МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(Дипломная работа)

На тему «Системы аунтификации и идентификации при работе протоколов дистанционной автоматизации корабельной связи»

Исполнитель _____ Шарипов Рамиль Ренатович
(подпись) (фамилия, имя, отчество)

Руководитель _____ Яготинцева Наталья Владимировна
(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Бурлов Вячеслав Георгиевич
(подпись) (фамилия, имя, отчество)

«____» _____ 2025 г.

Санкт–Петербург

2025

ВВЕДЕНИЕ

В условиях современного мореплавания, характеризующегося высокой степенью технологической интеграции и возрастанием угроз в киберпространстве, обеспечение защищённой связи между суднами, береговыми службами и вспомогательными объектами приобретает критически важное значение. В этом контексте особую роль играют процессы идентификации и аутентификации, являющиеся неотъемлемыми элементами общей системы информационной безопасности в корабельной связи. Применение безэкипажных надводных суден в Северном Морском Пути является достаточно перспективным направлением, поскольку использование БЭНС сокращает затраты на экипаж, а также снижает риски вреда их здоровью.

Северный морской путь – один из кратчайших путей, проходящий вдоль Северного Ледовитого океана от Мурманска, до Владивостока. Его преимущество – сокращение времени перевозки судов с крупногабаритным грузом, когда другие методы могут быть недостаточными, вроде железнодорожных путей, или могут оказаться слишком дорогими, как например, авиаперевозки.

Однако для эффективного функционирования безэкипажных судов в СевМорПути необходимо произвести модернизацию портовой инфраструктуры, которые ходят в данный регион, а также произвести ряд разработок по усовершенствованию технологии безэкипажного транспорта.

Актуальность исследования определяется необходимостью создания надёжных и защищенных систем идентификации и аутентификации для автоматических комплексов связи, эксплуатируемых в условиях Арктики. Развитие Северного морского пути, усложнение задач мониторинга, связи и навигации, а также внедрение безэкипажных катеров требуют обеспечения устойчивой работы судовых систем при ограниченном доступе к высокоскоростным каналам связи. В этих условиях особую значимость

приобретает разработка систем идентификации и аутентификации для протоколов дистанционной автоматизации корабельной связи.

Целью данной выпускной квалификационной работы является разработка концепции системы автоматизации аутентификации и идентификации между узлами связи и безэкипажными катерами, эксплуатируемыми в условиях Арктики, с учётом требований и особенностей радиосреды Северного Морского Пути и подходов к безопасности.

Задачи исследования:

1) Проанализировать сущность процессов аутентификации и идентификации, применительно судоходству.
2) Проанализировать существующие решения в области идентификации и аутентификации судов при работе протоколов дистанционной корабельной связи
3) Выявить особенности радиосвязи в условиях СевМорПути
4) Разработать концептуальную систему для идентификации и аутентификации судов в Арктических условиях с учетом особенностей радиосреды.

Объект исследования: системы аутентификации и идентификации

Предмет исследования: особенности процессов аутентификации и идентификации в условиях эксплуатации в Северном Морском Пути

В первой главе раскрыты исторические аспекты, опознавания и идентификации судов, сами понятия аутентификация и идентификация применительно судоходству, их роли в осуществлении данных процессов, а также произведен анализ существующих решений.

Во второй главе проведена работа по выявлению уязвимостей в обеспечении безопасного радиообмена для автоматической идентификации и аутентификации безэкипажных судов. Рассмотрены теоретические основы построения для построения легковесных и устойчивых информационных систем.

В третьей главе были разработаны форматы, а также классификация сообщений и логика их обмена для реализации бесперебойной работы в условиях низких пропускных способностей каналов связи. Вычислена скорость передачи данных, с учетом радиосреды в Северном Морском Пути и накладных расходов от используемых технологий.

Глава 1. Научно-теоретические и прикладные основы идентификации и аутентификации в судоходстве

1.1 Исторические аспекты идентификации морских судов

Проблема идентификации морских судов имеет глубокие исторические корни и непосредственно связана с необходимостью обеспечения безопасности, навигационной прозрачности и устойчивости морской торговли и военной деятельности. Ещё задолго до появления электронных систем судовладельцы, капитаны и государственные органы стремились к тому, чтобы каждый морской объект можно было однозначно опознать в пространстве и во времени. Первоначально такая идентификация осуществлялась на основе визуальных признаков, среди которых доминировали флаги, окраска корпуса, знаки принадлежности к определённой державе или флотилии, а также уникальные конструкционные особенности судна. Эти средства носили символический и правовой характер, но были крайне ограничены по своим возможностям, особенно в условиях ограниченной видимости или большой дистанции.

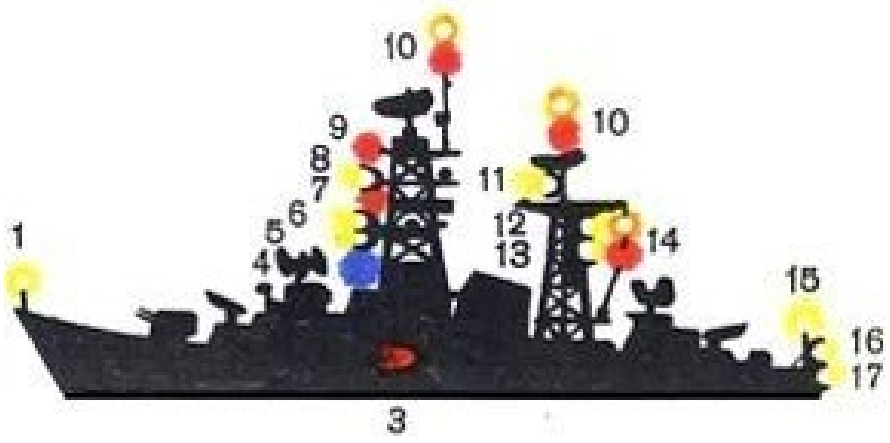

Рисунок 1.1.1. Виды судовых сигнальных огней.

1 — штаговый якорный (включается, когда корабль стоит на якоре); 2 — правый отличительный (ходовой, включается, когда корабль идет);
3 — левый отличительный; 4 — дежурный (его зажигает дежурный корабль); 5 — нижний топовый (ходовой); 6 — нижний буксирный (его включает буксирующий корабль); 7 и 9 — аварийные огни (будучи включеными, означают, что корабль не может управляться); 8 — верхний буксирный; 10 — клотиковые огни (для переговоров в ночное время по азбуке Морзе); 11 — верхний топовый (ходовой); 12 — флаг манский (означает присутствие на борту старшего начальника — флагмана); 13 — верхний кильватерный (включается для того, чтобы идущему сзади кораблю было удобнее держать строй; 14 — гафельные огни (включаются, когда надо показать, что корабль военный; например, при входе ночью на рейд); 15 — гакабортный якорный; 16 — нижний кильватерный; 17 — гакабортный ходовой.

