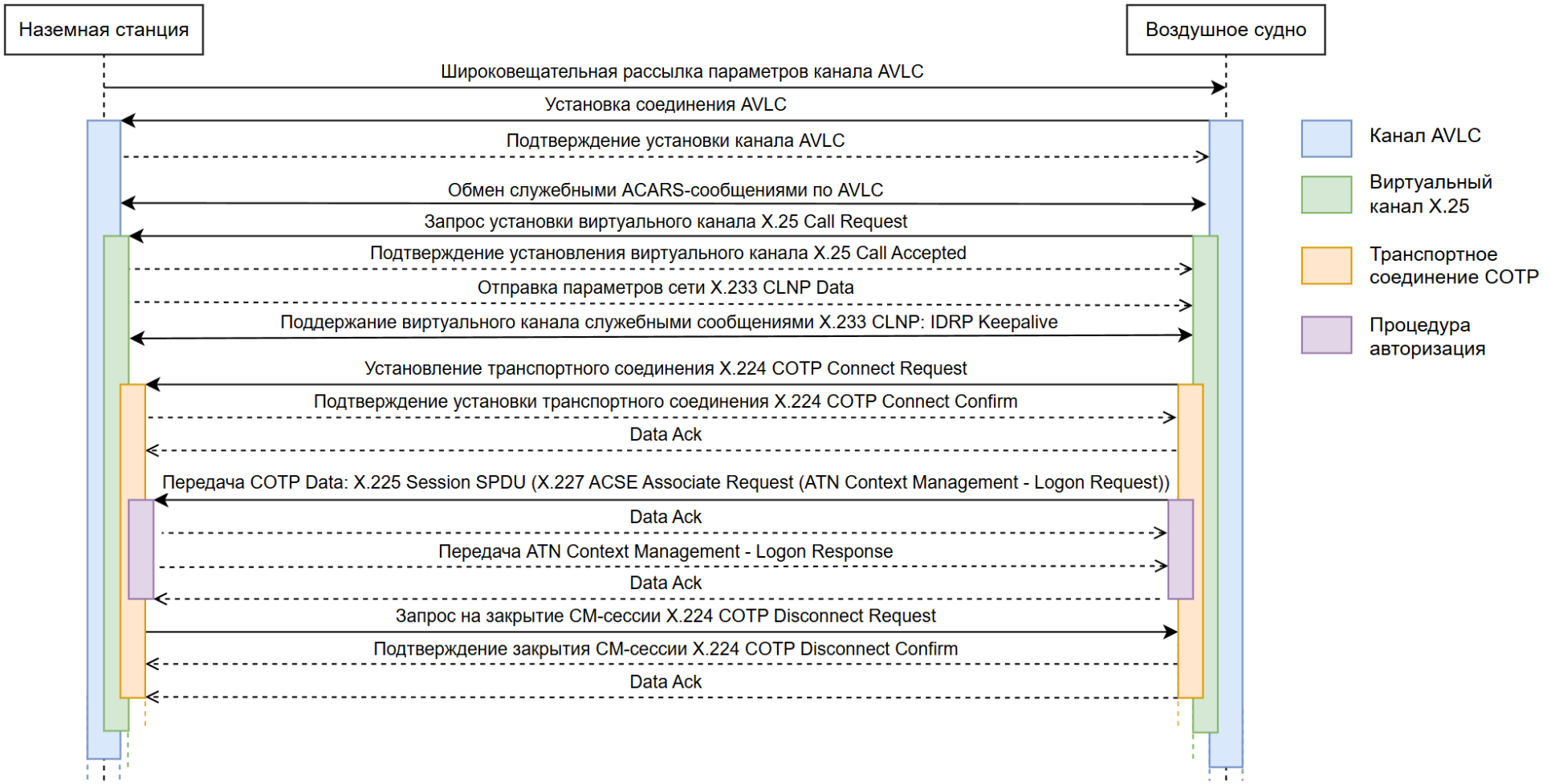

Рисунок 3.2 - Процесс регистрации в сети УВД

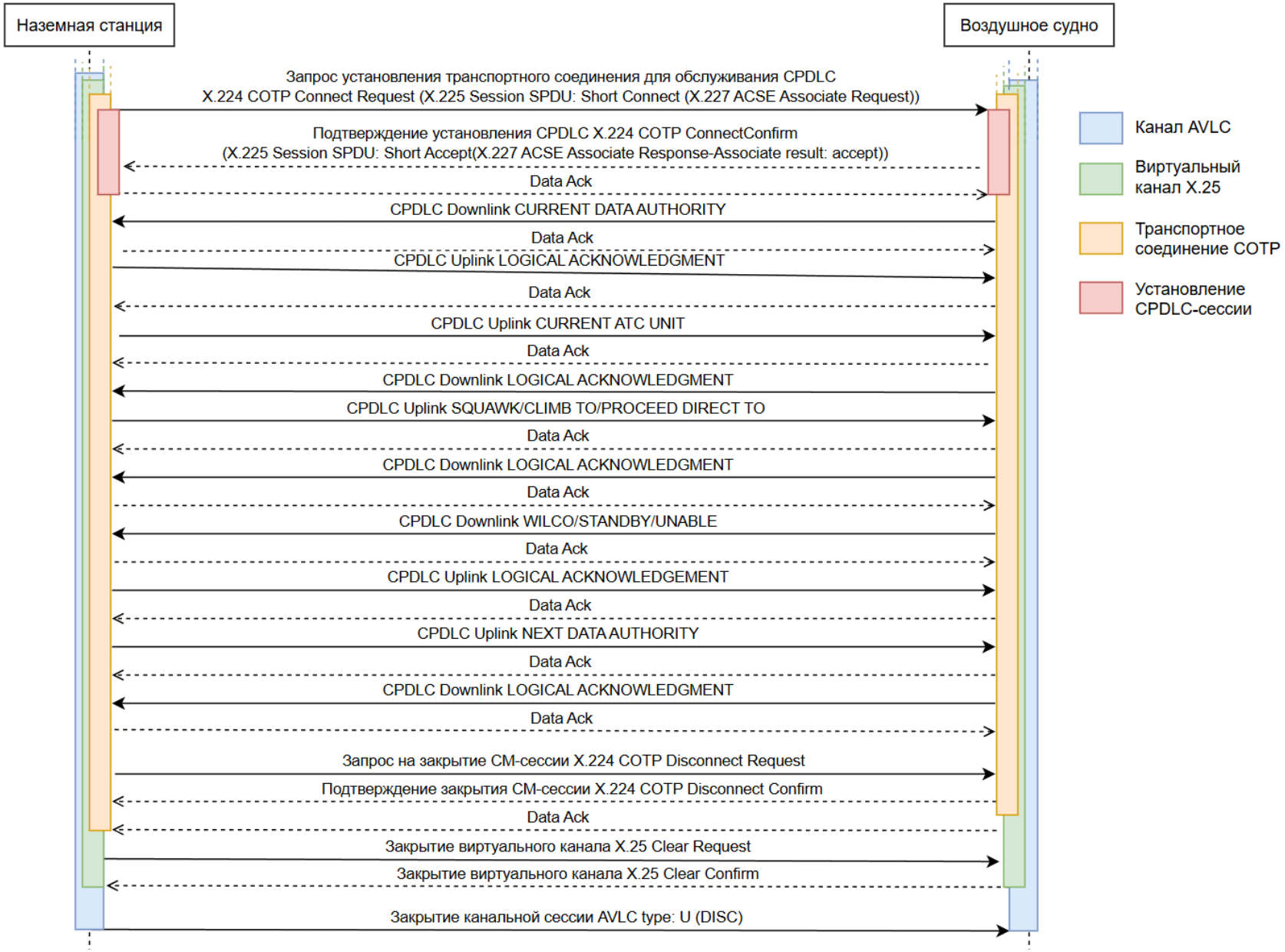

Рисунок 3.3 - Установление CPDLC-сессии и обмен прикладными сообщениями

Приведённый фрагмент иллюстрирует наблюдаемость заголовков X.25/CLNP/COTP – содержимое прикладного уровня CPDLC приведено для контекстной демонстрации и при формировании транзакций не используется.

На основе выделенных потоков CPDLC вычисляется единый набор агрегированных характеристик, включающий длительность взаимодействия, количество сообщений в прямом и обратном направлениях, суммарный объём переданных данных, а также показатели активности и простоя. После квантования указанных параметров формируются транзакции, которые используются в качестве входных данных для алгоритма многомерного анализа частых наборов признаков.

Дополнительно при формировании транзакций используются параметры физического уровня канала связи, регистрируемые при приёме авиационных радиосообщений. В анализируемом трафике VDL-2 для каждого принятого кадра доступно значение уровня принимаемого сигнала (RSSI). Значение RSSI характеризует условия распространения радиосигнала в канале «воздух–земля» и не связано с содержимым передаваемых сообщений или их прикладной семантикой. В рамках предлагаемого метода RSSI рассматривается как количественный признак физического уровня, не зависящий от используемого протокольного стека.

При формировании потока значения RSSI агрегируются по временному окну, соответствующему данному потоку информационного обмена. В простейшем случае используется среднее значение RSSI в пределах потока, которое затем подвергается квантованию и включается в состав транзакции в виде дискретного элемента, относящегося к измерению физического уровня. Включение RSSI в состав транзакции позволяет учитывать влияние условий радиоканала на устойчивость и временную структуру информационного обмена, что критично при анализе НСВ в каналах «воздух–земля», где деградация физического уровня может сопровождать активные сетевые воздействия.

Имя параметра	Описание
Flow Duration	длительность обмена в пределах транзакции
Total Fwd Packets	число сообщений в направлении GS → AC
Total Backward Packets	число сообщений в направлении AC → GS
Total Length of Fwd Packets	суммарный объём данных GS → AC
Total Length of Bwd Packets	суммарный объём данных AC → GS
Flow IAT Mean	средний интервал между сообщениями
Active Mean	средняя длительность активных участков обмена
Idle Mean	средняя длительность пауз в обмене

Таблица 1. Признаки потока

Имя параметра	Описание
Source	Источник
Destination	Приемник
Protocol	Протокол
Timestamp	Дата и время

Таблица 2. Признаки контекста

Имя параметра	Описание
RSSI	уровень принимаемого сигнала
PPM	частотное отклонение принимаемого сигнала

Таблица 3. Радиопараметры канала

Имя параметра	Описание
AVLC I Count	число информационных кадров
AVLC S Count	число служебных кадров
AVLC U Count	число управляющих кадров
X25 Data Count	число кадров передачи данных
X25 RR Count	число кадров подтверждения
COTP CC Count	число подтверждений соединения

Таблица 4. Признаки протоколов

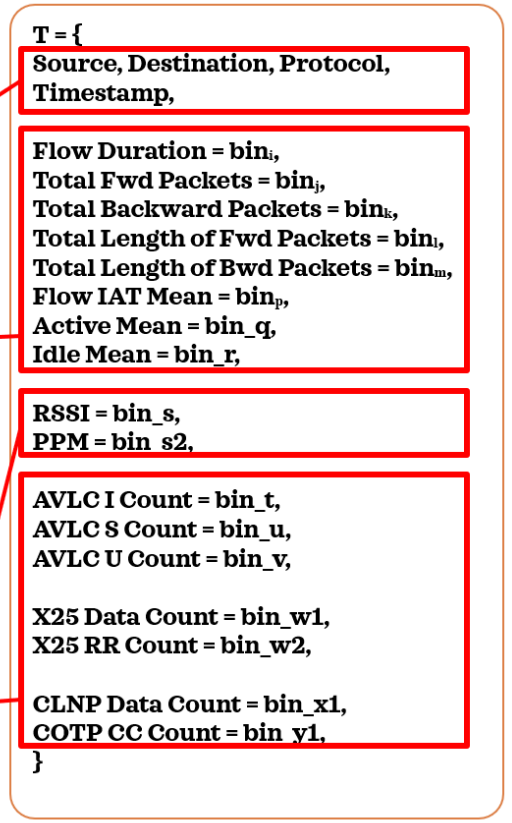

Рисунок 3.4 - Принцип формирования многомерной транзакции

Таким образом, при анализе многомерных событий информационного обмена в контуре УВД известные методы Apriori и FP-Growth оказываются недостаточными. Это обусловлено тем, что они не учитывают структуру данных, в которых каждая транзакция представлена множеством разнотипных признаков.

Для решения этой проблемы в рамках настоящего исследования разработан метод многомерного анализа частых наборов признаков транзакций информационного обмена в контуре УВД, модифицирующий известный метод FP-Growth под особенности многомерных данных, характерных для разнородных источников в контуре УВД (т.е. как бортовыми системами, так и наземными узлами сети). Его применение позволяет выявлять частые сочетания признаков, встречающиеся одновременно в различных измерениях, что особенно важно при обработке событий, формируемых разнородными источниками в гетерогенной инфраструктуре воздушного транспорта.

Ключевым отличием предлагаемого метода от известного FP-Growth является введение понятия измерения (атрибута) для каждого элемента. В типичных реализациях FP-Growth элемент представляет собой единственное значение без указания его принадлежности к определенному полю (например, «80» может означать как порт, так и длину пакета). В предлагаемом методе каждый элемент кодируется в виде пары: $\{\text{значение}, \text{измерение}\}$. Например,

элемент $a{:}\,1$ означает значение a из первого атрибута,

элемент $d{:}\,2$ — значение d из второго атрибута.

Таким образом, данные из разных источников могут быть сопоставлены в одном дереве, не теряя своей контекстной структуры.

Предлагаемый метод использует модифицированное многомерное FP-дерево, в котором каждый узел хранит не только значение признака, но и его принадлежность к измерению. Структура дерева строится в два этапа:

1. Первый проход по данным — производится подсчёт частоты всех возможных значений по каждому измерению. Редкие значения, не

удовлетворяющие минимальному порогу поддержки, отбрасываются. Оставшиеся элементы сортируются по убыванию частоты.

2. Второй проход — на основе отсортированных транзакций строится многомерное дерево. При этом узлы дерева кодируют не только значения, но и измерения. Если элемент уже существует в текущем пути, его счётчик увеличивается, иначе создаётся новый узел.

Метод построения и расширения многомерного дерева частых признаков реализуется по принципу, аналогичному формированию дерева частых паттернов. На начальном этапе структура дерева содержит единственный корневой узел, помеченный нулевым значением. После считывания множества признаков сетевого события в дерево добавляются узлы, содержащие тег признака, его измерение и счётчик встречаемости, отражающий количество событий, сопоставленных с данным путём.

Построение многомерного дерева частых наборов признаков транзакций осуществляется последовательно.

1. На первом этапе выполняется однократный проход по множеству зарегистрированных сетевых событий для определения значения поддержки каждого признака. Признаки, не удовлетворяющие минимальному порогу поддержки, исключаются. Частые признаки упорядочиваются по убыванию встречаемости. Для рассматриваемого примера наибольшую поддержку имеет признак a:1, за которым следуют b:1, c:1, d:2 и e:2.

2. При повторном проходе по множеству событий формируется структура многомерного дерева частых признаков. При обработке множества признаков {a:1, b:1} создаются узлы a:1 и b:1, формирующие путь null → a:1 → b:1, что соответствует кодированию данного события. Счётчики всех узлов на пути принимают значение 1.

3. При чтении второго множества признаков {b:1, c:1, d:2} создаётся новый набор узлов, формирующий путь null → b:1 → c:1 → d:2. Счётчики узлов на пути также устанавливаются равными 1. Несмотря на наличие общего признака b:1, пути не пересекаются, поскольку множества признаков не имеют общего префикса.

4. Третье множество признаков {a:1, c:1, d:2, e:2} имеет общий префикс с первым множеством {a:1, b:1}. В результате путь null → a:1 → c:1 → d:2 → e:2 частично перекрывается с ранее построенным путем null → a:1 → b:1 в узле a:1. Счётчик встречаемости узла a:1 увеличивается до значения 2, а вновь созданные узлы c:1, d:2 и e:2 получают значение 1.

5. Аналогичным образом каждое последующее множество признаков сопоставляется с путями многомерного дерева частых признаков, что обеспечивает его последовательное расширение и накопление статистических зависимостей.

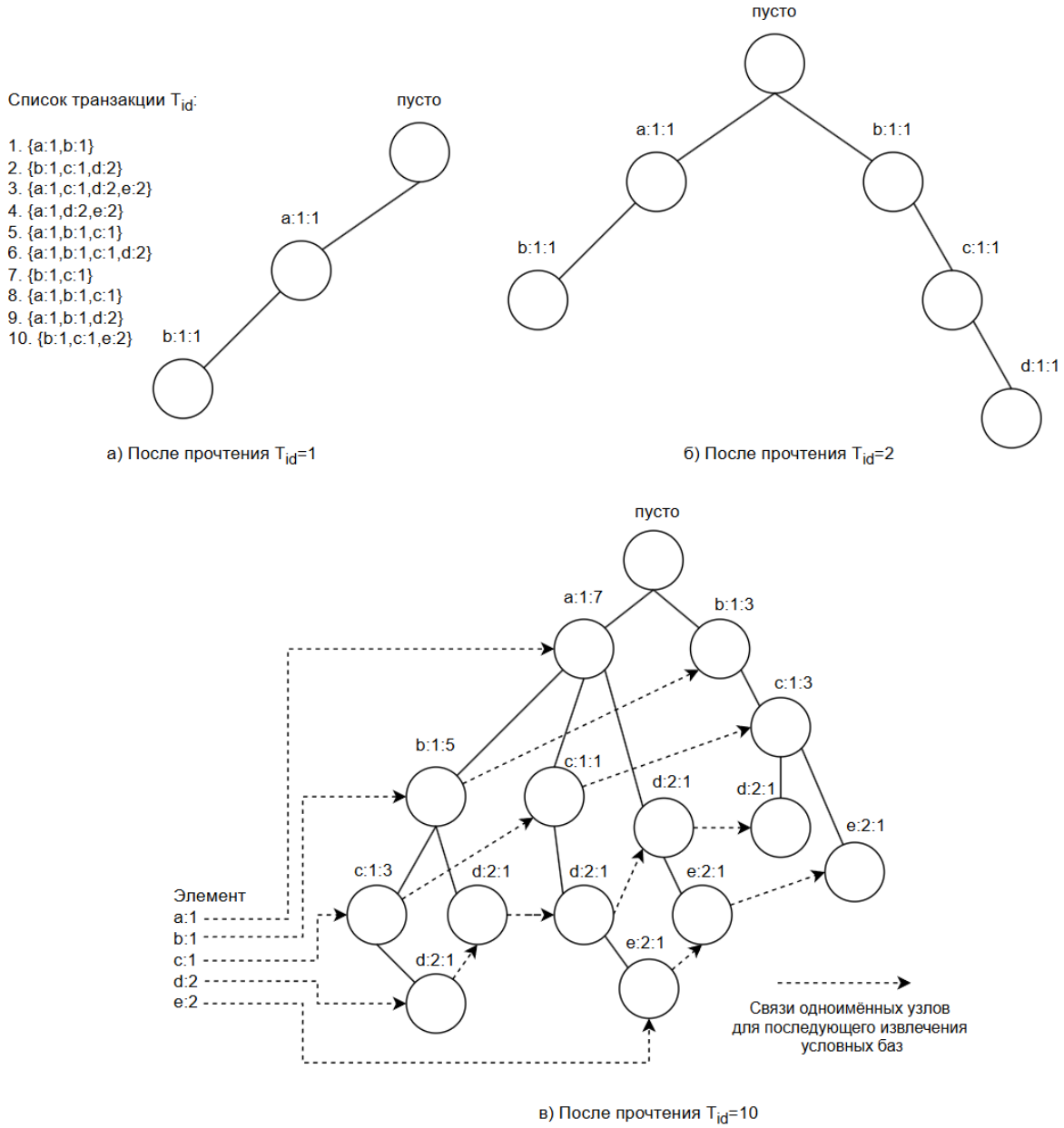

Рисунок 3.5 – Процесс построения многомерного дерева частых наборов признаков

Итоговая структура многомерного дерева частых наборов признаков после обработки совокупности транзакций представлена на рисунке 3.5. Из исходных данных исключены редкие признаки, а оставшиеся упорядочены по убыванию значения поддержки.

Структура дерева позволяет извлекать частые паттерны с учётом принадлежности признаков к своим измерениям. В одномерных моделях значения анализируются совместно, без сохранения связей между полями. В рассматриваемом подходе такие связи сохраняются — например, между номером ВС и временем передачи пакета. За счёт этого выявляются более сложные комбинации признаков, отражающие возможные сценарии НСВ в контуре УВД.