Развитие мореплавания в эпоху Великих географических открытий и становление международной торговли породили необходимость в более структурированной и стандартизированной системе идентификации. Государства начали формировать свои судовые реестры, в которых каждому судну присваивался определённый регистрационный номер и документальное подтверждение права на плавание под определённым флагом. Уже в XVIII–XIX веках идентификационные признаки судна начали включать не только название, но и порт приписки, имя судовладельца, а также технические параметры: водоизмещение, тип, тоннаж, габариты. Однако вся эта информация оставалась на бумажных носителях и не могла быть оперативно проверена в условиях морской навигации, особенно при встрече судов в открытом море или вблизи стратегических проливов.

Серьёзный импульс к формализации и стандартизации идентификационных процедур был дан с развитием военно-морского флота и усилением контроля над морскими путями в XIX веке. Возникновение паровых судов, способных проходить большие расстояния независимо от погодных условий, а также рост пиратства и контрабанды потребовали от

государств введения более надёжных форм учёта и контроля за передвижением судов. Именно в этот период начал активно использоваться визуальный обмен сигналами — в частности, сигнальные флажные коды, позволявшие передавать не только команды и сообщения, но и коды, указывающие на принадлежность судна к конкретному государству или организации. Такие системы, однако, оставались ограниченными в своём функционале, требуя непосредственной видимости и значительных навыков расшифровки со стороны экипажа.

XX век стал поворотным в истории идентификации морских судов. С распространением радиосвязи стало возможным использовать радиопозывные как средство не только связи, но и аутентификации. Каждому судну начали присваиваться уникальные радиопозывные, регистрируемые в международных организациях. Это нововведение позволило значительно расширить возможности дистанционной идентификации: судно, находящееся на значительном расстоянии, могло быть опознано по радиосигналу, даже при отсутствии визуального контакта. Радиопозывной стал неотъемлемой частью международного морского права и вошёл в состав всех форм отчётности и обмена информацией на море.

Следующий этап в развитии идентификационных средств связан с бурным развитием цифровых и телекоммуникационных технологий, а также с возникновением международных институтов, регулирующих безопасность мореплавания. Одним из ключевых событий стало учреждение Международной морской организации (IMO, International Maritime Organization), которая взяла на себя задачу координации стандартов идентификации и регистрации морских судов. В 1987 году была принята система номеров IMO, представляющая собой уникальный числовой идентификатор, присваиваемый каждому судну на всём протяжении его существования. В отличие от названия или флага, которые могли изменяться при продаже судна или смене порта приписки, номер IMO сохраняется

неизменным и позволяет обеспечить непрерывность наблюдения за объектом независимо от его статуса и текущей юрисдикции.

Нарастающая сложность логистических и навигационных задач, обусловленная глобализацией и ростом объёма морских перевозок, поставила вопрос об автоматизации процессов идентификации. В 1990-е годы была введена система MMSI (Maritime Mobile Service Identity), предназначенная для идентификации не только судов, но и береговых станций, спасательных средств, а также групп судов.

MMSI – Maritime Mobile Service Identity. Он всегда состоит из 9 цифр, например, 667557000, и обязательно содержит трехзначный код страны, так называемый MID – Maritime Identification Digits. Например, MID 273 означает Россию, коды 232, 233, 234 и 235 отведены для Великобритании, 338, 366, 367, 368, 369 – для США.

Существуют три основных разновидности MMSI:

1. Для судовых радиостанций. MMSI формируется так: MIDXXXXXX

   MID – код страны, X – любая цифра от 0 до 9.
2. Для береговых радиостанций: коду страны предшествуют два нуля: 00MIDXXXX
3. Групповой MMSI. Присваивается сразу группе судов: флотилии, пароходству и т.д., всегда начинается с одного ведущего нуля: 0MIDXXXXX

MMSI-коды стали частью автоматизированных систем связи, включая ГМССБ (Глобальную морскую систему связи при бедствии) и АИС (автоматическую систему идентификации), и используются в радиообмене для облегчения поиска, установления связи, подтверждения личности объекта. Эти системы, являясь результатом десятилетий эволюции, стали краеугольным камнем современных автоматизированных протоколов связи в судоходстве, обеспечивая непрерывность, точность и безопасность информационного обмена между морскими объектами.

ГМССБ (GMDSS) - глобальная морская система связи при бедствии, использующая современные наземные, спутниковые и судовые системы радиосвязи. Система разработана членами Международной морской организации (IMO) и представляет собой существенное усовершенствование способов аварийной связи. Все суда, попадающие под действие Международной Конвенции о безопасности жизни на море (SOLAS) должны полностью соответствовать требованиям ГМССБ.

Вся акватория мирового океана разбита на районы. Каждый район обусловлен каналами связи с ситуационно-координационным центром, тем самым выход в каждый район должен сопровождаться обеспечением поддержки связи по этим каналам. Это достигается путем установки на борту специализированного оборудования. Районы нумеруются и имеют следующее определение и каналы связи:

1. Район А1 — это район, в котором осуществляется передача данных по каналу УКВ, хотя бы с одной береговой станцией, оборудованной системой ЦИВ.
2. Район А2 — это район, в котором связь осуществляется на ПВ, хотя бы с одной береговой станцией, оборудованной системой ЦИВ, за исключением района А1.
3. Район А3 — это район, в котором связь происходит через спутниковую систему связи Инмарсат, за исключением районов А1 и А2.
4. Район А4 — это акватория мирового океана, которая не вошла в районы А1, А2 и А3.

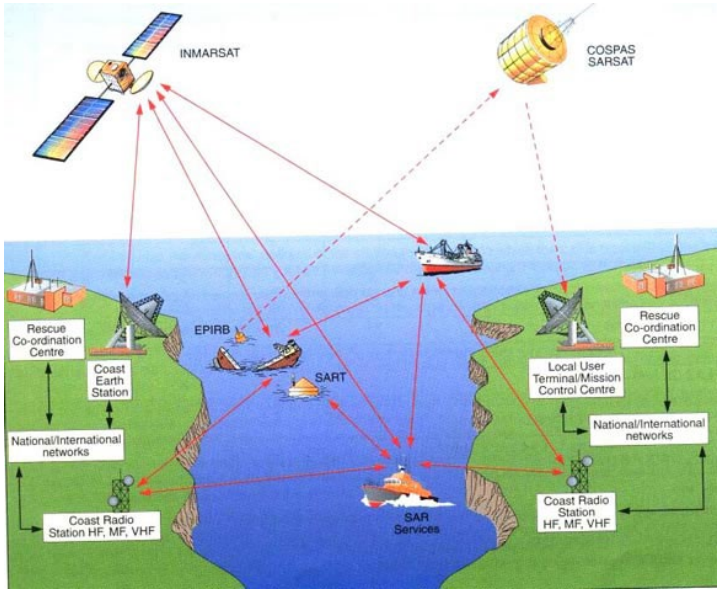

Рисунок 1.1.2 Наглядная схема системы ГМССБ

Таким образом, исторический путь развития систем идентификации в судоходстве демонстрирует поэтапный переход от субъективных и визуальных методов к объективным, стандартизированным, а затем и автоматизированным цифровым протоколам. Каждое последующее поколение средств идентификации отвечало на вызовы своего времени, связанные с ростом числа судов, усложнением навигационных маршрутов, появлением новых угроз — как природных, так и техногенных, а в последние десятилетия — и киберугроз. Сегодня идентификация судов является не просто вспомогательной процедурой, но необходимым компонентом комплексной системы морской безопасности и управления трафиком, без которой невозможно функционирование современных судоходных маршрутов, включая такие труднодоступные и стратегически важные зоны, как Северный морской путь.

1.2 Понятие идентификации и аутентификации в информационных системах корабельной связи

В условиях растущей цифровизации судоходства и широкого распространения дистанционных технологий управления морскими объектами особое значение приобретает корректное понимание процессов идентификации и аутентификации в рамках информационных систем

корабельной связи. Эти понятия, будучи тесно связанными между собой, представляют собой самостоятельные логико-функциональные компоненты общей архитектуры обеспечения доверенности, защищённости и управляемости морских коммуникационных сетей.

Идентификация, в общем смысле, представляет собой процедуру установления уникальности объекта в информационной системе. В контексте судоходства и, в частности, корабельной связи, под идентификацией подразумевается процесс получения и интерпретации формализованных сведений о морском объекте, позволяющих однозначно установить его принадлежность, статус и права на участие в радиообмене или навигационном взаимодействии.[5] К числу таких сведений относятся радиопозывные, международный номер IMO, идентификатор MMSI, наименование судна, флаг, порт приписки, а также разнообразные технические метаданные, присваиваемые судну в процессе его регистрации в международных или национальных реестрах.

Номер ИМО состоит из трёхбуквенной латинской аббревиатуры «IMO», за которой следует число из семи цифр. Первые шесть из них являются уникальным порядковым номером судна, а седьмая цифра — контрольная. Целостность номера ИМО может быть проверена по его контрольной цифре. Это производится путём умножения каждой из первых шести цифр на множитель от 2 до 7, соответствующий их позиции считая справа налево. Полученные числа суммируются и последняя цифра суммы должна совпадать с контрольной цифрой. Например, для IMO 9311622 (танкер «Владимир Тихонов»): (9×7) + (3×6) + (1×5) + (1×4) + (6×3) + (2×2) = 112 — выделенная цифра 2 совпадает с последней цифрой в номере, следовательно, он — целостный.

Рисунок 1.2.1 ИМО-номер судна

При этом важно подчеркнуть, что идентификация всегда опирается на некий внешний источник доверия — базу данных, реестр или централизованную систему сертификации, к которой производится обращение для подтверждения корректности полученных идентификационных данных. Современные автоматизированные средства судовой связи позволяют осуществлять подобные запросы в реальном времени или в полуавтоматическом режиме, что, с одной стороны, ускоряет процесс установления связи, но с другой — увеличивает уязвимость системы к подделке идентификационных параметров.

Аутентификация является логическим продолжением и дополнением процесса идентификации, направленным не только на установление факта, кто или что участвует в сеансе связи, но и на подтверждение того, что данный участник действительно обладает правами, соответствующими заявленному идентификатору. Если идентификация отвечает на вопрос "кто это?", то аутентификация определяет "насколько мы можем быть уверены, что это именно он?". В условиях корабельной связи, особенно в системах дистанционного управления и навигации, аутентификация критически важна, поскольку подмена источника сигнала или попытка внедрения ложной информации может привести к дестабилизации навигационной обстановки, угрозе столкновения или искажения данных о положении судов. [1]

Методы аутентификации могут быть разнообразны. В классическом подходе они делятся на симметричные и асимметричные криптографические методы, а также на многофакторные схемы, включающие в себя подтверждение по нескольким каналам или признакам. На практике информационных системах чаще всего применяются аутентификация с помощью цифровых сертификатов (PKI), шифрование с использованием SSL/TLS (в том числе с выполнением процедуры handshake), проверка по времени и физическим характеристикам передачи (например, анализ времени задержки сигнала в реальном канале). Однако применение многих из этих методов в условиях ограниченных каналов связи, например, в КВ-диапазоне или при работе через спутниковые ретрансляторы в условиях Севморпути, может быть затруднено из-за громоздкости пакетов, временных задержек и дороговизны трафика. [2]

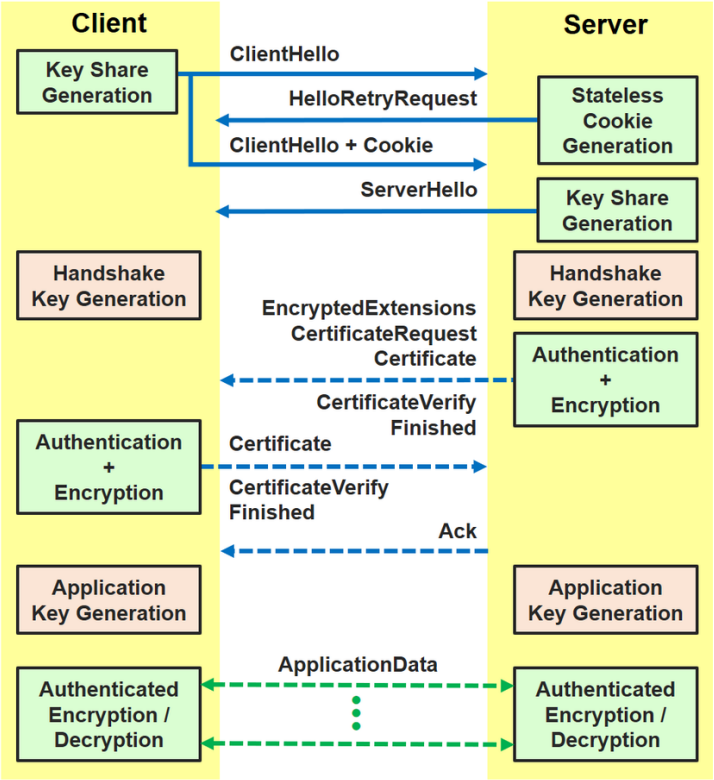

Рисунок 1.2.2. Формат "рукопожатия" DTLS 1.3

Таким образом, в современных автоматизированных корабельных системах идентификация и аутентификация выступают как взаимодополняющие процессы, обеспечивающие целостность, подлинность и

достоверность коммуникационных взаимодействий между морскими объектами и береговой инфраструктурой. Они образуют фундамент доверенной среды связи и являются обязательными элементами в архитектуре таких протоколов, как ГМССБ, АИС, LRIT, а также в интегрированных судовых платформах, осуществляющих управление движением, телеметрию и дистанционную диагностику технических систем судна.