Модификация метода FP-Growth ориентирована на обработку многомерных данных, характеризующих транзакции информационного обмена в контуре УВД. Разработанный метод учитывает распределённый характер источников выявлять корреляции между событиями, происходящими в различных сегментах УВД. В результате удаётся учитывать принадлежность каждого признака к отдельному измерению и сохранить логическую структуру записей. Это позволяет извлекать устойчивые многомерные зависимости между атрибутами, характерными для определённых форм сетевой активности.

Учет многомерной структуры признаков и распределённого характера источников данных требует формализации процесса их обработки. С этой целью разработана модель, описывающая уровневую организацию обработки потока событий СПД в контуре УВД. Общая структура модели представлена на рисунке 3.6. Модель формализует обработку потока событий СПД в контуре УВД по следующим уровням:

1. уровень сбора телеметрии. На базовом уровне функционируют подсистемы телеметрии, регистрирующие параметры трафика в каналах авиационной связи. Это бортовые шлюзы, приёмники ACARS/CPDLC, сетевые коммутаторы систем УВД и маршрутизаторы наземных сетей. В ряде случаев в состав сбора может быть включён поток сообщений ADS-B как дополнительный

источник телеметрических данных. Зафиксированные события описываются в виде векторов признаков:

$$x_i = \left\{a_1^{(i)}, a_2^{(i)}, \dots, a_m^{(i)}\right\}, i = 1, 2, \dots, N, \quad (3.1)$$

где каждый $a_m^{(i)}$ — значение k-го признака в i-м событии. Таким образом формируется наблюдаемая последовательность сетевых событий:

$$X = \{x_1, x_2, \dots, x_N\}, \quad (3.2)$$

2. уровень предварительной обработки. Для приведения информации к единому формату используется нормализация: устраняются дублирующие события, синхронизируются временные метки, проводится выравнивание структуры данных. На выходе получается нормализованная последовательность, пригодная для анализа:

$$\tilde{X} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N\}, \quad (3.3)$$

Каждое событие $\tilde{x}_i$ — это преобразованный вектор, сохраняющий исходную семантику и обеспечивающий однородность по измерениям.

3. уровень корреляционного анализа. На этом уровне реализуется интеллектуальный анализ последовательности $\tilde{X}$ с помощью метода многомерного анализа частых наборов признаков сетевого трафика. Основная идея метода — построение многомерного дерева, в котором каждый узел дополнительно помечен атрибутом измерения. На основе построенного многомерного дерева выделяется множество частых многомерных шаблонов:

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

где θ_S — минимальный порог поддержки. Эти шаблоны отражают устойчивые сочетания признаков, характерные для сценариев НСВ в контуре УВД.

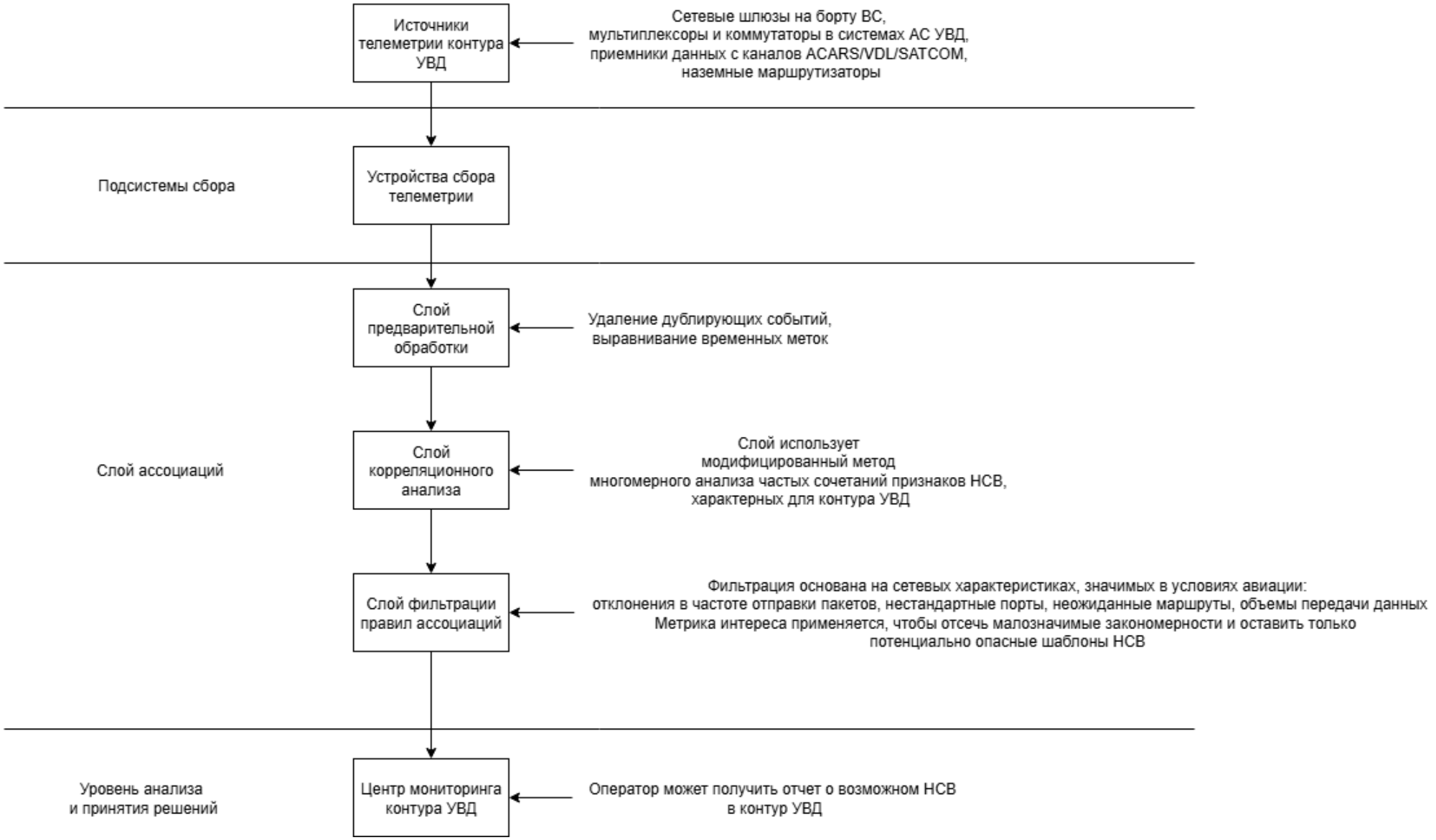

Рисунок 3.6 – Модель ассоциации событий безопасности в контуре УВД

4. Уровень фильтрации правил ассоциаций. Каждому паттерну p_j из множества P сопоставляется ассоциативное правило вида $A \Rightarrow B$, для которого рассчитываются метрики эффективности:

- поддержка: $support(A \Rightarrow B)$;

- достоверность (confidence): $conf(A \Rightarrow B) = \frac{count(A \cup B)}{count(A)}$;

- оценка степени интереса методом измерения степени нормы:

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

Отбор правил осуществляется по совокупности этих метрик. В первую очередь исключаются шаблоны с низкой поддержкой и достоверностью, затем — правила с $Lift \approx 1$, не несущие аналитической ценности. Блок-схема алгоритма фильтрации правил ассоциаций представлена на рисунке 3.3.

5. уровень анализа и принятия решений. На завершающем уровне в контуре УВД функционирует центр мониторинга, в котором осуществляется интерпретация выявленных закономерностей и выработка оперативных мер реагирования. Сведения, полученные в результате ассоциативного анализа, передаются оператору в виде отчёта, содержащего информацию о потенциально опасных сочетаниях сетевых характеристик, типичных для НСВ. Это позволяет не просто фиксировать отдельные подозрительные события, а отслеживать взаимосвязанные отклонения.

Таким образом, в рамках реализации метода многомерного анализа частых наборов признаков транзакций разработана модель ассоциации событий безопасности, адаптированная под особенности архитектуры контура УВД. В отличие от существующих подходов, предполагающих ограниченное множество источников событий, данная модель учитывает разнородные устройства (бортовые шлюзы, коммутаторы в системах УВД, наземные маршрутизаторы и др.). Модель обеспечивает агрегацию разнородных потоков и формирование интегрированных паттернов сетевой активности.

Алгоритм, реализующий предлагаемый метод, представлен на рисунке 3.7.

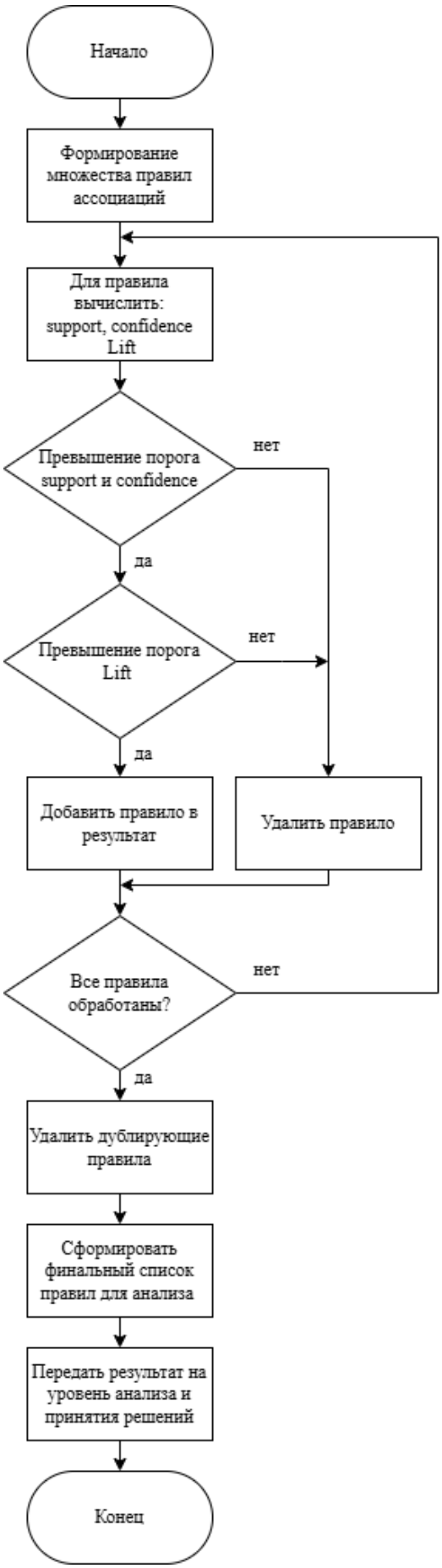

Рисунок 3.7 – Алгоритм фильтрации правил ассоциации

Разработанный алгоритм реализует процедуру отбора значимых ассоциативных правил на основе совокупности статистических метрик в контуре УВД. Алгоритм предполагает следующую последовательность операций:

1. формирование множества ассоциативных правил на основе выявленных частых наборов признаков в сетевых событиях;

2. для каждого правила вычисляются значения трёх параметров:

- уровень поддержки $support(A \Rightarrow B) = \frac{count(A \cup B)}{N}$,
- достоверность (confidence) $conf(A \Rightarrow B) = \frac{count(A \cup B)}{count(A)}$,
- степень интереса $Lift(A \Rightarrow B)$;

3. выполняется проверка: превышает ли правило заданные пороги по $support$ и $conf$. Если хотя бы одно условие не выполняется — правило исключается;

4. анализируется значение метрики $Lift$. Если оно близко к единице $Lift \approx 1$, то правило считается аналитически незначимым и также исключается;

5. при выполнении всех условий правило добавляется в результирующее множество;

6. после обработки всех правил осуществляется удаление избыточных правил, которые представляют собой частные случаи более общих зависимостей с теми же статистическими характеристиками;

7. формируется итоговый список ассоциативных правил для последующего анализа на уровне принятия решений;

8. результаты передаются в центр мониторинга в контуре УВД для дальнейшей интерпретации.

Алгоритм имеет ряд ограничений, обусловленных его эвристическим характером и требованиями к структуре входных данных.

Во-первых, точность отбора правил напрямую зависит от выбора пороговых значений $support$, $conf$ и $Lift$, которые должны быть заранее определены и адаптированы под особенности сетевого трафика в контуре УВД. Неправильно выбранные значения могут привести либо к потере значимых закономерностей, либо к включению избыточных, неинформативных правил.

Во-вторых, алгоритм не учитывает семантическую интерпретацию признаков, а опирается только на их статистическую взаимосвязь. Это может ограничить его применение при анализе редких, но критичных сценариев НСВ, не имеющих устойчивых частотных шаблонов.

Наконец, эффективность алгоритма зависит от полноты и репрезентативности входного множества событий, получаемого на предыдущих этапах анализа. В случае неполного покрытия журналов событий сетевого трафика или высокой степени шума в данных возможно снижение точности выявления значимых зависимостей.

Таким образом, сформирована методическая основа выявления признаков НСВ в контуре УВД на основе многомерного анализа частых наборов признаков сетевого трафика. Введено многомерное представление транзакций, позволяющее сохранять принадлежность признаков к различным измерениям и учитывать разнородность источников данных в авиационных сетях передачи данных, таких как ACARS и CPDLC.

Результаты данного параграфа были опубликованы в [102, 103].

3.2. Разработка и исследование метода формирования компактного представления транзакций информационного обмена в контуре управления воздушным движением для последующего анализа признаков несанкционированного вмешательства

Информационный обмен в контуре УВД характеризуется значительным объёмом, высокой степенью повторяемости событий и наличием множества нерелевантных сочетаний признаков (см. п. 3.1). При этом часто формируются

журналы, в которых сохраняются данные о многочисленных фрагментах обмена, не всегда имеющих отношение к потенциальным инцидентам. Это создаёт необходимость в предварительной фильтрации и структурной организации данных, направленной на сокращение вычислительной сложности.

В работе предлагается метод формирования компактного представления транзакций информационного обмена. Задача сводится к сжатию повторяющихся структур, исключению нерелевантных сочетаний и подготовке транзакций к дальнейшему этапу классификации (см. п. 3.3). Для этого предлагается использовать модифицированный метод, основанный на модификации известного метода дерева совместно встречающихся частых наборов Co-Occurent Frequent Item (COFI-tree). Такая адаптация направлена на обеспечение эффективной работы с большими наборами сетевых признаков, генерируемых в контуре УВД.

Среди известных методов поиска частых сочетаний признаков применяются подходы, основанные на стратегиях поиска в ширину и в глубину. Методы, использующие деревья частых паттернов (FP-growth, COFI-tree), позволяют сжать множество транзакций в компактную структуру и уменьшить количество операций за счёт повторного использования общих префиксов.

В частности, COFI-tree применяет стратегию локального построения деревьев для каждого часто встречающегося признака. Эти деревья извлекаются на основе единого FP-дерева, что позволяет минимизировать число операций и обеспечить устойчивую работу метода на массивах с высокой степенью дублирования информации. Тем не менее, при прямом применении в контуре УВД такой метод сталкивается с рядом ограничений, которые требуют модификации исходной структуры.

Алгоритм COFI-tree используется в качестве основы для формирования компактного представления часто встречающихся сочетаний признаков в авиационном сетевом трафике. Он позволяет организовать локальную обработку данных без генерации всех возможных комбинаций, что критически важно при анализе больших объёмов трафика. COFI-tree базируется на предварительно

построенном FP-дереве и реализует обработку каждого частого признака в виде выделенного поддерева, в котором отражены только связанные с ним транзакции.

Структура алгоритма предполагает трёхэтапную процедуру: построение FP-дерева по базе данных с фильтрацией по порогу поддержки; формирование отдельного дерева COFI для каждого частого признака на основе путей в FP-дереве; извлечение частых сочетаний из каждого COFI-дерева с последовательной очисткой и агрегацией результатов. За счёт такого подхода обеспечивается сжатие данных и минимизация числа повторных проходов.

Применение базового алгоритма COFI-tree в задачах анализа сетевого трафика авиационных СПД требует оценки его вычислительных характеристик. При этом выявляется ряд структурных ограничений, затрудняющих масштабируемость метода в условиях большого объёма данных.

Первое ограничение связано с построением таблицы заголовков FP-дерева. В классической реализации для связи однотипных узлов применяется односвязный список, проход по которому осуществляется линейно. При увеличении числа элементов это приводит к росту времени вставки и сложности доступа, а сама структура становится неэффективной для оперативного формирования COFI-деревьев.

Второе ограничение касается необходимости поочерёдной генерации и обработки отдельных деревьев COFI для каждого частого признака. При большом количестве таких признаков возрастает нагрузка на оперативную память, увеличивается число операций по пересчёту поддержки и фильтрации узлов, а общая продолжительность обработки возрастает. В контуре УВД, где обрабатывается потоковый трафик с высокой плотностью признаков, такие издержки делают стандартную реализацию метода затруднительной.

Таким образом, несмотря на конструктивные преимущества метода COFI-tree, его применение к задачам анализа сетевого трафика в контуре УВД требуют модификации.

Модификация метода COFI-tree осуществляется по двум направлениям: первое связано с изменением структуры таблицы заголовков часто встречающихся

признаков FP-дерева, второе — с пересмотром метода обработки этих признаков без использования классического построения COFI-деревьев.

В стандартной реализации FP-дерева таблица заголовков для каждого признака содержит указатель на связанный список узлов дерева. При вставке нового элемента осуществляется последовательный проход по всей цепочке, чтобы найти последний узел и добавить новый. Такая схема требует итеративного доступа и приводит к значительным затратам времени при увеличении числа транзакций и признаков. В контуре УВД, характеризующегося высокой плотностью повторяющихся элементов, подобный подход становится критически неэффективным.

Для устранения данной проблемы предложено решение, основанное на формировании цепочки узлов в обратном порядке. При добавлении нового узла связанный список перестраивается таким образом, что новый узел сразу получает ссылку на предыдущий, а указатель в таблице заголовков обновляется на текущий. Благодаря этому отпадает необходимость прохода по всей цепочке, поскольку каждый новый элемент добавляется в её начало, обеспечивая постоянное время вставки. На рисунке 3.8 показан фрагмент FP-дерева, отражающий структуру обратного связывания. Элементы одного типа объединяются в цепочки, упорядоченные от последнего к первому, что обеспечивает упрощение процедуры добавления и улучшение характеристик при построении дерева.

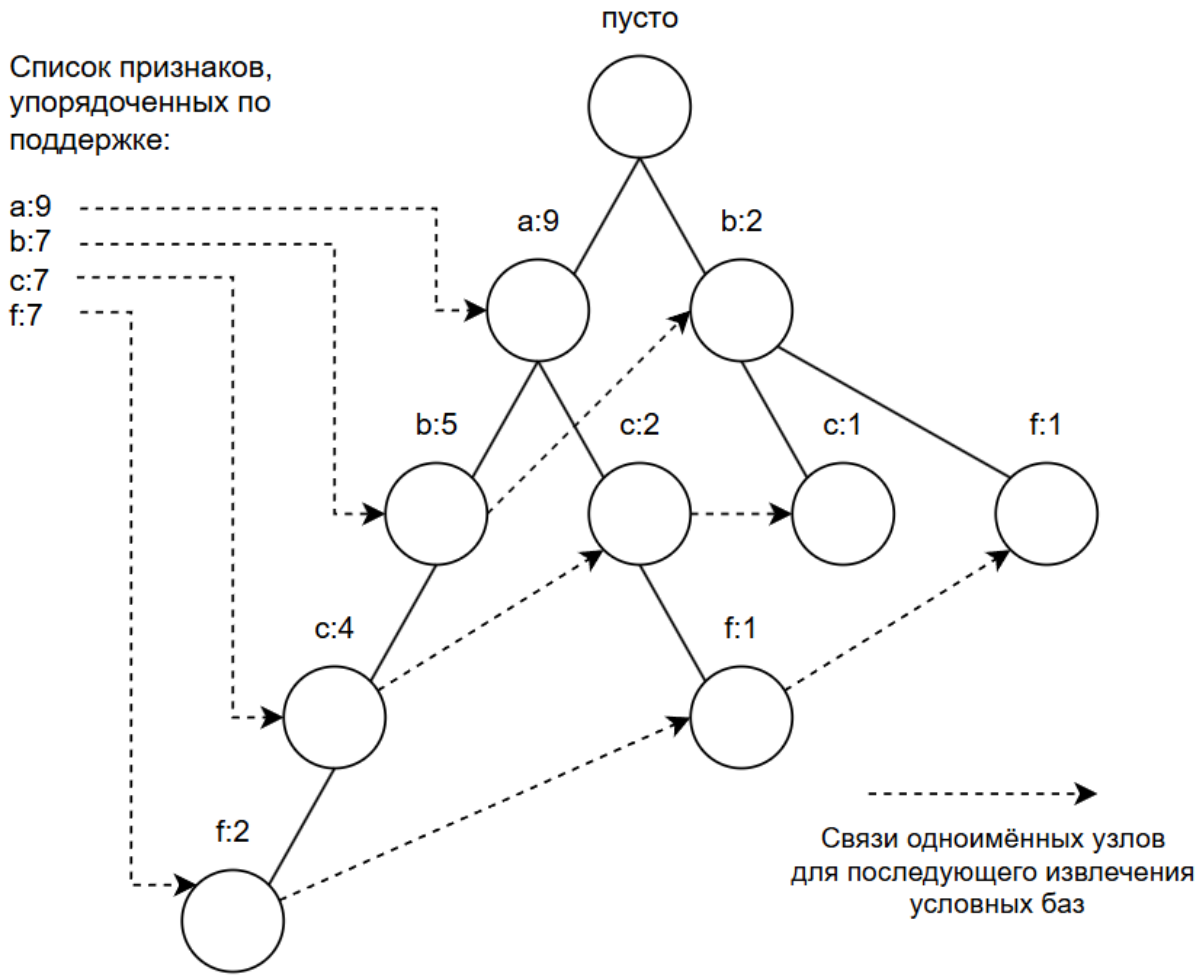

Рисунок 3.8 – Принцип формирования компактного представления транзакций на основе префиксного дерева частых наборов признаков

В исходной версии алгоритма COFI-tree для каждого частого признака создаётся отдельное условное дерево, что требует выделения памяти и повторного обхода структур. С ростом числа признаков и глубины дерева такие действия приводят к значительным издержкам. В предлагаемой модификации отказ от хранения и параллельной обработки множества COFI-деревьев, реализован через применение структуры анализа частых путей. Вместо формирования нового дерева для каждого признака осуществляется последовательная обработка соответствующих путей в исходном FP-дереве.