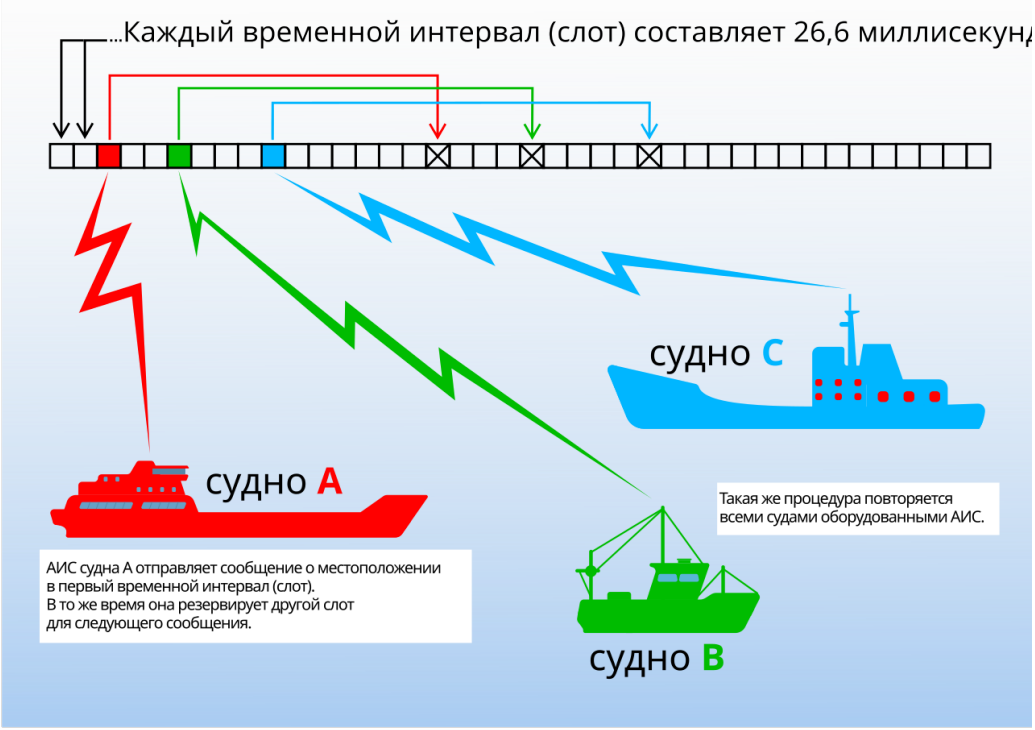

Рисунок 1.2.3 Принцип обмена информацией в АИС

Применение систем идентификации и аутентификации особенно актуально в рамках концепции дистанционной автоматизации судоходства, где прямое вмешательство человека сведено к минимуму, а роль цифровой среды как посредника возрастает в разы. Отсутствие достоверных механизмов установления личности источника данных в такой архитектуре может привести к потере управляемости судном, компрометации навигационной безопасности и, как следствие, к техногенным авариям. Именно по этой причине вопросы построения эффективной, устойчивой к внешним воздействиям, но при этом лёгкой по ресурсоёмкости системы идентификации и аутентификации выходят на передний план при проектировании

современных протоколов корабельной связи, особенно в специфических условиях работы на Севморпути.

1.3 Роль идентификации и аутентификации в дистанционной автоматизации корабельной связи

Современная морская отрасль всё более уверенно движется в направлении цифровизации и автоматизации управления, что особенно заметно в сфере корабельной связи. Разработка и внедрение дистанционных систем автоматизации судоходства обусловлены необходимостью повышения безопасности, надёжности и эффективности взаимодействия между судами, а также между судами и береговыми службами. В этом контексте особое значение приобретают механизмы идентификации и аутентификации, выступающие фундаментом доверенной цифровой среды, на которой базируется вся инфраструктура обмена данными.

Переход от традиционного радиосвязного взаимодействия к автоматизированным протоколам требует строгого контроля за тем, кто инициирует передачу информации, в какой форме и с какой степенью достоверности. В условиях, когда ключевые процессы связи становятся программно управляемыми, без участия человека в режиме реального времени, наличие формальных идентификаторов и механизмов проверки подлинности источника информации становится обязательным элементом архитектуры систем связи.

В частности, в системах дистанционного мониторинга, навигации и управления судном, передача управляющих или телеметрических данных требует подтверждения не только целостности передаваемой информации, но и её происхождения. Невозможность проверить, что сообщение поступило именно от доверенного отправителя, делает систему уязвимой к атакам типа spoofing (имитация подлинного источника) или injection (внедрение ложных данных). Примером таких рисков может быть подмена АИС-идентификатора судна в автоматической системе идентификации, что может привести к

созданию ложной навигационной обстановки, а в ряде случаев — к прямым авариям или нарушению морского права.[9]

Кроме того, автоматизация протоколов связи нередко реализуется в условиях ограниченных радио ресурсов, таких как коротковолновая (КВ) или ультракоротковолновая (УКВ) радиосвязь, а также дорогостоящие спутниковые каналы. В таких условиях особенно критично обеспечить эффективность протоколов, минимизировав объём передаваемой информации при сохранении всех требований к идентификации и аутентификации. Это требует разработки специализированных протоколов, адаптированных к низкоскоростным каналам и нестабильным условиям распространения радиоволн. Отказ от таких механизмов в пользу простоты передачи данных недопустим, поскольку ставит под угрозу базовую информационную безопасность судна.

Следует отметить, что в рамках Глобальной морской системы связи при бедствии (ГМССБ) и других международных инициатив ИМО и ИТУ, идентификация судна при передаче экстренных сообщений и в автоматических системах взаимодействия (например, при обмене координатами или подтверждении получения сигнала) должна происходить автоматически и однозначно. В случае отсутствия надёжных механизмов подтверждения источника сообщения может возникнуть ситуация ложной тревоги или, напротив, игнорирования реального сигнала бедствия. Таким образом, внедрение эффективных систем аутентификации позволяет не только защищать каналы связи от внешнего вмешательства, но и обеспечивать доверие к информации, полученной в рамках автоматизированных процедур, что критически важно в условиях экстремальных или нестабильных ситуаций, часто возникающих в приполярных широтах.