В рамках первого направления модификации улучшение касается метода обработки частых признаков. В стандартном методе COFI-tree для каждого часто

встречающегося элемента формируется отдельное условное дерево, что требует выделения дополнительной памяти, хранения локальных таблиц и повторной фильтрации. В рамках второго направления предлагаемая модификация исключает построение условных деревьев. Вместо этого используется последовательная обработка соответствующих путей в исходном FP-дереве, по которым извлекаются частые сочетания признаков. Отбор выполняется с учётом порога минимальной поддержки непосредственно при обходе, что позволяет отказаться от дополнительной фильтрации.

Отказ от генерации поддеревьев и переход к прямой обработке префиксных путей сокращают число операций и снижают нагрузку на оперативную память. Это особенно важно при анализе информационного обмена в контуре УВД, где обрабатываются большие потоки однотипных структур с высокой повторяемостью (см. п. 3.1). Предложенные изменения обеспечивают устойчивую работу алгоритма и сохраняют полноту извлечения частых сочетаний признаков. Это позволяет применять метод при обработке массивов данных значительного объёма. В предлагаемом методе COFI-дерево используется исключительно как промежуточная структура для извлечения базисов частых путей и не рассматривается как конечная форма представления данных.

Для иллюстрации предлагаемой модификации рассмотрим формирование условной структуры для признака G. Все пути, содержащие этот элемент, извлекаются из FP-дерева (см. рисунок 3.8), при этом поддержка каждого пути определяется как поддержка G в этом контексте.

Извлечённые пути подвергаются предварительной фильтрации: исключаются признаки, не удовлетворяющие минимальному порогу локальной поддержки. В рассматриваемом случае локально частыми относительно элемента G оказываются признаки H, A, F и E. Далее, после удаления нерелевантных признаков, каждый путь упорядочивается по возрастанию частоты оставшихся элементов. Это позволяет сократить количество ветвлений при построении дерева.

Формирование COFI-дерева начинается с создания корневого узла, соответствующего признаку G. Каждое из отсортированных сочетаний последовательно добавляется в структуру: если часть маршрута уже присутствует, значения счётчиков соответствующих узлов суммируются, в противном случае

формируется новая ветвь. Этот процесс повторяется до обработки всех входящих путей.

Предлагаемая модификация сохраняет корректность базового алгоритма COFI-tree, изменяя порядок обработки и форму хранения промежуточных результатов.

В отличие от известной реализации, каждому узлу COFI-дерева на этапе построения присваивается параметр участия (participation_counter), инициализируемый нулевым значением. Это позволяет исключить дополнительные итерации при последующей обработке и упростить подсчёт вложенных сочетаний. Связность между однотипными узлами поддерживается через таблицу заголовков с использованием указателей node-link, аналогично базовой структуре FP-дерева.

Полученное дерево G-COFI используется как компактное представление условной базы для признака G и применяется для извлечения значимых сочетаний. Его структура приведена на рисунке 3.9.

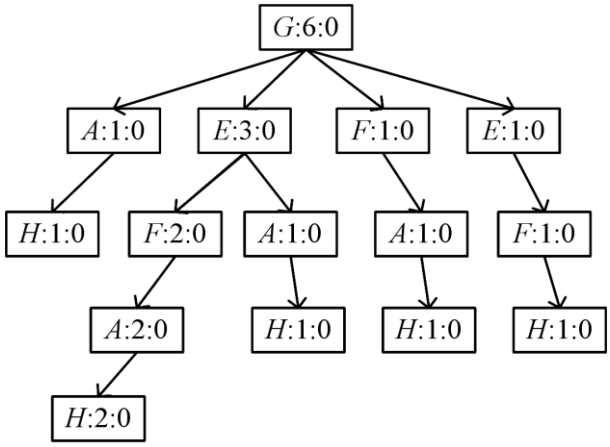

Рисунок 3.9 – Дерево G-COFI

Обработка частых сочетаний признаков в рамках предложенного метода выполняется с применением структуры суффиксных данных (Suffix Data Structure, SD), которая заменяет традиционный перебор всех комбинаций на основе COFI-деревьев. Такой подход позволяет эффективно агрегировать базисы частых путей и вычислять поддержки всех возможных сочетаний без необходимости хранения и анализа каждого условного дерева в отдельности.

На основе G-COFI-дерева, сформированного ранее (см. рисунок 3.9), производится извлечение базисов частых путей для признака G. Для этого выполняется проход от каждого локально частого признака снизу вверх. Если поддержка соответствующего узла превышает значение счётчика участия, фиксируется базис — последовательность признаков по пути, начинающемуся с G. Поддержка такого базиса определяется как разность между полной поддержкой узла и его текущим участием. В результате формируется множество базисов, таких как (GAH):1, (GEFAH):2, (GEAH):1 и др. Дерево с отображением сгенерированных базисов приведено на рисунке 3.10.

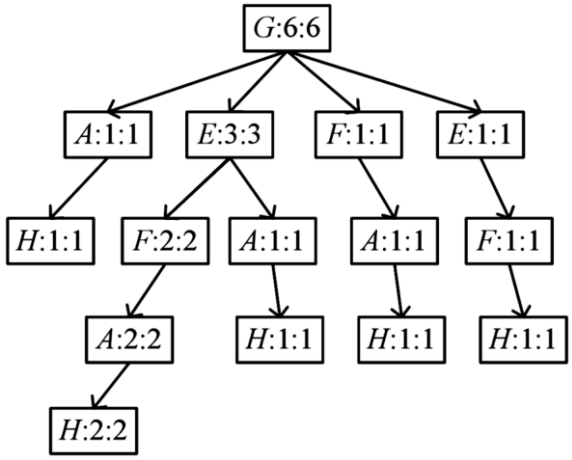

Рисунок 3.10 – COFI-tree после создания всех базисов часто встречающихся путей

В это время поддержка каждого узла в дереве G-COFI равна значению участия, а конечный базис частого пути равен (*GAH*): 1, (*GEFAH*): 2, (*GEAH*): 1, (*GFAH*): 1, (*GEFH*): 1.

Полученные базисы размещаются в структуре SD — циклическом односвязном списке, сегментированном по длине путей. Каждый сегмент содержит базисы фиксированной длины. Такая организация обеспечивает структурированное сравнение и агрегацию. Например, все базисы длины 3 (GAH) располагаются в одном сегменте, длины 4 — в другом и так далее. Структура SD после размещения всех базисов без учёта пересечений представлена на рисунке 3.11.

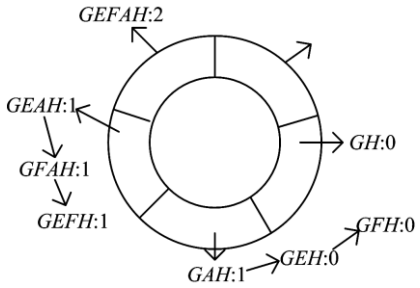

Рисунок 3.11 – Структура SD с частым базисом путей и попарным пересечением

На следующем этапе производится попарное сравнение базисов. Если базис меньшей длины входит в состав более длинного, его поддержка увеличивается на величину поддержки соответствующего базиса. Например, базис GAH:1, входящий в GEAH:1, GFAH:1 и GEFAH:2, получает итоговую поддержку 5. Новые базисы, возникающие при пересечении, добавляются в структуру SD с нулевой инициализацией поддержки. После перераспределения значений в SD сохраняются только те сочетания, поддержка которых превышает или равна заданному пороговому уровню. Структура после перерасчёта показана на рисунке 3.12, а примеры устойчивых сочетаний включают GH:6, GEH:4, GAH:5, GEAH:3, GEFH:3 и др.

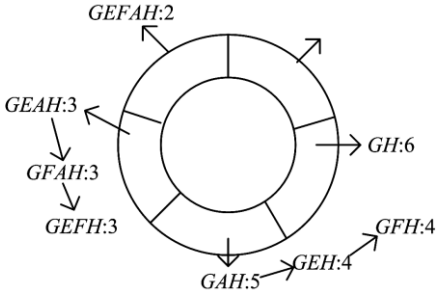

Рисунок 3.12 – Структура SD после изменения поддержки

Предлагаемый метод позволяет избавиться от необходимости последовательного обхода всех условных деревьев. Вместо этого результаты для каждого частого признака обрабатываются поэтапно, а после завершения операции соответствующий COFI-элемент удаляется. Таким образом, структура SD формирует агрегированное представление всей условной базы, не требуя

одновременного хранения всех поддеревьев, что снижает объём памяти и упрощает вычисления при масштабных входных данных.

Алгоритм, реализующий описанную процедуру, представлен на рис. 3.13.

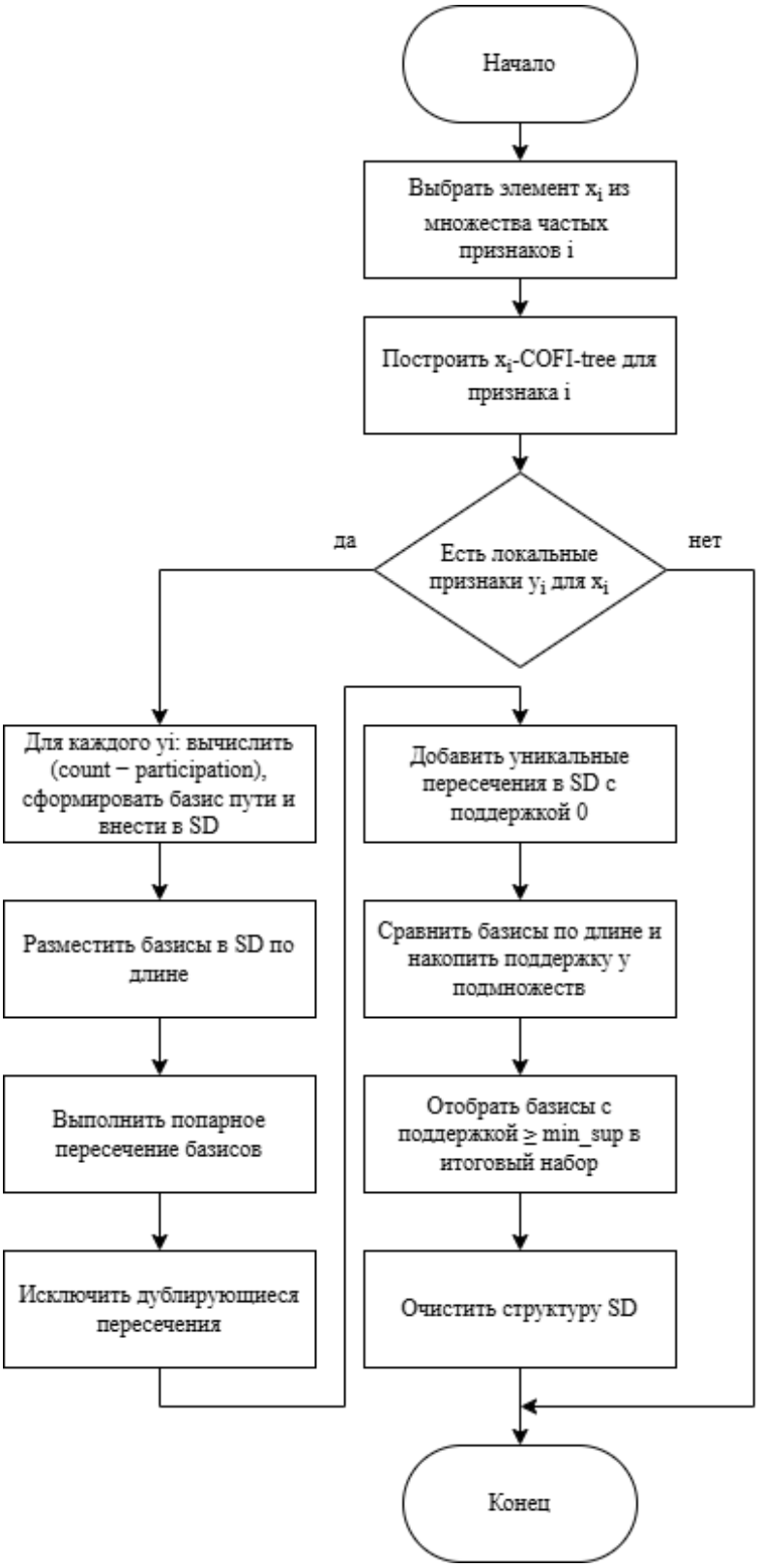

Рисунок 3.13 – Алгоритм извлечения частых сочетаний признаков на основе структуры SD

Разработанный алгоритм реализует поэтапную процедуру формирования устойчивых сочетаний часто встречающихся признаков. Обработка организована на основе анализа путей в COFI-деревьях с последующей агрегацией данных в структуре SD. Алгоритм выполняется в следующем порядке:

1. выбирается очередной признак из множества частых признаков, определённых на этапе предварительного анализа;

2. формируется соответствующая условная структура на основе COFI-подхода, отражающее связи между признаком и сопутствующими элементами;

3. выполняется проверка наличия локальных признаков, соответствующих заданному порогу поддержки;

4. для каждого найденного локального признака определяется разность между общей поддержкой и счётчиком участия; по результатам формируются базисы путей, которые упорядочиваются по длине и записываются в структуру SD;

5. формируются пересечения между базисами. Дубликаты отбрасываются, новые комбинации добавляются с нулевым значением поддержки;

6. поддержка каждого базиса пересчитывается с учётом вложенности в более длинные пути;

7. из общего множества отбираются те сочетания, которые соответствуют заданному порогу min_sup;

8. после завершения обработки признак исключается из рассмотрения, структура SD очищается, и выполняется переход к следующему элементу.

Такой порядок действий обеспечивает сокращение избыточных операций и позволяет выявлять значимые зависимости в массиве сетевых признаков без полного перебора всех комбинаций.

Таким образом, в разработан метод формирования компактного представления частых сочетаний признаков сетевого трафика в контуре УВД, основанный на модификации структуры FP-дерева и агрегации базисов частых путей в структуре SD. Предлагаемый подход позволяет существенно сократить объём хранимых данных и снизить вычислительные затраты при сохранении

полноты извлечения частых сочетаний признаков, сформированных на предыдущем этапе многомерного анализа (см. п. 3.1).

3.3. Разработка и исследование алгоритмов классификации транзакций информационного обмена в контуре управления воздушным движением в условиях несанкционированного вмешательства

Алгоритмы классификации транзакций информационного обмена в контуре УВД предназначены для выявления НСВ на основе статистически устойчивых сочетаний сетевых признаков информационного обмена. Входом алгоритмов классификации является компактное представление множества транзакций (см. п. 3.2). Указанное представление получается без потери информации, значимой для ассоциативного анализа, и сохраняет поддержку частых сочетаний признаков, выявленных в исходном потоке транзакций.

Применение метода компактного представления позволяет существенно сократить объём обрабатываемых данных. Так, при анализе реального сетевого трафика количество транзакций, сформированных на этапе многомерного анализа (п. 3.1), сокращается с сотен тысяч до десятков тысяч элементов при сохранении структуры частых сочетаний. Это делает задачу извлечения ассоциативных правил вычислительно реализуемой в условиях ограниченных ресурсов, характерных для применения в контуре УВД.

Алгоритм Apriori является классическим методом поиска ассоциативных правил, однако его применение ограничено при работе с большими объёмами данных из-за необходимости многократного сканирования базы и генерации большого количества промежуточных наборов-кандидатов. Более эффективным

решением в таких условиях считается алгоритм FP-growth, позволяющий строить дерево часто встречающихся элементов без генерации кандидатов. При этом при работе с разреженными наборами данных эффективность FP-growth также снижается, поскольку возникает необходимость построения большого количества условных деревьев. Эти ограничения учитываются при разработке алгоритмов, представленных ниже.

Входные данные алгоритма представляют собой последовательность транзакций (см. п. 3.2), каждому из которых присвоено обозначение I_i в соответствии с принадлежностью к определённому кластеру признаков. На первом этапе последовательность преобразуется в базу транзакций с использованием метода скользящего окна фиксированной длины. При этом исключаются повторы внутри окна, а новая транзакция формируется, как только окно достигает предельного размера или обнаруживается повторяющийся элемент. Полученная база транзакций, представленная в Таблице 3.1, представляет собой хронологическую структуру, поступающих от систем регистрации и предварительного анализа сетевых событий информационного обмена в контуре УВД, и служит входом для последующего ассоциативного анализа.

Таблица 3.1. – Сбор транзакций

Транзакции	Элемент	Транзакции	Элемент
T_1	I_3, I_1	T_6	I_2, I_6
T_2	I_1, I_2, I_4	T_7	I_2, I_4
T_3	I_2, I_3, I_1, I_5	T_8	I_2, I_4, I_5
T_4	I_1, I_7, I_3	T_9	I_2, I_1
T_5	I_3, I_4, I_1, I_5	T_{10}	I_1, I_3

Для каждой транзакции выполняется подсчёт частот (поддержки) появления отдельных элементов, представленный в Таблице 3.2, после чего формируется список часто встречающихся признаков, отсортированный по убыванию.

Таблица 3.2. – Частота (поддержка) каждого элемента

Элемент	Частота
I_1	7
I_2	6
I_3	5
I_4	4
I_5	3
I_6	1
I_7	1

Параллельно строится двумерная таблица, представленная в Таблице 3.3, в которую заносятся все пары признаков, зафиксированные в рамках каждой транзакции (см. табл. 3.4).

Таблица 3.3. – Двумерная таблица

Элемент	I_1	I_2	I_3	I_4	I_5	I_6	I_7
I_1	0	1	2	1	2	0	1
I_2	2	0	1	3	2	1	0
I_3	3	0	0	1	2	0	0
I_4	1	0	0	0	2	0	0
I_5	0	0	0	0	0	0	0
I_6	0	0	0	0	0	0	0
I_7	0	0	1	0	0	0	0

Элементы, чья поддержка не превышает установленного порога, исключаются из транзакций, после чего база пересобирается с учётом только значимых признаков. Результат представлен в Таблице 3.4.

Таблица 3.4. – Обновленный набор транзакций

Транзакции	Элемент	Транзакции	Элемент
T_1	I_1, I_3	T_6	I_2
T_2	I_1, I_2, I_4	T_7	I_2, I_4
T_3	I_1, I_2, I_3, I_5	T_8	I_2, I_4, I_5
T_4	I_1, I_3	T_9	I_1, I_2
T_5	I_1, I_3, I_4, I_5	T_{10}	I_1, I_3

На основе обновлённой базы строится многомерное FP-дерево (см п. 3.1), где каждый узел содержит информацию о признаке, количестве его повторений, родительской связи, а также специальные флаги Array и Leaf. Первый указывает на использование массивного запроса (для обработки разреженных признаков), а второй — на терминальность узла.

Обработка частых сочетаний признаков НСВ осуществляется в два этапа. Сначала анализируются разреженные элементы, для которых FP-growth показывает ограниченную эффективность. Частые пары в таких случаях извлекаются напрямую из двумерной таблицы. Например, элемент I_5 образует сочетания $\{I_1, I_5\}, \{I_2, I_5\}, \{I_3, I_5\}, \{I_4, I_5\}$, при этом поддержка рассчитывается как сумма значений по строкам и столбцам. Аналогично для других редких признаков фиксируются устойчивые сочетания, превышающие минимальный порог.