Идентификация и аутентификация также играют важнейшую роль в системах управления движением судов (Vessel Traffic Services, VTS), в которых обмен данными между судами и диспетчерскими центрами осуществляется по цифровым протоколам. Наличие надёжного

идентификатора позволяет диспетчеру точно сопоставить технические параметры судна с его фактическим положением и состоянием, а также принять оперативные меры в случае отклонения от маршрута или возникновения инцидента. Аутентификация в этом контексте необходима для исключения возможности дезинформации или компрометации данных, поступающих от судов, особенно в условиях высокой плотности движения.

Кроме прямых аспектов обеспечения безопасности, роль идентификации и аутентификации распространяется и на организационно-правовую плоскость. Надёжное установление принадлежности и подлинности переданных данных даёт возможность вести архивный учёт всех сеансов связи, составлять отчётность, устанавливать ответственность за принятые решения, а также проводить последующий анализ инцидентов. Это особенно важно в условиях роста автоматизации, когда решение о маневре или переходе через сложный участок маршрута может быть принято в автоматическом режиме, без участия человека.

Таким образом, идентификация и аутентификация в системах дистанционной автоматизации корабельной связи выступают как системообразующие категории, определяющие уровень защищённости, достоверности и юридической силы информационного взаимодействия между участниками судоходного процесса. Без их надлежащей реализации дальнейшее развитие морской автономной навигации, в том числе в труднодоступных регионах, таких как Северный морской путь, остаётся невозможным или сопряжённым с чрезмерно высоким уровнем риска.

1.4 Особенности судоходной радиосреды в условиях Арктики и Севморпути (КВ, УКВ, спутник)

Функционирование систем связи в высокоширотных морских районах, таких как Арктика и акватория Северного морского пути (СМП), характеризуется специфическими физико-географическими и радиотехническими условиями, которые существенно влияют на

эффективность и устойчивость обмена информацией между судами, а также между судами и береговой инфраструктурой. Эти особенности необходимо учитывать при разработке и внедрении систем дистанционной автоматизации, включая процедуры идентификации и аутентификации, поскольку стабильность канала связи в арктических широтах напрямую определяет, как безопасность судоходства, так и работоспособность распределённых информационных комплексов.

В первую очередь необходимо отметить, что Арктика представляет собой регион с крайне неблагоприятными условиями для распространения радиоволн, особенно в коротковолновом (КВ) и ультракоротковолновом (УКВ) диапазонах. Высокая ионосферная активность, частые магнитные бури и резкие изменения солнечной радиации вызывают нестабильность отражающих слоёв атмосферы, от которых зависит прохождение КВ-сигнала. Это приводит к значительным временным задержкам, затуханию сигнала, стохастическим помехам и эффекту "радиотени", когда радиосигнал оказывается частично или полностью недоступен на определённых участках маршрута.

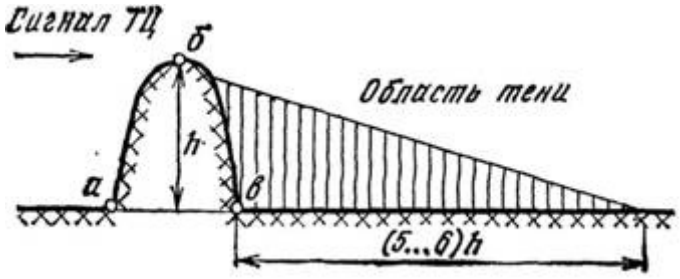

Рисунок 1.4.1 Область "радиотени", где сигнал недоступен

Коротковолновая радиосвязь (КВ), традиционно используемая для обеспечения дальнего радиопокрытия в условиях отсутствия ретрансляторов, имеет как преимущества, так и значительные ограничения в арктических условиях. С одной стороны, благодаря ионосферным отражениям она позволяет охватывать большие расстояния при малом энергопотреблении. С другой стороны, нестабильность этих отражений в приполярных регионах делает КВ-связь крайне непредсказуемой, особенно в периоды солнечной

активности. Кроме того, КВ-связь ограничена по полосе пропускания, что делает передачу объёмных пакетов данных, характерных для современных криптографических протоколов аутентификации, крайне затруднённой или невозможной без адаптации. [5]

Влияние слоёв ионосферы на распространение радиоволн в КВ-диапазоне:

Слой F2 — самый верхний из ионизированных слоёв ионосферы. Концентрация этого слоя повышается днем, летом она выше, чем зимой. Максимальное распространение для связи одним скачком до 4000 км. Чем выше концентрация слоя, тем более высокая частота может ещё отразиться от ионосферы.

Слой F1 — существует только днем. Максимальное распространение для связи одним скачком до 3000 км. Ночью сливается со слоем F2.

Слой E — отражающий слой, наименее подвержен солнечной активности. Максимальное распространение для связи одним скачком до 2000 км. МПЧ зависит только от угла отражения.

Слой Es — слой E спорадический. Возникает спорадически (изредка), чаще в экваториальных широтах. Характеристики как у слоя E.

Слой D — самый нижний из ионизированных слоёв ионосферы и единственный поглощающий слой для радиоволн КВ диапазона. Существует только днем. Ночью исчезает. При исчезновении слоя D ночью, становится возможен прием слабых и далеко расположенных радиостанций.

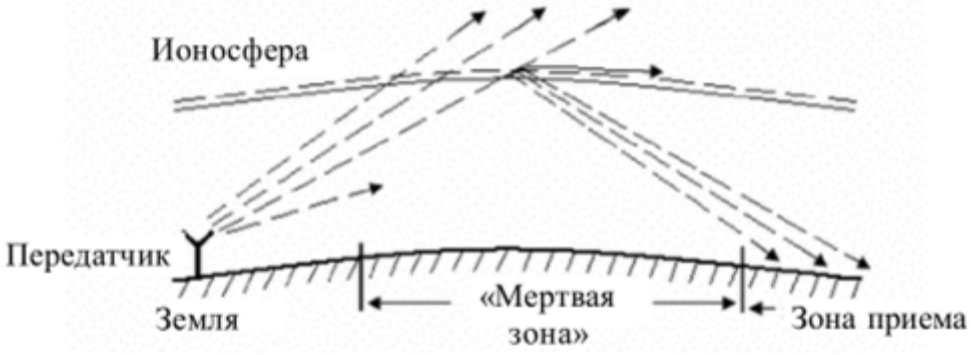

Рисунок 1.4.2 Пространственное распространение КЕ-волн

Ультракоротковолновая связь (УКВ), в свою очередь, обеспечивает надёжное и устойчивое соединение на малых расстояниях — до 30–40 километров при прямой видимости. В условиях Арктики, где значительная часть маршрута пролегает через необжитые и неоснащённые береговыми станциями регионы, УКВ-связь оказывается эффективной лишь при непосредственной близости судов друг к другу. Кроме того, рельеф береговой линии, ледовая обстановка и наличие преград (включая ледовые поля и айсберги) могут вызывать отражения, переотражения и искажения сигнала, особенно при низкой высоте антенн. Это делает УКВ малопригодным для реализации полноценной системы автоматического радиоконтроля судов на всём протяжении маршрута. [5]

Рисунок 1.4.3 Распространение УКВ волн в зоне “Прямой видимости”

Спутниковая связь, на первый взгляд, представляет собой наиболее универсальное решение для арктических регионов. Современные спутниковые системы связи, включая такие стандарты как Inmarsat, Iridium и Starlink, обеспечивают высокую пропускную способность, надёжность и глобальное покрытие. Однако даже эти системы имеют свои ограничения при работе в высоких широтах. Во-первых, большинство геостационарных спутников (включая Inmarsat) имеют низкую эффективность в районах за пределами 75-й параллели северной широты, из-за малых углов возвышения

сигнала и частых блокировок линии визирования. Во-вторых, системы со сплошным покрытием (например, Iridium) обеспечивают связь через низкоорбитальные спутники, но требуют частой перенастройки каналов и используют платную инфраструктуру, что делает постоянное соединение экономически затратным, особенно для коммерческих операторов.

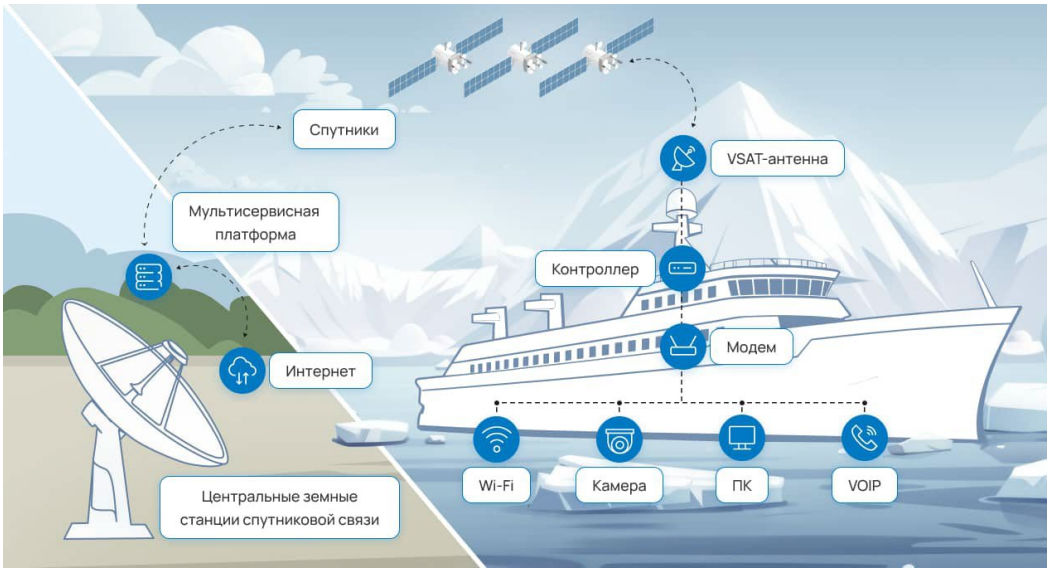

Рисунок 1.4.4 Оснащение спутниковой корабельной связи

Дополнительно стоит учитывать особенности электромагнитной обстановки в Арктике, включая высокую плотность естественных помех (шумы от полярного сияния, грозовой активности, магнитосферных выбросов), что требует от судовых радиокомплексов высокого уровня селективности и помехозащищённости. Такие помехи особенно критичны при передаче низкоуровневых идентификационных или управляющих сигналов, которые могут быть полностью поглощены радиофоном, не вызвав срабатывания ни у судовой, ни у береговой аппаратуры. Это создает угрозу "молчаливой потери" данных — ситуации, когда передача формально состоялась, но ни одна из сторон её не интерпретировала корректно.

Существуют и организационно-правовые особенности, ограничивающие использование определённых диапазонов и технологий в арктическом регионе. Так, не все страны допускают использование шифрования на определённых частотах, особенно в международных водах.

Это может повлечь необходимость компромиссов между степенью защищённости и правомерностью используемого протокола, особенно в вопросах аутентификации, где защита данных является приоритетом.

В совокупности перечисленные факторы обуславливают необходимость создания специализированных, адаптивных протоколов идентификации и аутентификации, способных функционировать в условиях высокой нестабильности радиосреды, ограниченного объёма трафика и частичной недоступности глобальных сетей. Такие протоколы должны быть лёгкими по структуре, устойчивыми к частичной потере данных, способными к повторной синхронизации и перезапросу критической информации, а также удовлетворяющими требованиям энергетической и вычислительной эффективности.

Таким образом, особенности радиосреды Арктики и Севморпути формируют специфические требования к проектированию и эксплуатации систем корабельной связи, в частности — к подсистемам идентификации и аутентификации. Игнорирование этих факторов способно привести к полной деградации связной инфраструктуры, потере контроля за судоходством и невозможности реализации даже базовых функций дистанционного управления морскими объектами в одном из наиболее стратегически важных регионов мира.

1.5 Сравнительный анализ существующих решений: возможности и ограничения

На современном этапе развития судовой связи и автоматизации процессов управления морскими объектами на глобальном уровне используется множество решений в области идентификации и аутентификации. Эти решения варьируются от базовых методов передачи идентификаторов (например, MMSI) до комплексных криптографических протоколов с многофакторной верификацией. Однако в контексте применения таких систем в условиях ограниченной пропускной способности каналов (КВ,

УКВ, арктические спутниковые сети), а также с учётом требований к надёжности и энергоэффективности, становится очевидным, что универсального и одновременно адаптивного решения пока не существует. Следовательно, необходим критический обзор имеющихся подходов, их возможностей и характерных ограничений, особенно в применении к условиям дистанционной автоматизации корабельной связи.

Автоматическая система идентификации (АИС) является одной из наиболее распространённых систем, обеспечивающих базовую идентификацию судов в режиме реального времени. Она обеспечивает широкое покрытие и интегрирована с большинством навигационных комплексов. В основе АИС лежит передача идентификаторов MMSI, названия судна, его координат, скорости, курса и других параметров навигации.