Затем выполняется анализ плотных элементов путём последовательного обхода FP-дерева. Стратегия обхода зависит от значений параметров Array и Leaf:

- Array = 0, Leaf = 0 — ветвь продолжается с накоплением информации;
- Array = 0, Leaf = 1 — узел сохраняется, ветвь завершается;
- Array = 1, Leaf = 0 — узел пропускается, переход к следующему;
- Array = 1, Leaf = 1 — ветвь завершается без обработки

Для каждого плотного признака извлекаются частые сочетания, выявленные в пределах префиксов дерева. После этого найденные множества объединяются методом Apriori: на основе частых пар формируются кандидаты на тройки (например, $\{I_1, I_3, I_5\}$), которые проверяются по критерию поддержки (см. п. 3.1).

На основе полученных частых множеств формируются ассоциативные правила. Для каждой пары $A \Rightarrow B$ вычисляется достоверность ($confidence$), определяющая вероятность появления признаков группы B при наличии A. Например, при $conf(I_3, I_5 \Rightarrow I_1) = 1$ и пороге достоверности 0,8 соответствующее правило считается значимым. Если в структуре события отсутствуют очевидные причинно-следственные связи между признаками, решение принимается на основе статистической устойчивости выявленного шаблона.

Формализованное описание предложенных алгоритмов представлено в блок-схемах на рис. 3.14-3.16. Эти блок-схемы отражают основные процедуры: формирование базы транзакций, построение и обработку многомерного дерева частых наборов событий, а также извлечение и фильтрацию ассоциативных правил между признаками событий, выявленных в результате предварительного анализа сетевого трафика.

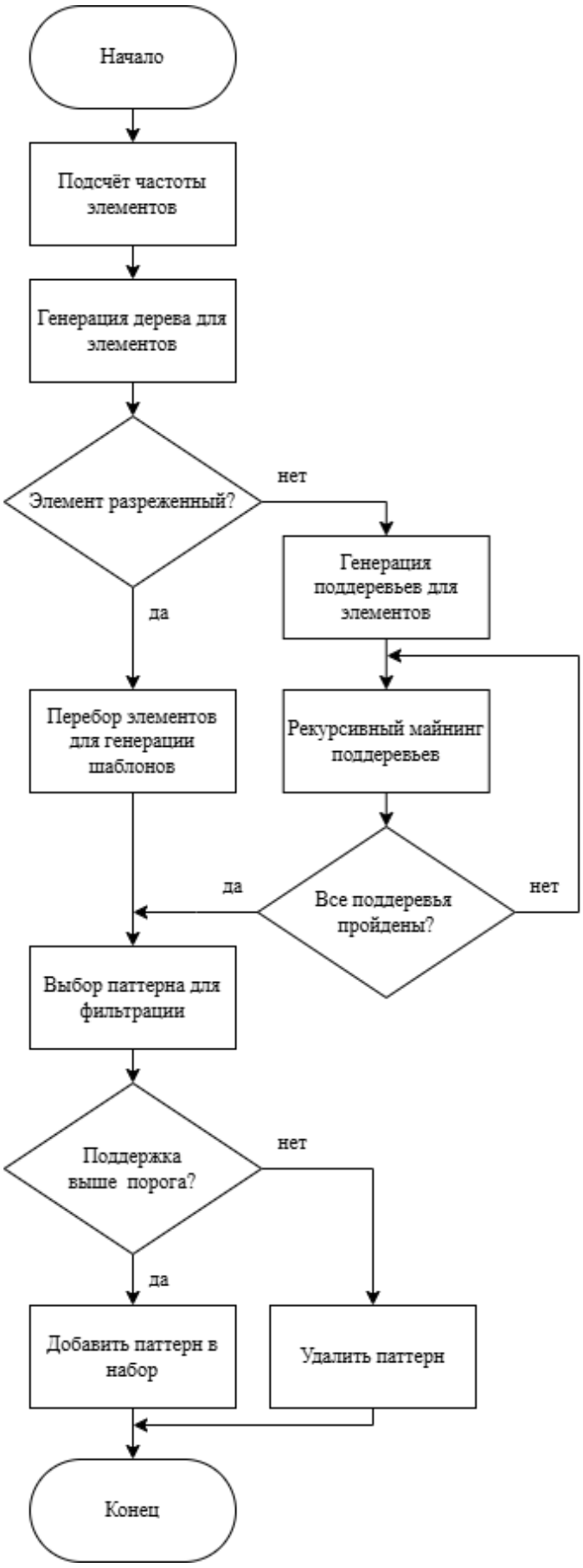

Рисунок 3.14 - Алгоритм 1. Блок-схема алгоритма формирования ассоциативных правил по разреженным и плотным признакам

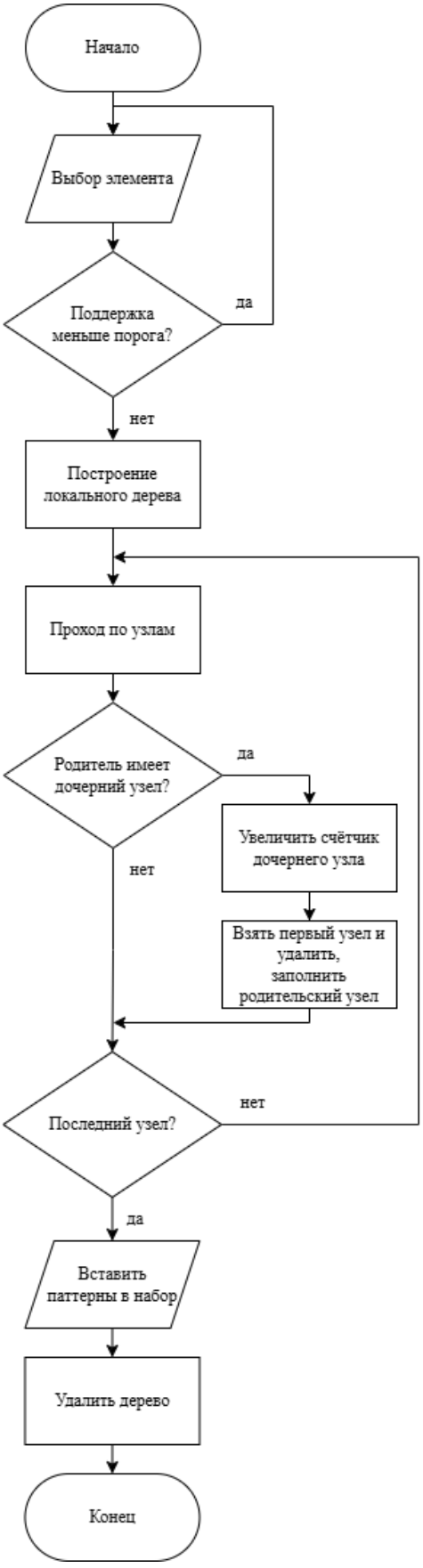

Рисунок 3.15 - Алгоритм 2. Блок-схема формирования сочетаний частых признаков

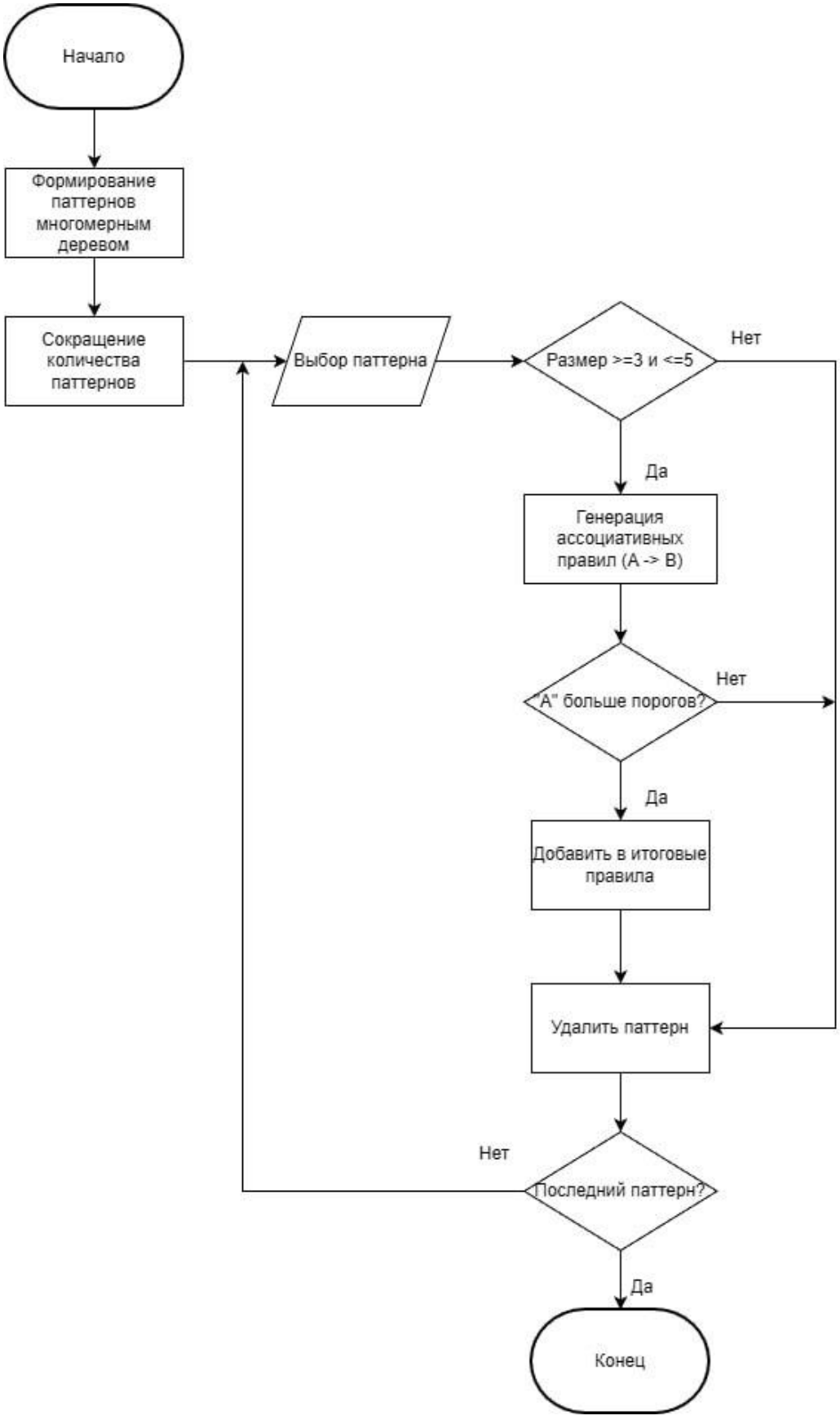

Рисунок 3.16 - Алгоритм 3. Блок-схема алгоритма фильтрации ассоциативных правил

Разработка реализует последовательную обработку сетевого трафика информационного обмена в контуре УВД для выявления устойчивых сочетаний признаков с последующей генерацией ассоциативных правил. Алгоритм выполняется в следующем порядке:

1. выполняется загрузка исходного массива транзакций, сортировка по временной метке и группировка признаков по типу (сетевые, временные, потоковые). Анализ проводится в скользящем окне длительностью 30 минут с шагом 15 минут;

2. для числовых признаков, содержащих более 100 уникальных значений, применяется локальная дискретизация: диапазон делится на пять сегментов bin0–bin4. Каждая запись преобразуется в транзакцию, содержащую кодированные признаки. (см. п. 3.1);

3. на основе набора транзакций строится дерево частот, в котором узлы упорядочены по убыванию частоты. Определяются разреженные и плотные признаки по критерию количества совместных появлений. Разреженные признаки подлежат прямому анализу, плотные — рекурсивному разложению с формированием поддеревьев;

4. для плотных признаков строятся вложенные структуры путей, по которым извлекаются устойчивые сочетания признаков (рис. 3.14). Проверка поддержки выполняется на каждом уровне построения;

5. для каждого признака, преодолевшего порог min_sup, формируется локальная структура, ограниченная измерениями, к которым он принадлежит. Построенные поддеревья очищаются от нерелевантных элементов и используются для извлечения паттернов в пределах одного контекста. (рис. 3.15);

6. локальные подструктуры обрабатываются параллельно. Извлечённые шаблоны группируются по длине и частоте, дубликаты исключаются. Уникальные базисные пути агрегируются в фильтрационную структуру;

7. сформированная совокупность паттернов передаётся на этап фильтрации. Повторно применяется порог min_sup. Паттерны с длиной от трёх до пяти признаков переходят к формированию правил. (рис. 3.16);

8. из отобранных сочетаний формируются ассоциативные правила вида A→B. Достоверность рассчитывается по классическому показателю confidence. Правила с confidence ниже 0.9 исключаются из рассмотрения;

9. рассчитывается степень интереса lift по формуле (3.5). Если значение близко к единице, правило считается статистически незначимым и удаляется. Сочетания с $lift >> 1$ отбираются для дальнейшего использования;

10. выполняется фильтрация: если в выборке содержится правило меньшей длины, обладающее теми же метриками достоверности и корреляции, более длинное удаляется как избыточное.

Таким образом, разработаны алгоритмы формирования и фильтрации ассоциативных правил для анализа информационного обмена в контуре УВД, отличающиеся совместной обработкой плотных и разреженных признаков без построения условных деревьев и позволяющие выявлять устойчивые частотные шаблоны НСВ в условиях отсутствия этапа предварительного обучения и неполноты априорной информации о сценариях атак.

Для перехода от выявления частотных шаблонов к задаче обнаружения и классификации НСВ требуется разработка алгоритма, обеспечивающего применение сформированного набора ассоциативных правил к потоку транзакций в контуре УВД. Такой алгоритм должен учитывать, что отдельное событие не содержит полного набора признаков атаки, а решение о наличии НСВ целесообразно принимать на основе совокупности совпадений его признаков с правилами ассоциаций.

Так же, поскольку общий набор ассоциативных правил включает сочетания, не специфичные для конкретного сценария НСВ в контуре УВД, для повышения точности классификации необходимо отфильтровать правила по конкретному шаблону атаки.

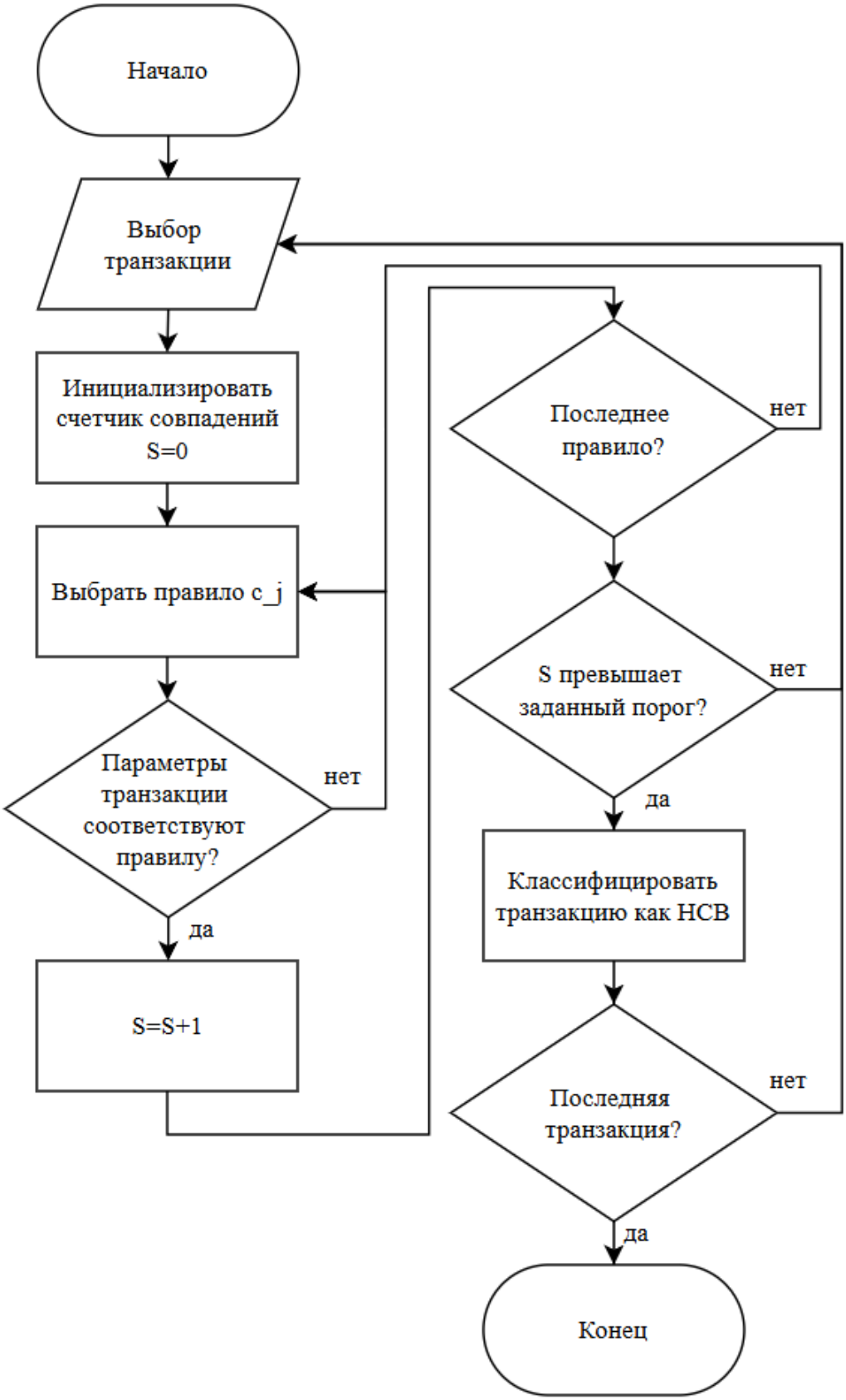

Рисунок 3.17 - Блок-схема алгоритма классификации транзакций информационного обмена в контуре УВД

Формализованное описание алгоритма классификации представлен на рис. 3.17. Последовательность работы алгоритма заключается в следующем:

1. из потока сетевого обмена последовательно извлекается очередная транзакция, характеризующее параметры передачи данных в контуре УВД на сетевом уровне;

2. инициализируется счётчик совпадений S, отражающий количество ассоциативных правил, условия которых выполняются для текущей транзакции;

3. последовательно перебираются все правила c_j. Для каждого правила проверяется выполнение ограничений, задаваемых данным правилом, по отношению к вектору признаков текущего события;

4. в случае выполнения условий очередного правила значение счётчика S увеличивается на единицу. Если условия не выполняются, переход осуществляется к проверке следующего правила;

5. после проверки всех ассоциативных правил значение счётчика сравнивается с заданным порогом;

6. если выполняется условие, транзакция классифицируется как НСВ по определенному сценарию. В противном случае событие относится к нормальному функционированию СПД в контуре УВД;

7. результат классификации фиксируется и используется для последующего анализа, статистической обработки и формирования итоговых показателей эффективности обнаружения НСВ.

Таким образом, разработаны алгоритмы классификации транзакций информационного обмена в контуре УВД, основанные на агрегированном применении множества ассоциативных правил, полученных методами частотного анализа.

Выводы по главе 3

В третьей главе были получены следующие основные результаты и выводы:

1. формализовано представление сетевого информационного обмена в контуре УВД в виде транзакций, формируемых на основе агрегированных временных, трафиковых и физических характеристик потоков. Установлено, что транзакция не соответствует отдельной протокольной единице передачи данных и формируется как обобщённое описание потока взаимодействия между узлами сети за ограниченный интервал времени, что обеспечивает применимость методов ассоциативного анализа к авиационным каналам передачи данных;

2. разработан метод многомерного анализа частых наборов признаков транзакций в контуре УВД, учитывающий принадлежность каждого признака к соответствующему измерению. В отличие от известного FP-Growth, предложенный метод обеспечивает сохранение структуры многомерных транзакций и позволяет выявлять устойчивые сочетания признаков, характерные для сетевой активности в контуре УВД;

3. разработан метод формирования компактного представления частых сочетаний признаков транзакций в контуре УВД, ориентированный на обработку больших массивов транзакций. Предложена модификация, основанная на изменении структуры таблицы заголовков FP-дерева и отказе от параллельного хранения и обработки множества условных деревьев. Использование связного списка обратного порядка и последовательной обработки префиксных путей позволяет снизить вычислительные затраты и обеспечить устойчивую работу алгоритма при высокой плотности признаков, характерной для сетевого трафика в контуре УВД;

4. разработан алгоритм обработки частых сочетаний признаков на основе структуры SD, обеспечивающий агрегацию базисов частых путей и корректный пересчёт поддержки вложенных сочетаний без необходимости полного перебора

всех комбинаций. Применение структуры SD позволяет существенно сократить потребление оперативной памяти и сохранить полноту извлечения частых сочетаний признаков при масштабировании объёма входных данных;

5. разработаны алгоритмы формирования ассоциативных правил, учитывающий совместную обработку плотных и разреженных признаков. Для разреженных элементов извлечение устойчивых сочетаний осуществляется на основе двумерной таблицы совместной встречаемости, что позволяет избежать построения условных деревьев и снизить вычислительные затраты. Для плотных элементов применяется последовательный обход многомерного дерева частых признаков с контролем структуры ветвлений, что обеспечивает извлечение частых сочетаний в пределах префиксных путей. Полученные множества объединяются с использованием ограниченного применения метода Apriori, что позволяет сформировать полный набор статистически устойчивых паттернов при контролируемом росте числа кандидатов;

6. разработан алгоритм классификации транзакций, основанный на агрегированном применении множества ассоциативных правил. Решение о наличии НСВ принимается по количественному критерию совместного выполнения правил в рамках одной транзакции. Такой подход позволяет учитывать фрагментарный характер проявлений НСВ в сетевом трафике и повышает устойчивость классификации в условиях неполноты наблюдаемых признаков.

Глава 4. Апробация методов и алгоритмов обнаружения несанкционированного вмешательства в контуре управления воздушным движением

4.1. Структурные особенности информационного обмена в контуре управления воздушным движением и условия его нарушения при несанкционированном вмешательстве

Для рассмотрения условий реализации НСВ в контуре УВД необходимо учитывать возможность внедрения ложных сообщений в заранее зафиксированный и воспроизведённый радиоэфир.

Представляя среду информационного обмена в контуре УВД как систему с распределённой архитектурой, опишем её основные составляющие.

СПД в контуре УВД может быть представлена как совокупность N передающих и M принимающих устройств, взаимодействующих в рамках радиоканала VDL-2 «воздух–земля». Обмен сообщениями осуществляется во времени и представляет собой последовательность сетевых взаимодействий, формируемых между бортовыми и наземными подсистемами.

Обобщённая схема наблюдаемого информационного обмена и условий его нарушения в контуре УВД представлена на рисунке 4.1.

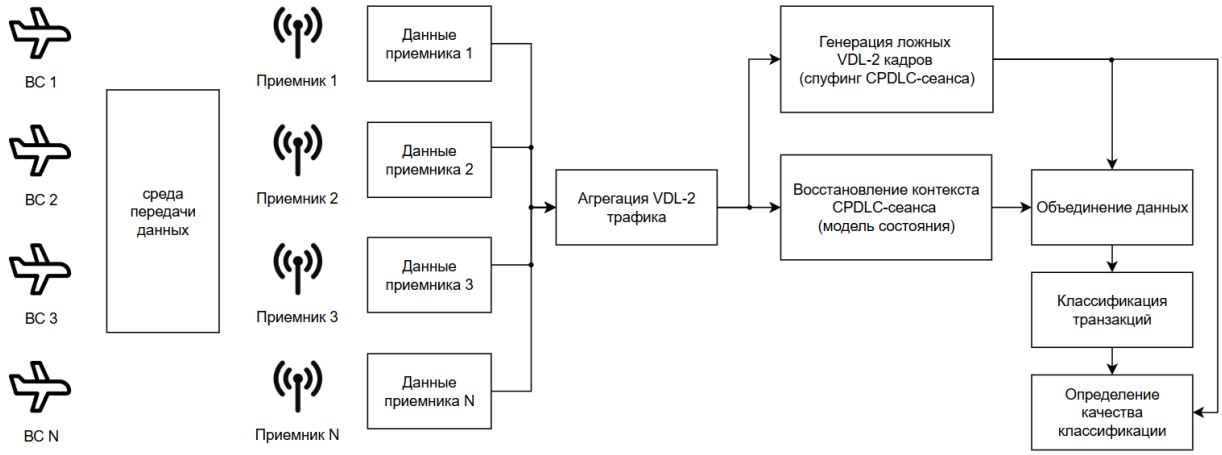

Рисунок 4.1 - Моделирование несанкционированного вмешательства в информационный обмен с использованием реальных сообщений в контуре УВД

Для анализа условий НСВ предполагается возможность внедрения дополнительных сообщений в поток наблюдаемого обмена. Такие воздействия могут осуществляться в произвольные моменты времени и соответствовать формальной структуре протокольного стека (AVLC, X.25, COTP, ACSE), что не позволяет выявить их на уровне прикладной семантики, однако приводит к изменению характеристик транзакций информационного обмена.

Приём и декодирование сообщений выполняется с использованием программно-определяемых радиоприёмников (SDR) и программных средств на базе dumpvdl2.

Современные SDR и программные обеспечивают не только приём, но и формирование радиосигналов в широком диапазоне частот, включая одновременный приём на нескольких частотах. Доступность таких устройств и их технические характеристики в теоретическом плане допускают возможность воспроизведения сигналов, соответствующих каналам передачи данных в контуре УВД, что следует учитывать при анализе угроз НСВ.

Ниже приведены характерные фрагменты информационного обмена, полученные при приёме и декодировании сигналов VDL-2. Примеры отражают типовые сценарии взаимодействия в стеке ATN/OSI и используются для иллюстрации структуры передаваемых данных и последующего выделения признаков.

Листинг 4.1

Пример декодирования запроса на регистрацию в сети УВД

```
[2020-09-25 01:49:28 GMT] [136.975] [1.0/-48.3 dBFS] [49.3 dB] [0.7 ppm] [S:0] [L:100] [F:0] [#0]
2A3197 (Ground station, On ground) -> 78157D (Aircraft): Command
  AVLC type: I sseq: 1 rseq: 7 poll: 0
    X.25 Data: grp: 11 chan: 255 sseq: 5 rseq: 5 more: 0
    Reasm status: skipped
    X.233 CLNP Data (compressed header):
      LRef: 0x0 Prio: 11 Lifetime: 97 Flags: 0xc0
      PDU Id: 12880
      X.224 COTP Connect Request:
        src_ref: 0x4c75 dst_ref: 0x0000
        Initial Credit: 15
        Protocol class: 4
        Options: 02 (use extended PDU formats)
        Calling transport selector: 65 6d
        Called/responding transport selector: 02 02
        TPDU size (bytes): 512
        ATN checksum: 75 3f 71 ea
        Checksum: 38 25
        Additional options: 0x00
        Ack time (ms): 1000
        Priority: 3
        Inactivity timer (ms): 360000
        X.225 Session SPDU: Short Connect
          X.227 ACSE Associate Request:
            Application context name: { 1.3.27.3.1 }
            AP title: { 1.3.27.2.10570260.0 }
            AE qualifier: 22
            ATCUplinkMessage: <empty PDU>
```

Передача осуществляется в составе AVLC-кадра типа I и содержит данные уровня X.25, инкапсулирующие протокол CLNP. На транспортном уровне наблюдается сообщение COTP Connect Request, сопровождаемое запросом на установление ассоциации прикладного уровня.

Подтверждение установления соединения осуществляется в обратном направлении от ВС к наземной станции. На транспортном уровне фиксируется сообщение COTP Connect Confirm, что свидетельствует об успешном установлении

соединения. Прикладным ответом регистрации в сети УВД является сообщение Associate result: accept.

Далее, рассмотрим прикладной обмен сообщениями по CPDLC. Передача управляющего сообщения показана ниже:

Листинг 4.2

Передача управляющего сообщения по CPDLC

```
[2020-09-25 14:24:15 GMT] [136.975] [1.1/-47.0 dBFS] [48.2 dB] [0.9 ppm] [S:0] [L:120] [F:0] [#1]
2A3197 (Ground station, On ground) -> 424963 (Aircraft): Command
AVLC type: I sseq: 2 rseq: 7 poll: 0
 X.25 Data: grp: 11 chan: 255 sseq: 7 rseq: 4 more: 0
  Reasm status: skipped
  X.233 CLNP Data (compressed header):
   LRef: 0x41 Prio: 11 Lifetime: 97 Flags: 0xc0
   PDU Id: 13511
   X.224 COTP Data (extended):
    dst_ref: 0x0033
    sseq: 2 req_of_ack: 0 EoT: 1
    ATN checksum: 09 a4 3d dc
    CPDLC Uplink Message:
     Header:
      Msg ID: 3
      Timestamp: 2020-09-25 14:24:05
      Logical ACK: required
     Message data:
      SQUAWK [code]
      Code: 4262
```

Передача осуществляется в рамках установленного соединения с использованием транспортных блоков данных COTP. Сообщение требует 2 подтверждения со стороны ВС: автоматическое подтверждение получения управляющего сообщения LOGICAL ACKNOWLEDGEMENT, и сообщения WILCO/UNABLE/STANDBY, которым экипаж ВС должен ответить диспетчеру:

Листинг 4.3

Ответное сообщение CPDLC

```
[2020-09-25 14:24:25 GMT] [136.975] [-33.4/-46.5 dBFS] [13.1 dB] [-0.1 ppm] [S:0] [L:54] [F:2] [#0]
424963 (Aircraft, Airborne) -> 2A3197 (Ground station): Command
AVLC type: I sseq: 4 rseq: 7 poll: 0
 X.25 Data: grp: 11 chan: 255 sseq: 7 rseq: 2 more: 0
  Reasm status: skipped
  X.233 CLNP Data (compressed header):
   LRef: 0x41 Prio: 11 Lifetime: 40 Flags: 0xf6
   PDU Id: 18
   X.224 COTP Data (extended):
    dst_ref: 0x4cb3
    sseq: 3 req_of_ack: 0 EoT: 1
    ATN checksum: 55 a9 29 ac
    CPDLC Downlink Message:
     Header:
      Msg ID: 3
      Msg Ref: 3
      Timestamp: 2020-09-25 14:24:23
      Logical ACK: required
     Message data:
      WILCO
```

Представленные фрагменты демонстрируют многоуровневую структуру информационного обмена в VDL-2, включающую канальный уровень AVLC, сетевой уровень X.25 и протоколы стека ATN/OSI. Анализ журналов позволяет выделить устойчивые комбинации признаков, соответствующие различным типам протокольных взаимодействий. Указанные признаки используются при формировании транзакционного представления трафика и последующем обнаружении НСВ без анализа семантики передаваемых сообщений.

На рисунке 4.2 представлена модель нарушения функционирования сеанса CPDLC, при котором за счёт искусственного прерывания соединения формируется последовательность повторных установлений сеанса CPDLC, что приводит к увеличению служебной нагрузки, снижению эффективности использования канала связи и деградации информационного обмена.

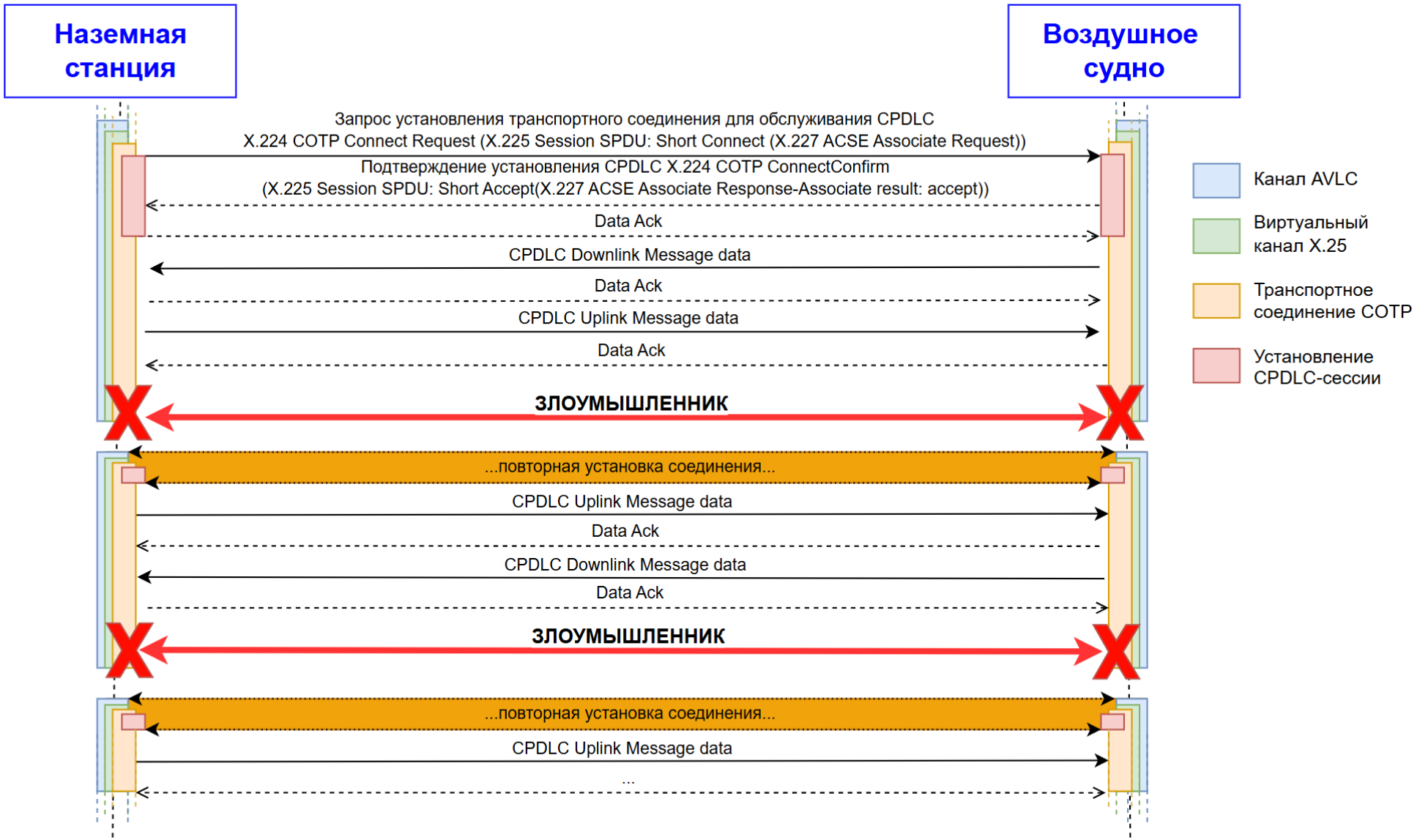

Рисунок 4.2 - Модель нарушения функционирования сеанса CPDLC

Таким образом, приём и декодирование сообщений CPDLC с использованием доступных SDR и программных инструментов не представляет существенной сложности и позволяет получить структурированную информацию о сетевом взаимодействии, а также проводить НСВ в контуре УВД. Получаемые данные отражают параметры протокольного обмена и могут рассматриваться как источник признаков при анализе НСВ.

Переходя к экспериментальной апробации, отметим, что разработанные методы и алгоритмы ориентированы на выявление отклонений в структуре и динамике транзакций информационного обмена (см. п. 3.1) на уровне сетевого взаимодействия. При этом анализ осуществляется без привлечения информации прикладного уровня, поскольку передаваемые сообщения могут быть формально корректными.

Методические рамки экспериментальной апробации ограничены рассмотрением активных форм НСВ, при которых нарушитель инициирует или модифицирует сетевое взаимодействие и тем самым формирует наблюдаемый трафик. Пассивные воздействия, не сопровождающиеся передачей сообщений в канал связи, не рассматриваются, поскольку не приводят к изменению характеристик транзакций.

В качестве исходной выборки для проведения экспериментальной апробации и сравнительного анализа использован набор данных CICIDS2017, содержащий размеченные потоки сетевого трафика с различными сценариями активных воздействий. Выбор данного набора обусловлен его потоковой природой и наличием широкого спектра аномалий, сопровождающихся изменением статистических характеристик транзакций, а также отсутствием репрезентативных авиационных наборов данных, отражающих специфику информационного обмена в контуре УВД.

Сценарии, представленные в CICIDS2017, рассматриваются как обобщённые модели активных сетевых воздействий, эквивалентные по структуре и динамике транзакций воздействиям, возникающим в контуре УВД. Такой подход позволяет оценить чувствительность разработанных методов и алгоритмов к выявлению

характерных отклонений в потоках транзакций при активном вмешательстве в информационный обмен.

В рамках экспериментальной апробации результаты анализа транзакций интерпретируются через классы активных несанкционированных воздействий, выделяемые на основе характера формирования транзакций и их влияния на параметры функционирования канала управления.

Первый класс характеризуется активным навязыванием служебного сетевого взаимодействия. Такие воздействия проявляются в виде серий нетипичных управляющих и служебных транзакций, не соответствующих штатной структуре обмена, и сопровождаются аномальным распределением временных и сетевых характеристик.

Второй класс связан с нарушением доступности канала связи и проявляется в перегрузке ресурсов передачи данных. На уровне транзакций это выражается в устойчивых отклонениях трафиковых и временных параметров, приводящих к деградации или прерыванию обмена информацией.

Третий класс объединяет координированные воздействия, при которых аномальные транзакции формируются несколькими источниками и обладают согласованной структурой и динамикой, что приводит к нарушению доверия к источникам информационного обмена.

Таким образом, рассмотренная структура информационного обмена и выделенные классы активных несанкционированных воздействий формируют основу для экспериментальной проверки разработанных методов и алгоритмов обнаружения НСВ. Представленные модели воздействий позволяют перейти к количественной оценке их обнаружения на основе анализа транзакционного представления трафика.

4.2. Исследование эффективности методов и алгоритмов обнаружения несанкционированного вмешательства

В качестве первого сценария апробации рассмотрен класс активных сетевых воздействий, связанных с активным навязыванием служебного сетевого взаимодействия в канале управления. Данный класс НСВ характеризуется формированием кратковременных транзакций, не приводящих к устойчивому развитию сеанса обмена, и направлен на формирование и проверку возможности логического сетевого взаимодействия между узлами в контуре УВД.

В рамках эксперимента в качестве модели такого НСВ использован сценарий *Port Scan* из набора данных CICIDS2017. При этом указанный сценарий используется исключительно как экспериментальная модель активной сетевой аномалии, формирующей последовательность короткоживущих транзакций с отсутствием развития логического обмена. Такой характер сетевого поведения соответствует активному навязыванию служебного взаимодействия и может быть наблюдаем на уровне транзакций независимо от конкретной протокольной реализации.

Для сценария Port Scan характерны следующие признаки транзакций: *Flow Duration, Total Fwd Packets, Total Backward Packets, Total Length of Fwd Packets, Active Mean* и *Idle Mean*. Пример используемого шаблона ассоциативных правил приведён на рис. 4.3.

Анализ сообщений VDL-2 показывает, что в авиационных каналах также наблюдаются события, эквивалентные по своей роли и структуре активному сетевому воздействию. В частности, в канале VDL-2 фиксируются одиночные или серийные кадры AVLC, не сопровождающиеся последующей передачей кадров информационного типа AVLC-I, что приводит к формированию кратковременных транзакций без развития обмена с последующим сбросом канала. Аналогичные

ситуации имеют место при передаче сообщений CPDLC, где инициирование виртуального канала X.25 и последующего транспортного взаимодействия COTP не приводит к устойчивому обмену данными.

```
Attack,Group,Values
PortScan,network,FIN Flag Count=0
PortScan,network,SYN Flag Count=0
PortScan,network,RST Flag Count=0
PortScan,network,PSH Flag Count=0
PortScan,network,ACK Flag Count=0
PortScan,temporal,Flow Duration=bin0
PortScan,traffic,Total Fwd Packets=bin0
PortScan,traffic,Total Backward Packets=bin0
PortScan,traffic,Total Length of Fwd Packets=bin0
PortScan,traffic,Total Length of Bwd Packets=bin0
PortScan,traffic,Active Mean=bin0
PortScan,traffic,Idle Mean=bin0
```

Рисунок 4.3 – Шаблон ассоциативных правил для сценария PortScan

Результаты апробации показали, что применение классифицирующих ассоциативных правил, сформированных на основе заданного шаблона, позволяет существенно сократить объём исходного множества правил и повысить точность выявления аномальных транзакций. После оптимизации параметров (длина правила — 2, порог совпадений — 150) достигнуто значение $F1 - \text{меры} = 0{,}93\%$, что подтверждается результатами тестирования, представленными на рис. 4.4.

Анализ зависимости доли истинно положительных решений от доли ложноположительных (ROC-кривая), приведённой на рис. 4.5, демонстрирует значение площади под кривой AUC = 0,93. Полученный результат свидетельствует о высокой чувствительности к выявлению транзакций, соответствующих сценарию активного служебного сетевого взаимодействия в канале управления, при сохранении допустимого уровня ложных срабатываний.