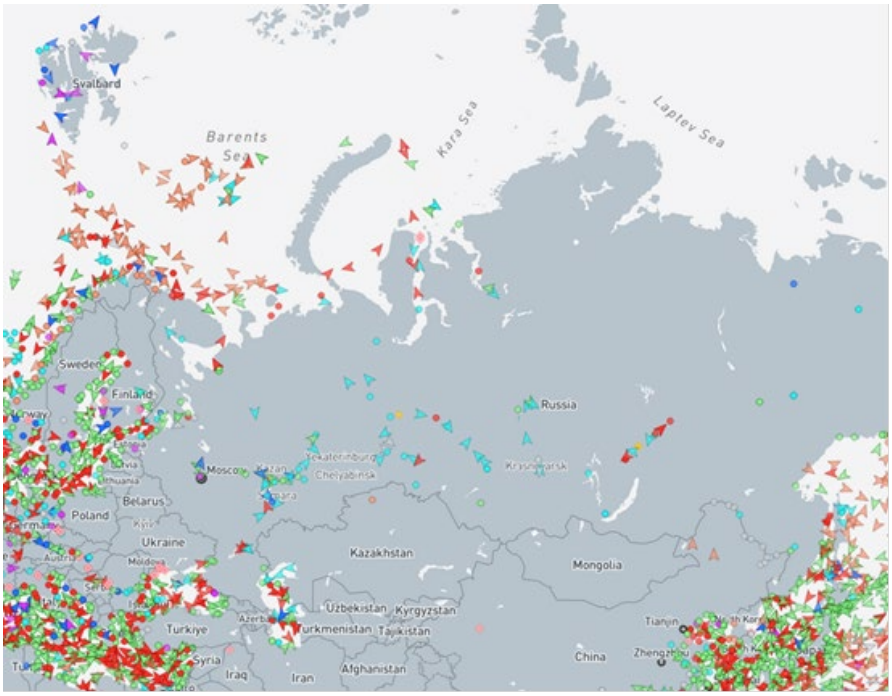

Рисунок 1.5.1 Карта судовой обстановки, полученная системой АИС[17]

Оборудование АИС работает в УКВ-диапазоне, что означает зону охвата порядка 30 морских миль. В этом радиусе суда могут обмениваться информацией, выстраивая на судовых дисплеях полноценную картину навигационной обстановки заданного района.

Глобальная навигационная спутниковая система обеспечивает оборудование АИС необходимыми данными. Также синхронизирует работу всех систем, находящихся в заданном районе. Работе оборудования АИС свойственна жесткая синхронизация по времени. Глобальная морская система связи при бедствии (ГМССБ), в свою очередь, использует более защищённые каналы для обмена информацией, включая возможность передачи сообщений через спутниковые и КВ-сети. Однако даже в рамках ГМССБ идентификация осуществляется преимущественно на основании MMSI и радиопозывных, без системной привязки к инфраструктурам аутентификации. Хотя некоторые спутниковые провайдеры (например, Inmarsat) допускают использование зашифрованных каналов связи, общая архитектура системы остаётся уязвимой, поскольку большинство коммерческих судов эксплуатируют базовые конфигурации терминалов связи без поддержки криптографических протоколов. Кроме того, в условиях ограниченного трафика передача больших объёмов данных (например, цифровых сертификатов) становится непрактичной, что существенно ограничивает реализацию полноценной аутентификации.

Рассматривая классические протоколы аутентификации, такие как TLS, DTLS, IPsec, можно отметить их широкую распространённость в телекоммуникациях и высокую степень криптографической стойкости. Однако прямая их имплементация в судовых радиоканалах вызывает ряд затруднений. Во-первых, TLS и его производные протоколы требуют предварительного обмена ключами, верификации сертификатов и выполнения «рукопожатий», в ходе которых осуществляется согласование алгоритмов, шифров и сессий. Все эти операции требуют передачи значительного количества вспомогательной информации. В условиях КВ-диапазона, где скорость передачи составляет единицы или десятки килобит в секунду, такое взаимодействие становится чрезмерно ресурсоёмким и подверженным сбоям. Во-вторых, устойчивость таких протоколов к потере пакетов невысока: в

нестабильной среде передача может обрываться на любом этапе, приводя к невозможности установления защищённого соединения. [6]

Наконец, необходимо упомянуть об отраслевых решениях, разработанных для специфических условий эксплуатации, включая системы радиолокационного слежения с элементами цифровой подписи, протоколы аутентификации в системах контроля над рыболовными судами и технологию e-navigation. Хотя некоторые из этих систем обладают высокой степенью надёжности, их внедрение требует значительных капитальных вложений, изменения архитектуры судового оборудования и пересмотра юридической базы. Это ограничивает возможность их повсеместного применения, особенно для коммерческого или гражданского флота, эксплуатирующего устаревшую или частично модернизированную технику.

Таким образом, существующие решения по идентификации и аутентификации в судовой связи демонстрируют широкий спектр возможностей, но одновременно страдают от ограничений, связанных с объёмом передаваемых данных, отсутствием встроенной криптографической стойкости, слабой адаптацией к нестабильной радиосреде и высокой стоимостью модернизации. Это указывает на необходимость разработки специализированных, облегчённых по структуре и адаптивных к арктическим условиям протоколов, которые смогут обеспечить базовые функции идентификации и аутентификации без перегрузки канала связи и оборудования. Именно к такому направлению и следует обратиться при проектировании протоколов для дистанционной автоматизации судоходства в условиях Северного морского пути.

Глава 2. Технические и организационные аспекты построения системы идентификации и аутентификации

2.1 Требования к системам аутентификации при низкоскоростной связи

Реализация механизмов аутентификации в условиях низкоскоростных радиоканалов связи, таких как коротковолновая (КВ) или узкополосная спутниковая связь, требует строгого учёта физико-технических ограничений. Основной проблемой в таких условиях становится нехватка пропускной способности, высокая вероятность потери пакетов, ограниченное энергопитание судовых терминалов и нестабильная ионосферная обстановка. В связи с этим к системам аутентификации предъявляются не только криптографические, но и телекоммуникационные требования.

Во-первых, аутентификация должна быть «облегчённой» по трафику. Современные протоколы TLS/SSL требуют передачи порядка 3–7 КБ данных только для установки защищённой сессии (обмен ключами, сертификатами и служебными заголовками). [6] При типичной скорости КВ-связи ~300–1200 бит/с передача такого объёма займёт от нескольких десятков секунд до нескольких минут. Это неприемлемо для большинства применений в реальном времени. Следовательно, механизм аутентификации должен помещаться в объём не более 256-512 байт на сессию, причём с возможностью фрагментации.

Во-вторых, протокол должен быть устойчивым к потере пакетов и предусматривать автоматическую повторную синхронизацию. Это означает отказ от длинных handshake-сессий и предпочтение одношаговым или псевдоасинхронным протоколам. Примером может служить механизм HMAC, в котором передаётся короткое сообщение и его контрольная сумма, сформированная по заранее согласованному ключу. При этом сам ключ не передаётся, что экономит трафик и повышает стойкость. [20]

HMAC (hash-based message authentication code*)*, код аутентификации (проверки подлинности) сообщений, использующий хеш-функции, или код аутентификации сообщений, использующий хеш-функции с ключом — в информатике (криптографии), один из механизмов проверки целостности информации, позволяющий гарантировать то, что данные, передаваемые или хранящиеся в ненадёжной среде, не были изменены посторонними лицами. Механизм HMAC использует имитовставку (MAC), описан в RFC 2104, в стандартах организаций ANSI, IEF, ISO и NIST. MAC — стандарт, описывающий способ обмена данными и способ проверки целостности передаваемых данных с использованием секретного ключа. Два клиента, использующие MAC, как правило, используют общий секретный ключ. HMAC — надстройка над MAC; механизм обмена данными с использованием секретного ключа (как в MAC) и хеш-функций. В названии может уточняться используемая хеш-функция: HMAC-MD5, HMAC-SHA1, HMAC-RIPEMD128, HMAC-SHA256.