Precision

87.78%

Recall

99.84%

TP=49920, FP=6949, TN=43051, FN=80

Предсказания

	Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length
0	192.168.10.3-192.168.10.19-88-55341-17	192.168.10.19	55341	192.168.10.3	88	17	2017-07-07 01:00:00	440	2	2	352	358	176	
1	192.168.10.25-224.0.0.251-5353-5353-17	192.168.10.25	5353	224.0.0.251	5353	17	2017-07-07 01:00:00	1002497	26	0	1274	0	49	
2	192.168.10.16-192.168.10.50-60060-22-6	192.168.10.50	22	192.168.10.16	60060	6	2017-07-07 01:00:00	75	1	2	0	0	0	
3	192.168.10.12-192.168.10.50-35396-22-6	192.168.10.50	22	192.168.10.12	35396	6	2017-07-07 01:00:00	77	1	2	0	0	0	
4	192.168.10.16-192.168.10.50-60060-22-6	192.168.10.16	60060	192.168.10.50	22	6	2017-07-07 01:00:00	210	1	1	0	0	0	
5	192.168.10.16-192.168.10.50-60058-22-6	192.168.10.50	22	192.168.10.16	60058	6	2017-07-07 01:00:00	82	1	2	0	0	0	
6	192.168.10.9-192.168.10.50-6493-25909-6	192.168.10.50	25909	192.168.10.9	6493	6	2017-07-07 01:00:00	20	3	0	18	0	6	
7	192.168.10.3-192.168.10.19-53-61453-17	192.168.10.19	61453	192.168.10.3	53	17	2017-07-07 01:00:00	201	2	2	88	188	44	
8	192.168.10.255-192.168.10.5-137-137-17	192.168.10.5	137	192.168.10.255	137	17	2017-07-07 01:00:00	1513591	39	0	1950	0	50	
9	192.168.10.9-192.168.10.50-6492-21-6	192.168.10.50	21	192.168.10.9	6492	6	2017-07-07 01:00:00	67	1	3	6	18	6	

Рисунок 4.4 – Результат тестирования для Port Scan

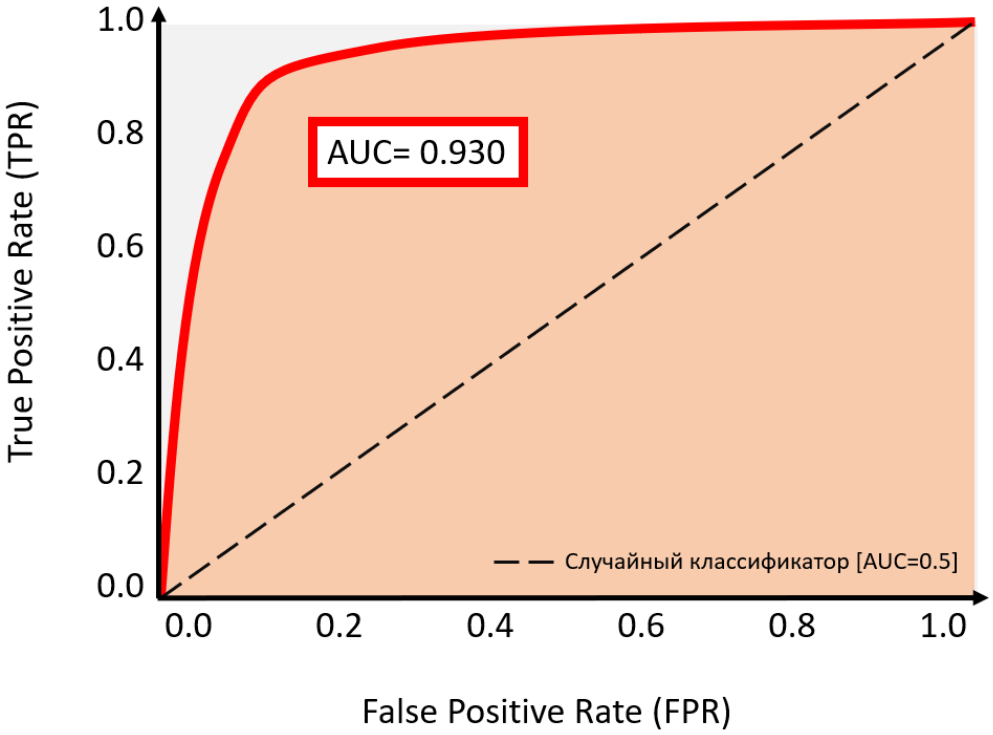

Рисунок 4.5 – ROC-кривая для атаки Port Scan

В качестве второго сценария апробации рассмотрен класс активных сетевых воздействий, приводящих к нарушению доступности канала управления за счёт перегрузки сетевого взаимодействия. Данный класс НСВ характеризуется формированием плотного потока однотипных транзакций, сопровождающихся сокращением интервалов простоя и увеличением непрерывной активности информационного обмена, что приводит к деградации или временному отказу канала передачи данных.

В рамках апробации в качестве модели такого воздействия использован сценарий DDoS из набора данных CICIDS2017. Указанный сценарий применяется не как конкретная прикладная атака, а как обобщённая модель перегрузочного сетевого воздействия, формирующего устойчивую аномальную структуру транзакций. Такой характер сетевого поведения проявляется на уровне агрегированных характеристик потоков и не зависит от прикладной семантики передаваемых сообщений.

Для сценария DDoS характерны признаки транзакций, отражающие наличие двустороннего логического взаимодействия и нагрузочный характер передачи данных. В используемом шаблоне ассоциативных правил задействованы следующие группы признаков: сетевые индикаторы активности (PSH Flag Count, ACK Flag Count), временные характеристики взаимодействия (Flow Duration), а также агрегированные показатели обмена Active Mean, Idle Mean, Total Fwd Packets, Total Backward Packets, Total Length of Fwd Packets, Total Length of Bwd Packets. Пример используемого шаблона классифицирующих ассоциативных правил приведён на рис. 4.6.

```
Attack,Group,Values
DDOS,network,PSH Flag Count=1
DDOS,network,ACK Flag Count=1
DDOS,temporal,Flow Duration=bin0|bin2|bin3|bin4
DDOS,traffic,Total Fwd Packets=bin0
DDOS,traffic,Total Backward Packets=bin0
DDOS,traffic,Total Length of Fwd Packets=bin0
DDOS,traffic,Total Length of Bwd Packets=bin0
DDOS,traffic,Active Mean=bin0
DDOS,traffic,Idle Mean=bin0|bin1|bin2|bin3|bin4
```

Рисунок 4.6 – шаблон ассоциативных правил для сценария DDoS

Результаты апробации показали, что использование классифицирующих ассоциативных правил, сформированных на основе заданного шаблона, позволяет существенно снизить количество ложноположительных срабатываний по сравнению с применением полного множества ассоциативных правил. После оптимизации параметров (минимальная длина правила — 4, порог совпадений — 150) достигнуты значения $Precision = 95{,}45\%$, $Recall = 82{,}94\%$ и $F1 - \text{мера} = 88{,}7\%$, что подтверждается результатами тестирования, представленными на рис. 4.7.

Precision

95.45%

Recall

82.94%

TP=10367, FP=494, TN=12006, FN=2133

Предсказания

	Init_Win_bytes_forward	Init_Win_bytes_backward	act_data_pkt_fwd	min_seg_size_forward	Active Mean	Active Std	Active Max	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label	Predicted	fires
4395	8192	229	2	20	0	0	0	0	0	0	0	0	DDoS	DDoS	212
4396	-1	-1	1	40	0	0	0	0	0	0	0	0	BENIGN	BENIGN	0
4397	256	-1	4	20	0	0	0	0	0	0	0	0	DDoS	DDoS	152
4398	256	229	6	20	4603068	0	4603068	4603068	65500000	0	65500000	65500000	DDoS	BENIGN	46
4399	229	256	4	20	33999	0	33999	33999	35100000	39200000	62800000	7390670	BENIGN	BENIGN	20
4400	256	-1	4	20	0	0	0	0	0	0	0	0	DDoS	DDoS	152
4401	229	256	4	20	1234856	0	1234856	1234856	70400000	0	70400000	70400000	BENIGN	BENIGN	26
4402	256	229	6	20	2001	0	2001	2001	36100000	43400000	66800000	5479913	DDoS	BENIGN	50
4403	8192	229	2	20	0	0	0	0	0	0	0	0	DDoS	DDoS	212
4404	256	-1	3	20	2	0	2	2	5727986	0	5727986	5727986	DDoS	DDoS	152

Рисунок 4.7 – Результат тестирования для DDoS

Анализ ROC-кривой, приведённой на рис. 4.8, демонстрирует значение площади под кривой AUC, приближенное к 0,9. Полученные результаты подтверждают устойчивость к выявлению перегрузочных сетевых воздействий в контуре УВД при изменении интенсивности и структуры трафика.

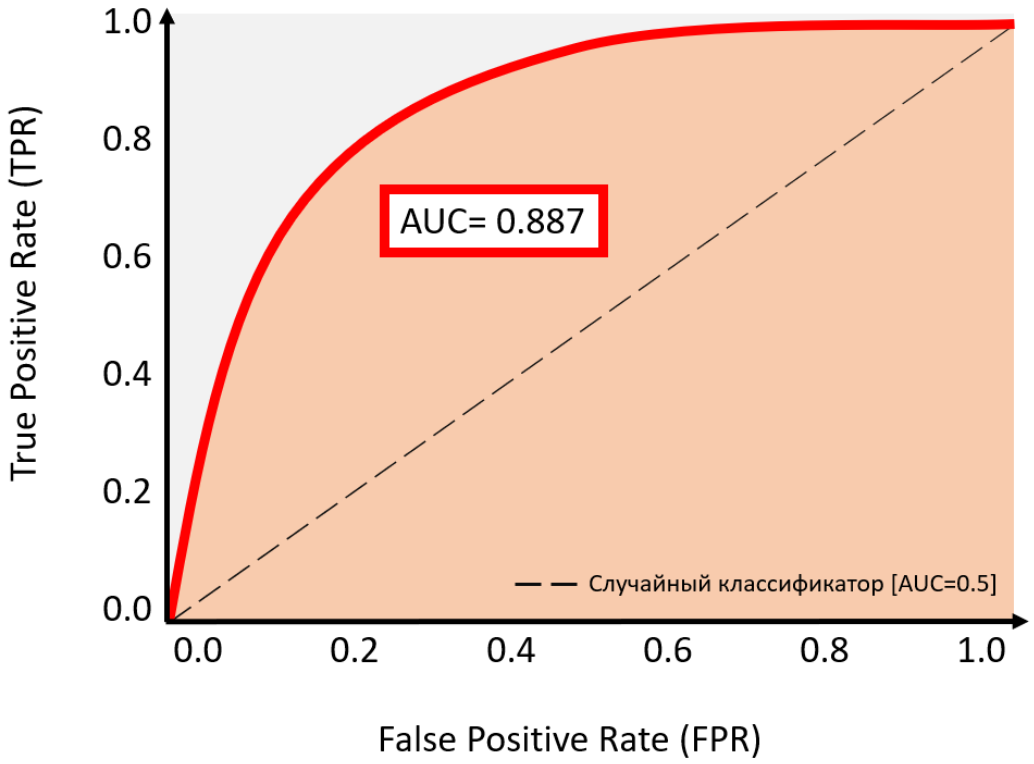

Рисунок 4.8 - ROC-кривая для атаки DDoS

В качестве третьего сценария апробации рассмотрен класс активных сетевых воздействий, характеризующихся координированным формированием аномальных транзакций несколькими источниками. Данный класс НСВ отличается устойчивостью во времени, согласованностью параметров сетевого обмена и формированием повторяющихся паттернов взаимодействия, не характерных для штатного функционирования каналов управления в контуре УВД.

В рамках апробации в качестве модели такого воздействия использован сценарий Botnet из набора данных CICIDS2017. Указанный сценарий применяется как обобщённая модель координированного активного сетевого воздействия, при котором множество узлов формируют однотипные транзакции с согласованными

характеристиками. Такой характер сетевого поведения проявляется на уровне агрегированных параметров потоков и не зависит от прикладной семантики передаваемых сообщений.

Для сценария Botnet характерны признаки транзакций, отражающие серийность и согласованность сетевого обмена. В используемом шаблоне классифицирующих ассоциативных правил задействованы временные индикаторы (Bwd IAT Min), показатели интенсивности обмена (Flow Packets/s, Bwd Packets/s), а также агрегированные характеристики структуры трафика (Total Length of Fwd Packets, Fwd Packet Length Max, Bwd Header Length). Пример шаблона классифицирующих ассоциативных правил для данного сценария приведён на рис. 4.9.

```
Attack,Group,Values
Bot,network,ID_net=Destination Port=8080
Bot,temporal,Bwd IAT Min=bin0
Bot,traffic,Init_Win_bytes_forward=bin0
Bot,traffic,Init_Win_bytes_backward=bin0|bin1
Bot,traffic,Bwd Packets/s=bin0
Bot,traffic,Bwd Header Length=bin0
Bot,traffic,Total Length of Fwd Packets=bin0
Bot,traffic,Flow Packets/s=bin2
Bot,traffic,Fwd Packet Length Max=bin0
```

Рисунок 4.9 – Шаблон ассоциативных правил для сценария Botnet.

Результаты апробации показали, что применение классифицирующих ассоциативных правил позволяет выделить устойчивые аномальные паттерны транзакций и существенно сократить исходное множество ассоциативных правил. При использовании параметров, аналогичных сценарию DDoS (минимальная длина правила — 4, порог совпадений — 150), получены значения $Precision = 100\%$ и $Recall = 91{,}20\%$ (рис. 4.10).

Precision

100.00%

Recall

91.20%

TP=1793, FP=0, TN=50000, FN=173

Предсказания

	Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Pac
0	192.168.10.3-192.168.10.50-389-42144-6	192.168.10.50	42144	192.168.10.3	389	6	2017-07-07 08:59:00	112740560	32	16	
1	192.168.10.3-192.168.10.5-389-54107-17	192.168.10.5	54107	192.168.10.3	389	17	2017-07-07 09:00:00	126	2	2	
2	192.168.10.3-192.168.10.14-389-50981-17	192.168.10.14	50981	192.168.10.3	389	17	2017-07-07 09:00:00	130	2	2	
3	192.168.10.3-192.168.10.5-53-54104-17	192.168.10.5	54104	192.168.10.3	53	17	2017-07-07 09:00:00	148	2	2	
4	192.168.10.3-192.168.10.5-88-49169-6	192.168.10.5	49169	192.168.10.3	88	6	2017-07-07 09:00:00	71	1	4	
5	192.168.10.3-192.168.10.14-53-58421-17	192.168.10.14	58421	192.168.10.3	53	17	2017-07-07 09:00:00	140	2	2	
6	192.168.10.14-224.0.0.252-62000-5355-17	192.168.10.14	62000	224.0.0.252	5355	17	2017-07-07 09:00:00	416932	22	0	
7	192.168.10.3-192.168.10.25-53-64992-17	192.168.10.25	64992	192.168.10.3	53	17	2017-07-07 09:00:00	250	2	2	
8	192.168.10.3-192.168.10.14-389-58423-17	192.168.10.14	58423	192.168.10.3	389	17	2017-07-07 09:00:00	159	2	2	
9	192.168.10.3-192.168.10.9-53-62625-17	192.168.10.9	62625	192.168.10.3	53	17	2017-07-07 09:00:00	198	2	2	

Рисунок 4.10 – Результат тестирования для Botnet

Полученные результаты указывают на возможность выявления устойчивых фоновых аномальных режимов сетевого информационного обмена, формирующих предпосылки для реализации более сложных авиационных сценариев НСВ без анализа прикладного содержания сообщений.

Площадь ROC-кривой, приведённой на рис. 4.11, превышает 0,9, что соответствует высокому качеству классификации.

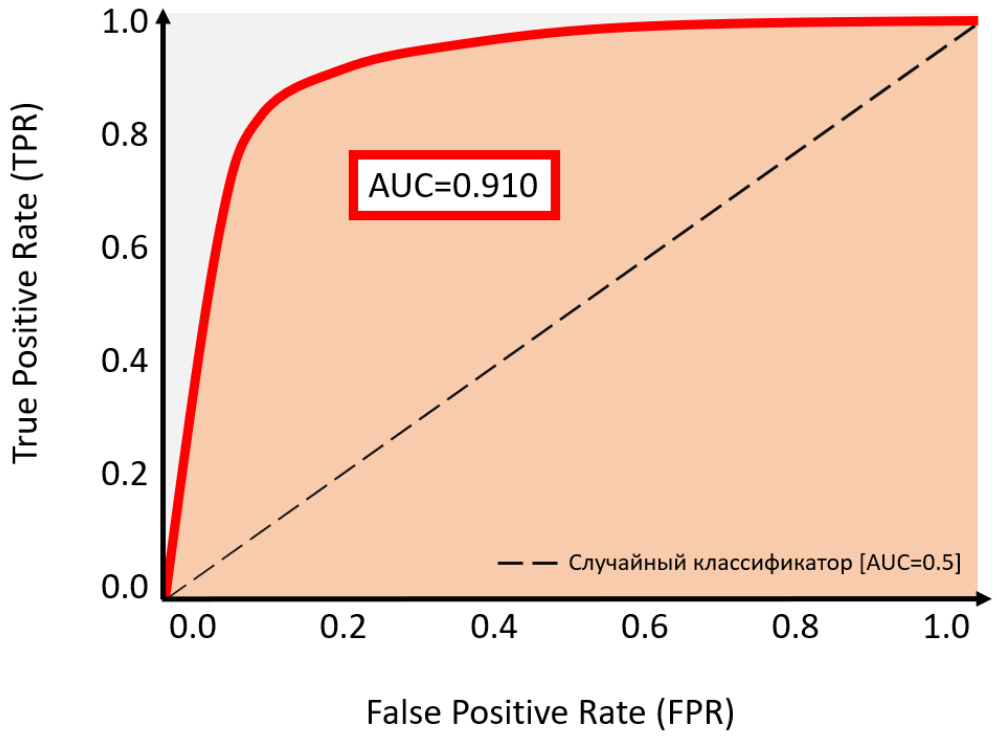

Рисунок 4.11 - ROC-кривая для атаки Botnet

Результаты апробации подтверждают, что разработанные методы и алгоритмы выявляют активные сетевые воздействия, проявляющиеся в структуре и динамике транзакций информационного обмена в контуре УВД. Выявляемые классы воздействий формируют наблюдаемые предпосылки для реализации авиационных сценариев НСВ, включая спуфинг, обрыв связи и возможное изменение траектории полёта, при сохранении формальной корректности передаваемых сообщений.

Для оценки эффективности разработанных методов и алгоритмов выполнен сравнительный анализ с известными методами машинного обучения,

применяемыми для выявления сетевых аномалий. В качестве показателей качества использовались стандартные метрики Accuracy, Precision, Recall и F1-score, рассчитываемые по формулам (4.1)–(4.4). Итоговые значения метрик определялись методом микросреднего подхода (micro-average) по совокупности рассмотренных сценариев активных НСВ.

1. Точность классификации (Accuracy):

$$Accuracy = \sum_{i=1}^{K} \frac{TP^{[i]} + TN^{[i]}}{TP^{[i]} + FN^{[i]} + TN^{[i]} + FP^{[i]}} \tag{4.1}$$

2. Точность предсказания (Precision):

$$Precision = \sum_{i=1}^{K} \frac{TP^{[i]}}{TP^{[i]} + FP^{[i]}} \tag{4.2}$$

3. Полнота (Recall):

$$Recall = \sum_{i=1}^{K} \frac{TP^{[i]}}{TP^{[i]} + FN^{[i]}} \tag{4.3}$$

4. Гармоническое среднее точности и полноты (F1-мера):

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \tag{4.4}$$

Результаты приведены в таблице 4.1. Анализ показывает, что разработанные методы и алгоритмы НСВ в контуре УВД обеспечивают сопоставимый уровень точности с обучаемыми моделями, такими как метод опорных векторов и дерево решений, при отсутствии этапа предварительного обучения. Значение F1-меры составляет 92,7 %, что свидетельствует о сбалансированном соотношении точности и полноты при выявлении активных сетевых воздействий в контуре УВД.

Таблица 4.1. Результаты эксперимента

Метод	Accuracy	Precision	Recall	F1-score	Этап обучения
Дерево решений	99,8%	99,7%	99,9%	99,8%	Требуется
Метод опорных векторов	95%	94%	91%	92%	Требуется
Нейронная сеть	83%	85%	80%	82%	Требуется
Байесовский метод	14%	20%	12%	15%	Требуется
K-средних	60%	30%	75%	43%	Требуется
Предлагаемые методы и алгоритмы	93.9%	89.3%	96.3%	92.7%	Не требуется

Особенностью разработанных методов и алгоритмов является высокая полнота выявления НСВ (Recall = 96,3 %), что имеет принципиальное значение для задач защиты от НСВ, где пропуск опасного воздействия недопустим и может привести к авиационному инциденту. В отличие от известных методов машинного обучения, требующих наличия размеченных данных и адаптации модели под конкретный тип трафика, разработанные методы и алгоритмы функционируют в полностью автономном режиме и опираются на внутренние закономерности потока сетевых транзакций.

При проведении эксперимента была произведена оценка важности каждого из признаков, результаты представлены на рисунке 4.12.

Рисунок 4.12 – Вклад признаков при классификации транзакций

Таким образом, сравнительный анализ подтверждает, что разработанные методы и алгоритмы обеспечивают высокую точность и полноту выявления активных НСВ на уровне сетевого информационного обмена и обладают преимуществами в условиях отсутствия обучающих выборок и необходимости адаптации к разнородным авиационным каналам передачи данных.

Получено свидетельство о регистрации программы для ЭВМ (см. Приложение А) [104]. Результаты данного параграфа представлены в [105].

4.3. Рекомендации по внедрению методов и алгоритмов обнаружения несанкционированного вмешательства в контуре управления воздушным движением

Внедрение разработанных методов и алгоритмов обнаружения НСВ в контуре УВД должно осуществляться с учётом требований документов ИКАО, EUROCONTROL, EASA, RTCA и EUROCAE, при этом их применение не должно приводить к изменению логики протокольного обмена и процедур CPDLC. Ключевыми ограничениями являются обеспечение совместимости существующих

систем, непрерывности обслуживания и сохранение штатных характеристик функционирования каналов передачи данных, включая временные параметры обмена и порядок установления и сопровождения соединений.

С учётом указанных требований применение разработанных методов и алгоритмов должно выполняться как аналитическая функция, не участвующая в формировании и передаче сообщений. Методы и алгоритмы должны использовать только уже имеющиеся в системе данные информационного обмена, формируемые в процессе функционирования каналов связи и обработки сообщений. Такой подход позволяет исключить влияние на протокольные процедуры, исключает необходимость изменения существующих протоколов и обеспечивает возможность внедрения без модификации взаимодействия между наземными и бортовыми системами.

В наземном сегменте внедрение методов и алгоритмов обнаружения НСВ выполняется в соответствии с сертификационными требованиями Федерального агентства воздушного транспорта для комплекса средств автоматизации управления воздушным движением (КСА УВД). Указанными требованиями определяется состав КСА УВД:

1. групповые средства приёма и обработки информации;
2. автоматизированные рабочие места диспетчеров УВД;
3. средства документирования и воспроизведения информации;
4. средства единого времени;
5. средства технического управления и контроля;
6. пультовое оборудование;
7. комплект системного и прикладного программного обеспечения.

Методы и алгоритмы обнаружения НСВ реализуются в составе групповых средств приёма и обработки информации КСА УВД без дополнительного вмешательства в процессы передачи данных и изменения протокольной архитектуры. Размещение в групповых средствах приёма и обработки информации определяется составом КСА УВД, в котором остальные элементы комплекса выполняют функции отображения, документирования, управления и контроля. При

этом должны сохраняться автоматизированное взаимодействие диспетчер–пилот по CPDLC с использованием установленных сообщений, автоматическая регистрация информации технического управления и контроля, контроль качества и загруженности каналов передачи данных от средств взаимодействующих объектов, возможность разрешения и запрета выдачи в обработку информации, поступающей от источников наблюдения и из каналов передачи данных, а также соблюдаться требования к прикладному программному обеспечению.

Для бортового сегмента внедрение ограничено архитектурой бортовой авионики и распределением функций между её элементами. Применение разработанных методов и алгоритмов возможно в составе CMU, обеспечивающего обмен данными по каналу VDL-2 и функционирование служб CPDLC. Данный блок обеспечивает обработку сообщений и взаимодействие с наземными системами, что позволяет использовать его как точку внедрения без изменения других бортовых систем.

Внедрение в состав FMS не допускается, поскольку данный комплекс относится к контуру управления полётом ВС и его модификация в рамках задач анализа информационного обмена недопустима. Следовательно, применение разработанных методов и алгоритмов на борту ограничивается функциями, связанными с обработкой и передачей сообщений, без вмешательства в процессы управления полётом.

Рекомендации представлены на рисунке 4.13. На рисунке показано размещение методов и алгоритмов обнаружения НСВ в контуре УВД: в бортовом сегменте — на уровне CMU, в наземном сегменте — на уровне групповых средств приёма и обработки информации КСА УВД. В указанных элементах формируется уведомление о НСВ в канал VDL-2, который передаётся в средства отображения: на борту — экипажу, в наземном сегменте — диспетчеру. Полученная информация используется для принятия решения о дальнейшем использовании канала передачи данных и переходе на резервные каналы связи.

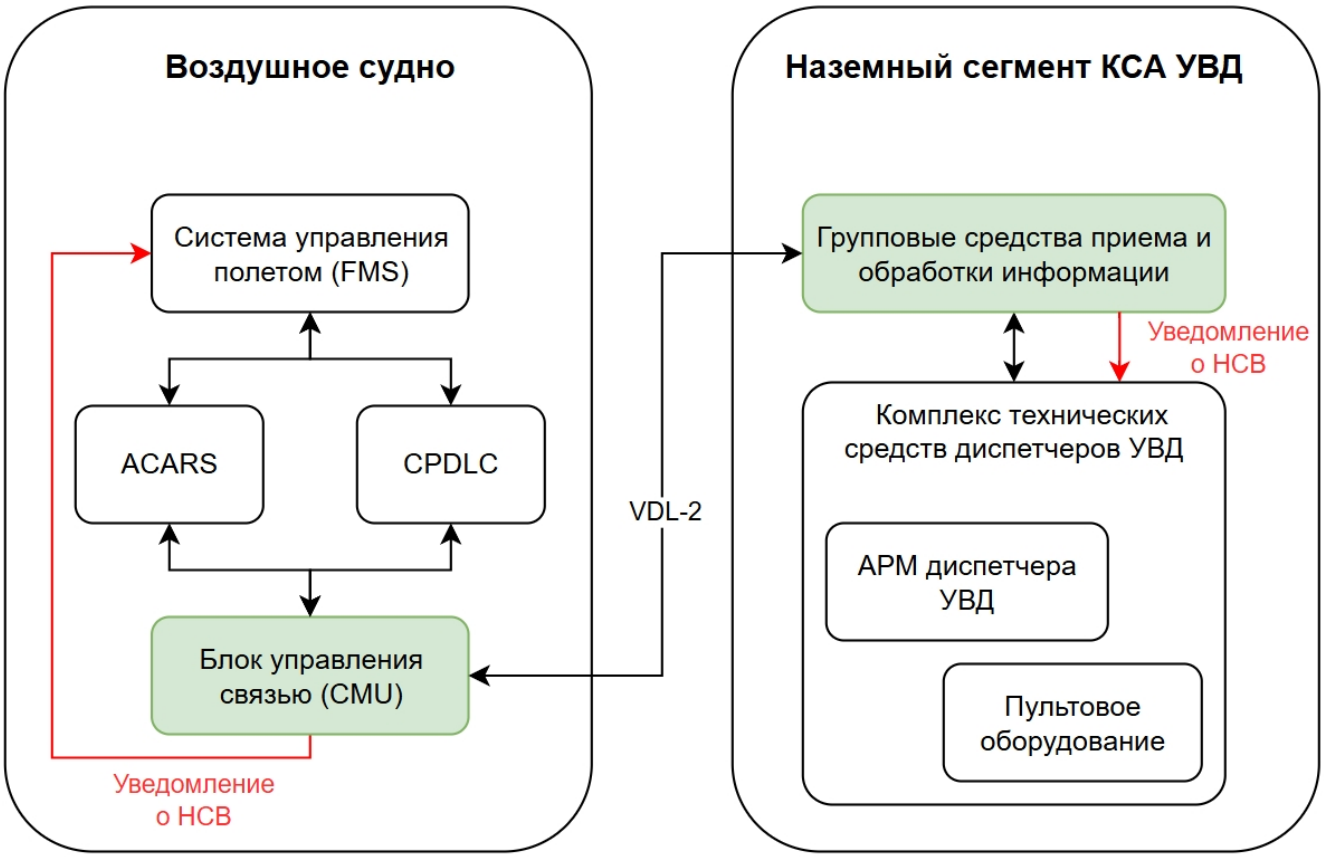

Рисунок 4.13 – Рекомендации по внедрению в контуре управления воздушным движением

Таким образом, основное применение разработанных методов и алгоритмов обнаружения НСВ в контуре УВД должно быть сосредоточено в наземном сегменте на уровне групповых средств приема и обработки информации, где доступны необходимые данные информационного обмена и обеспечиваются их обработка, объединение, регистрация и хранение. На борту ВС применение разработанных методов и алгоритмов ограничивается CMU и выполняется без изменения логики функционирования бортовых систем и без вмешательства в контур управления полётом.

Выводы по главе 4

В четвертой главе были получены следующие основные результаты и выводы:

1. Проведена апробация разработанных методов и алгоритмов обнаружения НСВ в контуре УВД на уровне сетевого информационного обмена. Подтверждена их работоспособность при анализе транзакций, формируемых на основе заголовков протоколов, без использования информации прикладного уровня и без анализа семантики передаваемых сообщений, что обеспечивает их применимость в контуре УВД в условиях НСВ. В отличие от известных методов машинного обучения, предлагаемый подход не требует предварительного этапа обучения и обеспечивает высокую полноту выявления НСВ.

2. Установлено, что внедрение разработанных методов и алгоритмов обнаружения НСВ в контуре УВД возможно без изменения штатного протокольного обмена при соблюдении требований международной нормативной базы ИКАО, EUROCONTROL, EASA, а также стандартов RTCA и EUROCAE, регламентирующих функционирование наземных и бортовых систем передачи данных.

3. Разработанные методы и алгоритмы обнаружения НСВ в контуре УВД применимы как в наземных системах в составе КСА УВД на уровне групповых средств приёма и обработки информации, так и на борту ВС в составе CMU.

Заключение

В работе решена актуальная **научно-техническая задача** разработки методов и алгоритмов обнаружения несанкционированного вмешательства в сети передачи данных систем управления воздушным движением на основе технологий искусственного интеллекта, имеющая существенное значение для развития авиационной отрасли Российской Федерации. Цель и задачи диссертационного исследования достигнуты.

В диссертационной работе получены следующие основные результаты:

1. проведён анализ СПД в контуре УВД. Показано, что рост объёмов передаваемой информации и применение устаревших технологий приводят к увеличению числа потенциальных уязвимостей и векторов НСВ;

2. проведён анализ НСВ в контуре УВД. Выделены векторы воздействия на автоматизированные системы УВД, бортовые компоненты и каналы «воздух–земля», установлены характерные направления реализации атак и их влияние на устойчивость информационного обмена;

3. проведён анализ методов и алгоритмов машинного обучения для обнаружения НСВ в контуре УВД. Установлено, что универсального решения не существует, большинство подходов требует размеченных данных и не учитывает специфику контура УВД, что обосновывает необходимость разработки методов, не зависящих от предварительного обучения;

4. разработана формализованная модель СПД в контуре УВД в виде графа, учитывающая вероятностные характеристики отказов узлов и каналов и сценарии НСВ;

5. разработана Е-модель угроз НСВ в контуре УВД, описывающая типовые сценарии атак с учётом особенностей телекоммуникационной инфраструктуры и обеспечивающая формализованное задание воздействий в рамках общей модели;

6. разработана стохастическая модель формирования НСВ на сетевой информационный обмен в контуре УВД, описывающая состояние системы в виде составного процесса с пуассоновским потоком внешних воздействий. Показано, что нарушение функционирования реализуется через два конкурирующих механизма — накопленный и мгновенный, для которых получены аналитические выражения вероятностей.

7. разработан метод многомерного анализа частых наборов признаков транзакций информационного обмена в контуре УВД, основанный на представлении элементов транзакции в виде пары «значение–измерение», что позволяет учитывать принадлежность признаков к различным атрибутам при их совместном анализе;

8. разработан метод компактного представления транзакций информационного обмена в контуре УВД на основе структуры суффиксных данных, позволяющие уменьшить объём обрабатываемых данных и обеспечить эффективный перебор сочетаний без полного обхода всех условных деревьев при сохранении информативности для дальнейшего анализа НСВ;

9. разработаны алгоритмы извлечения частых сочетаний признаков и классификации транзакций информационного обмена в контуре УВД, основанные на совместном использовании двумерной таблицы совместных появлений признаков и многомерной структуры частых элементов, обеспечивающие раздельную обработку плотных и разреженных признаков и на их основе формирование ассоциативных правил для выявления НСВ;

10. показано, что разработанные методы и алгоритмы обеспечивают сопоставимый уровень точности при отсутствии этапа обучения и превосходит сравниваемые решения по полноте (96,3%) выявления НСВ;

11. разработанные методы и алгоритмы обнаружения НСВ в контуре УВД применимы как в наземных системах в составе КСА УВД на уровне групповых средств приёма и обработки информации, так и на борту ВС в составе CMU.

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

1. совершенствование методов и алгоритмов обнаружения и предотвращения новых составных видов сценариев НСВ в контур УВД;

2. разработка репрезентативного авиационного набора данных, учитывающего специфику телекоммуникационных процессов в контуре УВД и применимого для тестирования алгоритмов обнаружения НСВ;

3. расширение области применения разработанных методов и алгоритмов на каналы управления и обмена данными с БАС, рассматриваемыми как элементы контура УВД, с учётом их особенностей и дополнительных сценариев НСВ.

Список используемых сокращений

УВД – управление воздушным движением

ОрВД – организация воздушного движения

СПД – сети передачи данных

НСВ – несанкционированное вмешательство

ВС – воздушное судно

БАС – беспилотные авиационные системы

АС УВД – автоматизированная система управления воздушным движением

VDL-2 – цифровой канал ОВЧ режима 2

HFDL – цифровой канал ВЧ

SATCOM – спутниковая связь

CPDLC – цифровая линия передачи данных «диспетчер-пилот»

CMU – блок управления связью

ACARS – адресно-отчётная система авиационной связи

FMS – система управления полетом

COTS – коммерческие программно-аппаратные решения

FP-Growth – метод роста частых шаблонов

COFI-tree – дерево совместно встречающихся частых наборов

SDR – программно-определяемый радиоприемник

КСА УВД – комплекс средств автоматизации управления воздушным движением

Список используемых источников

1. **Hillebrecht, A.; Marks, T.; Gollnick, V.** An aeronautical data communication demand model for the North Atlantic oceanic airspace // CEAS Aeronautical Journal. 2023. Vol. 14. No. 2. P. 553–567.

2. **Adamopoulou, E.; Daskalakis, E.** Applications and technologies of big data in the aerospace domain [Электронный ресурс] // Electronics. 2023. Vol. 12, iss. 10. ID: 2225. DOI: 10.3390/electronics12102225.

3. **ИКАО.** Civil Aviation Cybersecurity Action Plan [Электронный ресурс]. — International Civil Aviation Organization, 2014. — URL: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf (дата обращения: 12.03.2026).

4. **Eurocontrol**, Link 2000+ programme: Atc data link operational guidance for link 2000+ services, 2010.

5. **Collinson** R.P.G. Introduction to Avionics Systems. FourthEdition - Springer, 2023.

6. **Plass S.** (ed.) Future Aeronautical Communications. - Simon Plass ITAvE, 2016.

7. **ИКАО**, Aeronautical communications panel (acp) wg f, need for spectrum for future aeronautical air/ground communication systems, 2006.

8. **ERAA**, Unifying european air transport air traffic communication plans avanti air moves forward, J. Eur. Regions Airline Assoc, 2006.

9. **ИКАО**. Manual on VHF Digital Link (VDL) Mode 2 (Doc 9776/AN970). — 2nd ed. — Montreal: ICAO, 2015.

10. **Visée C.** VDL2 monitoring flights report: Analysis of the 2022 EUROCONTROL flight monitoring campaigns. — EUROCONTROL Network Management Directorate, 2023. — 39 p.

11. **Eurocontrol**, Datalink Capacity Analysis: Datalink Performance and Capacity Analysis – 2024 report. — EUROCONTROL Network Management Directorate, 2025. — 185 p.

12. **Eurocontrol**, Datalink Summer Performance Report. — EUROCONTROL, 2025. — 2 p.

13. **Eurocontrol**, Datalink FACT (perFormance And Capacity sTudy). — EUROCONTROL Network Management Directorate, 2025.

14. **Shingledecker, C.; Giles, S.; Darby, J.; Pino J.; Hancock T.R.**, Projecting the effect of cpdlc on nas capacity, in: Proc. 24th Digital Avionics Systems Conf. DASC 2005, vol. 1, 2005.

15. **Sabatini, R.** Cyber Security in the Aviation Context. - RMIT University School of Engineering – Aerospace Engineering and Aviation Discipline, 2016.

16. **Зыбин, Е. Ю.; Сельвесюк, Н. И.; Косьянчук, В. В.** Патент на полезную модель № 216356 U1 Российская Федерация, МПК H04L 12/02, H04L 47/32. Бортовой киберзащищенный концентратор данных : № 2022130255 : заявл. 22.11.2022 : опубл. 31.01.2023 / Е. Ю. Зыбин, Н. И. Сельвесюк, В. В. Косьянчук [и др.] ; заявитель ФАУ "ГосНИИАС". – EDN ULEKYR.

17. **Платошин, Г. А.; Косьянчук, В. В.; Гласов, В. В.** Патент на полезную модель № 232134 U1 Российская Федерация, МПК H04L 12/66, H04L 65/102. Высокоскоростной бортовой киберзащищенный шлюз : заявл. 26.12.2024 : опубл. 25.02.2025 / Г. А. Платошин, В. В. Косьянчук, В. В. Гласов [и др.] ; заявитель Федеральное автономное учреждение «Государственный научно-исследовательский институт авиационных систем». – EDN HXTUMC.

18. **Косьянчук, В. В.; Сельвесюк, Н. И.; Зыбин, Е. Ю.** Концепция обеспечения информационной безопасности бортового оборудования воздушного судна / В. В. Косьянчук, Н. И. Сельвесюк, Е. Ю. Зыбин [и др.] // Вопросы кибербезопасности. – 2018. – № 4(28). – С. 9-20. – DOI 10.21681/2311-3456-2018-4-9-20. – EDN VSVPVW.

19. **Мищенко, И. Б.; Косьянчук, В. В.; Зыбин, Е. Ю.; Платошин, Г. А.** Обеспечение кибербезопасности сверхзвукового пассажирского самолёта / И. Б.

Мищенко, В. В. Косьянчук, Е. Ю. Зыбин, Г. А. Платошин // Решетневские чтения : Материалы XXVIII Международной научно-практической конференции, посвященной 100-летию со Дня рождения генерального конструктора ракетно-космических систем академика Михаила Федоровича Решетнева: 2-х частях, Красноярск, 18–22 ноября 2024 года. – Красноярск: Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева, 2024. – С. 396-397. – EDN UJUXZD.

20. **Ганичев, А. А.** Модель угроз несанкционированного вмешательства в беспроводных информационных системах авионики / А. А. Ганичев, К. В. Пителинский, С.А. Кесель, В.А. Пиков // Вопросы защиты информации. – 2024. – № 4(147). – С. 35-43. – DOI 10.52190/2073-2600_2024_4_35. – EDN XIUJTJ.

21. **Петров, В. И.** Методика анализа программного обеспечения бортовых компьютеров воздушного судна на отсутствие недекларированных возможностей сигнатурно-эвристическим способом / В. И. Петров // Научный вестник Московского государственного технического университета гражданской авиации. – 2017. – Т. 20, № 1. – С. 186-193. – EDN XYGDSP.

22. **Antipov, I. S.; Arustamyan, S. S.; Ganichev, A. A.**, Intelligent Fuzzing Method for Aviation Information Systems as Part of the Secure Software Development Cycle / I. S. Antipov, S. S. Arustamyan, A. A. Ganichev [et al.] // Russian Engineering Research. – 2025. – Vol. 45, No. 5. – P. 685-690. – DOI 10.3103/S1068798X25700728. – EDN GSVQUW.

23. **Liu, J.X.; Jiang, H.; Dong, X.F,** et al. Dynamic collaborative sequencing method for arrival flights based on air tracffic density. Acta Aeronautica et Astronatutica Sinica, 2020, 41(7): 323717.

24. **Chen, Y. T.; Hu, M. H.; Yang, L.**, et al. Autonomous trajector planning and conflict management technology in restricted air space. Acta Aeronautica et Astronatutica Sinica, 2020, 41(9): 324045.

25. **Акиншин, Р. Н.** Обеспечение информационной защищенности автоматизированных систем управления воздушным движением в условиях роста интенсивности полетов: специальность 05.22.13 «Навигация и управление

воздушным движением» : автореферат диссертации на соискание ученой степени доктора технических наук / Акиншин Руслан Николаевич. – Москва, 2009. – 40 с. – EDN NKVXIT.

26. **Beeby, M.**, Aviation quality cots software: reality or folly, in: The 21st, Digital Avionics Systems Conference, 2002. Proceedings. vol. 1, 2002, pp. 5D2–1–5D2–10.

27. **Alford, L. D.**, The problem with aviation COTS, in IEEE Aerospace and Electronic Systems Magazine, vol. 16, no. 2, pp. 33-37, Feb. 2001, doi: 10.1109/62.904242.

28. **Mäurer, N.; Guggemos, T.; Ewert, T.; Gräupl,T.; Schmitt, C.; Grundner-Culemann, S.** Security in Digital Aeronautical Communications: A Comprehensive Gap Analysis // International Journal of Critical Infrastructure Protection. — 2022. — Vol. 38. — Art. 100549. — DOI: 10.1016/j.ijcip.2022.100549.

29. **Zhu, Y.; Wang, Z.; Guo, K.; Dan, Z.** L-band digital aeronautical communications system development status and challenges // Acta Aeronautica et Astronautica Sinica. — 2024. — Vol. 45, No. 10. — Art. 029161. — DOI: 10.7527/S1000-6893.2023.29161.

30. **Федеральный закон** от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» // Собрание законодательства РФ. — 2007. — № 7. — Ст. 837.

31. **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.

32. **ИКАО**. Assembly — 42nd Session. Resolutions [Электронный ресурс]. — Montreal: ICAO, 2025. — URL: https://www.icao.int/sites/default/files/Meetings/a42/Documents/Resolutions/a42_res_prov_en.pdf (дата обращения: 12.03.2026).

33. **Gonzalo, J.** Cybersecurity in aviation: a review of threats, solutions, and future directions // Scientific Journal of Engineering and Technology. — 2025. — Vol. 2, No. 2. — P. 149–157. — URL: https://journals.stecab.com/sjet/article/view/1198 (дата обращения: 12.03.2026).

34. **Post, J.E.; Cooke, D.L.; Patterson, M.D.** Failures of critical systems at airports: Impact on aircraft operations. // Safety Science. 2017. Vol. 94. P. 128–137. DOI: 10.1016/j.ssci.2017.01.003

35. **Kraut, J.M.; Kiken, A.; Billinghurst, S.; Morgan, C.A.; Strybel, T.Z.; Chiappe, D.; Vu, K.-P.L.** Effects of Data Communications Failure on Air Traffic Controller Sector Management Effectiveness, Situation Awareness, and Workload // Human Interface and the Management of Information. Interacting with Information (HCII 2011). Lecture Notes in Computer Science. – Berlin; Heidelberg: Springer, 2011. – Vol. 6772. – P. 493–499

36. **Subotic, B.; Stojkovic, I.; Milinkovic, S.** Controller recovery from equipment failures in air traffic control: A framework for the quantitative assessment of the recovery context // Reliability Engineering & System Safety. – 2014. – Vol. 132. – P. 167–177.

37. **Martini, D.** Cybersecurity in Aviation and ATM insights [Электронный ресурс]. — 3 December 2024. — URL: https://eu-lac-app.eu/public/uploads/Cybersecurity-in-Aviation-and-ATM-insights-COCESNA-ACCSA.pdf (дата обращения: 12.03.2026).

38. **ИКАО**. Global Operational Data Link Document (GOLD). Tech. rep. Second edition. International Civil Aviation Organization, Apr. 2013. URL: https://www.icao.int/APAC/Documents/edocs/GOLD _2Edition.pdf. (дата обращения: 12.03.2026).

39. **Orye, E.; Visky, G.; Maennel, O.** Analysing the Actual Use of Controller–Pilot Data Link Communications // Engineering Proceedings. — 2022. — Vol. 28, No. 1. — Art. 18. — DOI: 10.3390/engproc2022028018.

40. **Varun, S.; Jacobs, M.A; Dervisevic, A; De-Laurentis, D.** ADS-B and CPDLC fault modeling for safety assessment in a distributed environment. In: 2018 IEEE Aerospace Conference. Mar. 2018, pp. 1–14. DOI: 10.1109/AERO.2018.8396582.

41. **Habler, E.; Bitton, R.; Shabtai, A.** Evaluating the Security of Aircraft Systems [Электронный ресурс]. — 2022. — URL: https://arxiv.org/abs/2209.04028 (дата обращения: 12.03.2026).

42. **Ukwandu, E.; Ben Farah, M. A.; Hindy,** et al. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends // Information. — 2022. — Vol. 13, No. 3. — Art. 146. — DOI: 10.3390/info13030146.

43. **Eskilsson, S.; Gustafsson, H.; Khan, S.; Gurtov A.** 2020. Demonstrating ADS-B and CPDLC Attacks with Software-Defined Radio. In 2020 Integrated Communications Navigation and Surveillance Conference (ICNS). IEEE, 1B2–1.

44. **Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I.** 2017. Analyzing privacy breaches in the aircraft communications addressing and reporting system (acars). arXiv preprint arXiv:1705.07065 (2017).

45. **Lehto, A.; Sestorp, I.; Khan, S.; Gurtov, A.** Controller Pilot Data Link Communication Security: A Practical Study. In: 2021 Integrated Communications Navigation and Surveillance Conference (ICNS). 2021, pp. 1–11. DOI: 10.1109/ICNS52807.2021.9441649.

46. **Sathaye, H.; Noubir, G.; Ranganathan, A.** On the Implications of Spoofing and Jamming Aviation Datalink Applications // Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC). — 2022. — P. 548–560. — DOI: 10.1145/3564625.3564651.

47. **Buch,** et al. What the Hack Happened to the Flight Deck: Analyzing the Impact of Cyber Attacks on Commercial Flight Crews. – DOI: 10.2514/6.2019-0060

48. **Marco, D.; Manzo, A.; Ivaldi, M.; Hird, J.** Security Testing with Controller-Pilot Data Link Communications, 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 2016, pp. 526-531, DOI: 10.1109/ARES.2016.104

49. **Zhang, R.; Liu, G.; Liu, J.; Jan, P.** Analysis of Message Attacks in Aviation Data-Link Communication // IEEE Access. — 2018. — Vol. 6. — P. 68033–68042. — DOI: 10.1109/ACCESS.2017.2761768.

50. **Ганичев, А. А.** Статистический анализ потенциальных угроз информационной безопасности в бортовой сети воздушного судна / А. А. Ганичев, К. В. Пителинский, В. В. Бритвина // Вопросы защиты информации. – 2024. – № 1(144). – С. 11-22. – DOI 10.52190/2073-2600_2024_1_11. – EDN QDMBBK.

51. **Бекенева, Я. А.; Шипилов, Н. Н.; Майер, Ю. Л.; Шоров, А. В.** DRDoS-атаки и механизмы защиты от них // Известия СПбГЭТУ «ЛЭТИ» № 1/2017. - С. 1-7

52. **Gonzalo, J.** Cybersecurity in Aviation: A Review of Threats, Solutions, and Future Directions // Scientific Journal of Engineering and Technology. – 2025. – Vol. 2, No. 2. – P. 149–157. – DOI: 10.69739/sjet.v2i2.1198.

53. **ARINC** 823-1:2007. DataLink Security – Part 1: ACARS Message Security. – Annapolis: Aeronautical Radio, Inc., 2007. – 264 p.

54. **ARINC** 823-2:2008. DataLink Security – Part 2: Key Management. – Annapolis: Aeronautical Radio, Inc., 2008. – 72 p.

55. **Khan, S.; Gurtov, A.; Breaken, A.; Kumar, P.** A Security Model for Controller-Pilot Data Communication Link. In: 2021 Integrated Communications Navigation and Surveillance Conference (ICNS). 2021, pp. 1–10. DOI: 10.1109/ICNS52807.2021.9441637.

56. **Sacre, P.; Isaac D.** Link 2000+ Guidance to Airborne Implementers. — Eurocontrol, 2014.

57. **Sudarsanan, V. S.; Jacobs, M. A.; Dervisevic, A.; DeLaurentis, D.** ADS-B and CPDLC fault modeling for safety assessment in a distributed environment. Mar. 2018. DOI: 10.1109/AERO.2018.8396582.

58. **Петров, В. И.** Практическое применение методов машинного обучения в задаче определения истинности сообщений системы автоматического зависимого наблюдения / В. И. Петров, А. О. Машошин, Н. О. Машошин // Гражданская авиация на современном этапе развития науки, техники и общества : Сборник тезисов докладов Международной научно-технической конференции, посвященной 50-летию МГТУ ГА, Москва, 25–26 мая 2021 года. – Москва: ИД Академии Жуковского, 2021. – С. 377-380. – EDN NEBWFL.

59. **Ганичев, А. А.** Применение алгоритмов машинного обучения в задаче обнаружения несанкционированного вмешательства в авиационные сети передачи данных / А. А. Ганичев // Труды Академии наук авиации и воздухоплавания. – 2025. – № 1. – С. 49-59. – EDN GECJYU.

60. **Komviriyavut, T.; Sangkatsanee, P.; Wattanapongsakorn, N.;** et al. Network intrusion detection and classification with decision tree and rule-based approaches // International Symposium on Communications and Information Technology. Icheon:[s.n.], 2009:1046-1050.

61. **Kbbes, T.; Bouhoula, A.; Rusinowitch, M.** Efficient decision tree for protocol analysis in intrusion detection]. International Journal of Security C Networks, 2010, 5 (4), pp. 220-235.

62. **Sinapiromsaran, K.; Techaval, N.** Network intrusion detection using multi-attributed frame decision tree // International Conference on Digital Information C Communication Technology C its Applications. Bangkok, 2012:203-207.

63. **Sahu, S.; Mehtre, B. M.** Network intrusion detection system using J48 decision Tree // International Conference on Advances in Computing, Communications and Informatics. Kochi, 2015:1-6.

64. **Amini, M.; Jalili, R.** RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks. Computers C Security, 2006, 25 (6):459-468.

65. **Carpenter, G.; Grossberg, S.** Adaptive resonance theory[R]. CAS/CNS Technical Report Series-008, Cambridge, MA: MIT, 2003:89-90.

66. **Aljurayban, N. S.; Emam, A.** Framework for cloud intrusion detection system service // IEEE World Symposium on Web Applications and Networking. Sousse:IEEE, 2015:174-184.

67. **Ishitaki, T.; Elmari, D.; Liu, Y.,** et al Application of neural networks for intrusion detection in Tor networks // IEEE, International Conference on Advanced Information Networking and Applications Workshops. Gwangiu: IEEE, 2015:67-72.

68. **Bao, X.; Xu, T.; Hou, H.** Network intrusion detection based on support vector machine// International Conference on Management and Service Science. Wuhan, 2009:21-23.

69. **Li, H.; Gu, D.** A novel intrusion detection scheme using support vector machine fuzzy network for mobile ad Hocnetworks // Web Mining and Web-based Application. Wuhan 2009:47-50.

70. **Zhang, W.; Teng, S.; Zhu, H.;** et al. Fuzzy multi-class support vector machines for cooperative network intrusion detection // IEEE International Conference on Cognitive Informatics. Beijing: IEEE, 2010:811-818.

71. **Liu, Z.; Kang, J.; Li, Y.** A hybrid method of rough set and support vector machine in network intrusion detection // Signal Processing Systems (ICPS). Dalian, 2010:561-5 63.

72. **Lin, N.; Xiang, C.** A wavelet transform based support vector machine ensemble algorithm and its application in network intrusion detection // Fifth International Conference on Intelligent Systems Design and Engineering Applications. Hunan, 2014;109-113.

73. **Lin, L.; Zhang, Y.** Network intrusion detection method by least squares support vector machine classifier // IEEE International Conference on Computer science and Information Technology. Chengdu: IEEE, 2010:295-297.

74. **Wang, Z.** Fault diagnosis for wireless sensor network based on genetic-support vector machine // International Conference on Computer Science and Network Technology. Harbin, 2011:2691-2694.

75. **Hu, J.** Network intrusion detection algorithm based on improved support vector machine // International Conference on Intelligent Transportation, Big Data and Smart City. Halong Bay, 2015:523-526.

76. **Fung, C.; Zhang, J.; Boutaba, R.** Effective acquaintance management based on Bayesian learning for distributed intrusion detection networks. IEEE Transactions on Network C Service Management, 2012, 9 (3): 320-332.

77. **Guan, K.; Kong, X.** Research on application of Bayesian discriminant method in intrusion detection model // International Conference on Information Technology and Electronic Commerce. Dalian, 2014, pp.180-183.

78. **Modi, C.; Patel, R.; Patel, A.;** et al. Bayesian, classifier and snort-based network intrusion detection system in cloud computing // Computing Communication C Networking Technologies (ICCCNT). Coimbatore, 2012, pp. 1-7.

79. **Shivaii, S.; Patil, A.B.** Energy efficient intrusion detection scheme based on Bayesian energy prediction in WSN // 2015 Fifth International Conference on Advances in Computing and Communications (ICACC). Kochi, 2015, pp. 114-117.

80. **Klassen, M.; Yang, N.** Anomaly based intrusion detection in wireless networks using Bayesian classifier // IEEE Fifth International Conference on Advanced Computational Intelligence. // IEEE, 2012, p. 257-264.

81. **Xiao, L.; Chen, Y.; Chang, C. K.** Bayesian model averaging of Bayesian network classifiers for intrusion detection // IEEE 38th International Computer Software and Applications Conference Workshops. Vasteras; IEEE, 2014; pp. 128-133.

82. **Nia, F. Y.; Khali, M.** An efficient modeling algorithm for intrusion detection systems using C5.0 and Bayesian network structures // International Conference on Knowledge-Based Engineering and Innovation. Tehran, 2015, pp. 1117-1123.

83. **Han, X.; Xu, L.; Ren, M.;** et al A naive Bayesian network intrusion detection algorithm based on principal component analysis // International Conference on Information Technology in Medicine and Education. Huangshan, 2015, pp. 325-328.

84. **Kanungo, T.; Mount D. M.;** et al. An efficient K-means clustering algorithm; Analysis and implementation. IEEE Transactions on Pattern Analysis C Machine Intelligence, 2002, 24(7), pp. 881-892.

85. **Wang, S.** Research of intrusion detection based on an improved K-means algorithm// Second International Conference on Innovations in Bio-inspired Computing and Applications. Shenzhen, 2011, pp. 274-276.

86. **Meng, J.; Shang, H.; Ling, B.** The application on intrusion detection based on k-means cluster algorithm // International Forum on Information Technology and Applications. Chengdu, 2009, pp. 150-152.

87. **Wang, H.; Yang, H.; Xu, Z.;** et al. A clustering algorithm use SOM and K-means in intrusion detection // The International Conference on E-Business and E-Government. Guangzhou, China, 2010, pp. 1281-1284.

88. **Muda, Z.; Yassin, W.; Sulaiman, M.N.;** et al. Intrusion detection with K-means clustering and one R classification. // Journal of Information Assurance C Security, 2012,7(6), pp. 55-66.

89. **Jirachan, T.; Piromsopa, K.** Applying KSE-test and K-means clustering towards scalable unsupervised intrusion detection // International Joint Conference on Computer Science and Software Engineering. Songkhla, 2015, pp. 43-49.

90. **Li, T.; Wang, J.** Research on network intrusion detection system based on improved K-means clustering algorithm // International Forum on Computer Science Technology and Applications. Chongqing, 2010, pp. 76-79.

91. **Pathak, V.; Ananthanarayana, VS.** A novel multi-threaded K-means clustering approach for intrusion detection // IEEE International Conference on Computer Science and Automation Engineering.: IEEE, 2012. pp. 34-38.

92. **Eslamnezhad, M.; Varjani, A. Y.** Intrusion detection based on minmax K-means clustering // International Symposium on Telecommunications. Tehran, 2014. pp.804-808.

93. **Sandhya, G.; Julian, A.** Intrusion detection in wireless sensor network using genetic K-means algorithm // International Conference on Advanced Communication, Control and Computing Technologies. Ramanathapuram, 2014, pp. 1791-1794.

94. **Ashok, R.; Lakshmi, A.J.,** et al. Optimized feature selection with K-means clustered triangle svm for intrusion detection. // International Conference on Advanced Computing. Chennai, 2011, pp. 23-27.

95. **Tang, P.; Jiang, R.; Zhao, M.** Feature selection and design of intrusion detection system based on K-means and triangle area support vector machine // International Conference on Future Networks. Sanya, Hainan, 2010. pp. 144-148.

96. **Sharma, S. K.; Pandey, P.; Tiwari, S. K.;** et al. An improved network intrusion detection technique based on K-means clustering via naive Bayes classification // International Conference on Advances in Engineering, Science and Management, Nagapattinam. Tamil Nadu, India, 2012, pp. 417-422.

97. **Varuna, S.; Natesan, P.** An integration of K-means clustering and naive Bayes classifier for intrusion detection // International Conference on Signal Processing, Communication and Networking. Chennai, 2015.

98. **Muda, Z.; Yassin, W.; Sulaiman, M. N.,** et al. Intrusion detection based on K-means clustering and naive Bayes classification // International Conference on Information Technology in Asia. IEEE, 2011, pp. 1-6.

99. **Chandrasekhar, A. M.; Raghuveer, K.** Intrusion detection technique by using K-means, fuzzy neural network and SVM classifiers // International Conference on Computer Communication and Informatics. Coimbatore, 2013, pp. 1-7.

100. **Shah, F. M.; Biswas, N. A.; Tammi, W. M.;** et al. An improvised intrusion detection system with hybridization of neural network and K-means clustering over feature selection by PCA // International Conference on Computer and Information Technology. Dhaka,2015, pp. 317-322.

101. **Ганичев, А.А.; Петров, В.И.** Математическая модель угроз авиационной сети передачи данных в условиях несанкционированного вмешательства. Научный вестник МГТУ ГА. 2025;28(4):40-49. https://doi.org/10.26467/2079-0619-2025-28-4-40-49

102. **Ганичев, А. А.** Метод анализа многомерных сочетаний признаков сетевого трафика для выявления признаков несанкционированного вмешательства в авиационных сетях передачи данных. Научный вестник МГТУ ГА. 2025;28(5):8-21. https://doi.org/10.26467/2079-0619-2025-28-5-8-21

103. **Ganichev, A.A., Pikov, V.A., Kolesnikova, D.S.** et al. Research on Methods for Detecting Unauthorized Interference in Data Transmission Networks in Air Transport. J. Commun. Technol. Electron. 70, 756–765 (2025). https://doi.org/10.1134/S1064226926600474

104. **Ганичев, А. А.** Свидетельство о государственной регистрации программы для ЭВМ № 2025669371 Российская Федерация. Программа для обнаружения несанкционированного вмешательства в информационно-вычислительных процессах подсистемы телекоммуникаций АС УВД на основе интеллектуальных алгоритмов без этапа обучения : №2025665933 : заявл. 23.06.2025: опубл. 25.07.2025 / А. А. Ганичев, Гребенников М.А., Колесникова Д.С. – EDN XNFXDL.

105. **Ганичев, А.А.; Гребенников, М. А.** Многомерные правила ассоциации в задаче обнаружения несанкционированного вмешательства в контуре управления воздушным движением / М. А. Гребенников, А. А. Ганичев // Развитие науки в XXI веке: вызовы, достижения и перспективы : Сборник научных трудов по материалам III Международной научно-практической конференции, Анапа, 01 августа 2025 года. – Анапа: ООО "Научно-исследовательский центр экономических и социальных процессов" в Южном Федеральном округе, 2025. – С. 58-64. – EDN JXFOUQ]

Приложение А

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025669371

Программа для обнаружения несанкционированного вмешательства в информационно-вычислительных процессах подсистемы телекоммуникаций АС УВД на основе интеллектуальных алгоритмов без этапа обучения

Правообладатель: ***Ганичев Александр Александрович (RU)***

Авторы: ***Ганичев Александр Александрович (RU), Гребенников Матвей Андреевич (RU), Колесникова Дарья Сергеевна (RU)***

Заявка № **2025665933**

Дата поступления **23 июня 2025 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***25 июля 2025 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0692e7c1a6300bf54f240f670bcca2026
Владелец Зубов Юрий Сергеевич
Действителен с 10.07.2024 по 03.10.2025

Ю.С. Зубов