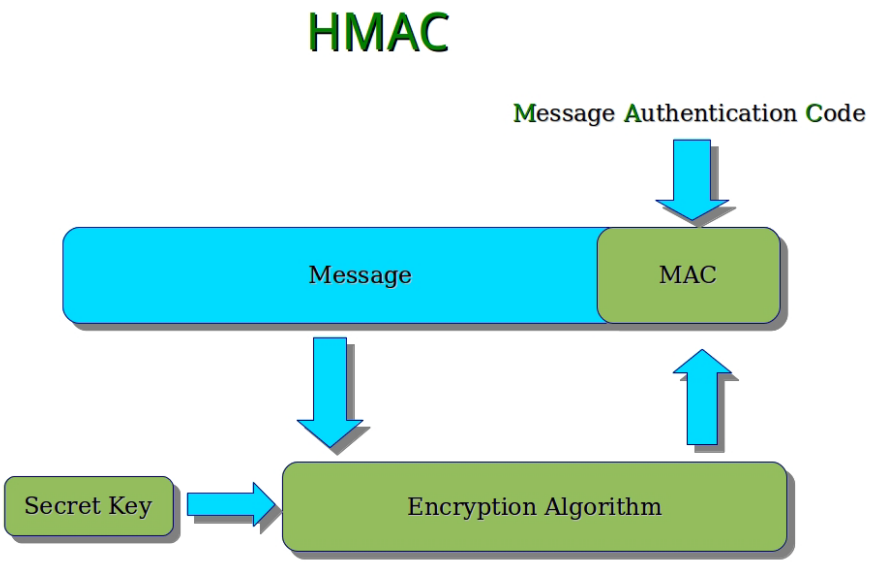

Рисунок 2.1.1 Блок-схема работы механизма HMAC

В-третьих, протокол должен быть независим от инфраструктуры публичных ключей (PKI). Сертификация через X.509 или OCSP (Online Certificate Status Protocol) требует регулярного доступа к внешним серверам доверия [13], что невозможно обеспечить при работе через КВ-связь или при периодических спутниковых сеансах. Вместо этого предпочтение следует отдавать предварительно согласованным статическим ключам, привязанным к MMSI или другому идентификатору судна.

В-четвёртых, необходимо учитывать ограничения вычислительных ресурсов на борту, особенно при использовании встроенных микроконтроллеров и DSP-модемов в системах связи. Ресурсоёмкие схемы RSA, DSA, особенно с длинами ключей более 2048 бит, создают чрезмерную нагрузку. Оптимальным решением в таких условиях являются легковесные алгоритмы, такие как:

- HMAC-SHA1 или HMAC-SHA256 с предварительно согласованным ключом;
- SipHash — хеш-функция для коротких сообщений;
- ChaCha20-Poly1305 — быстрая симметричная схема шифрования с верификацией.

В-пятых, протокол должен быть встроен в транспортный уровень без дублирования функций, уже обеспеченных самим протоколом (например, TCP). Проверка целостности данных может быть реализована средствами TCP/IP, тогда как аутентификация — через подпись полезной части сообщения, что минимизирует дублирование и снижает объём передачи.

Для иллюстрации можно привести следующую упрощённую схему обмена:

Передача: Данные + Временная метка + HMAC (ключ, Данные || Временная метка)

Объём:

- Полезная нагрузка — 200-250 байт
- Метка времени — 4 байта

- HMAC — 20 байт (SHA-1)

Итого: ~200-250 байт на один аутентифицированный пакет.

Такой формат позволяет вписаться в стандартный радиоблок КВ-связи,. Метка времени служит защитой от повторных атак, а хеш-сумма — механизмом верификации подлинности.

Таким образом, требования к системам аутентификации в условиях низкоскоростной связи можно свести к пяти основным критериям: минимизация объёма данных, устойчивость к потере пакетов, отказ от внешней инфраструктуры, вычислительная лёгкость и транспортная оптимизация. Эти требования служат базой для проектирования алгоритмов, пригодных к практическому применению в судоходстве, особенно в условиях Арктики и Севморпути, где доступ к широкополосным каналам либо отсутствует, либо экономически нецелесообразен.

2.2 Проблемы безопасности и угрозы при использовании стандартных протоколов (в том числе в КВ-диапазоне)

Использование стандартных протоколов аутентификации (например, TLS 1.2/1.3, IPSec, DTLS) в судовых системах связи, особенно при работе в КВ-диапазоне, сопровождается рядом специфических угроз и технических ограничений, напрямую влияющих на безопасность и целостность коммуникаций.

1. Подмена идентификатора (MMSI).

В КВ-связи данные часто передаются в незашифрованном виде, а идентификаторы судов (например, MMSI) легко перехватываются и подменяются злоумышленником. Это позволяет создавать «фантомные» суда в системе или выдавать одно судно за другое. Стандартные протоколы связи не включают обязательной проверки аутентичности источника, что делает атаку возможной даже при минимальных ресурсах.

2. Replay-атаки.

Из-за высокой нестабильности канала системы передачи данных часто повторяют сообщения. Злоумышленник может захватить сегмент данных, содержащий телеметрию или команду управления, и воспроизвести его позже, вызывая деструктивные сценарии (например, ложный сигнал бедствия или запуск команды управления двигателем). Отсутствие меток времени и подписей делает такие атаки незаметными.

3. Инъекция ложных данных в незашифрованные потоки.

В протоколах типа АИС злоумышленник может внедрить фальсифицированные пакеты без каких-либо последствий, поскольку аутентификация источника и контроль целостности не реализованы либо реализованы лишь на уровне контрольных сумм, которые легко пересчитываются. [21] Особенно опасно это в случаях, когда корабль передаёт управляющие команды или телеметрию в береговую систему автоматического контроля.

4. Атаки отказа в обслуживании (DoS) через перегрузку протокольными сообщениями.

TLS/DTLS требуют многоэтапного обмена данными для установления защищённого канала. В условиях КВ-связи, где передача одного пакета может занимать длительное время, многократные запросы или попытки согласования параметров шифрования приводят к истощению ресурсов приёмного устройства. В результате система блокируется или уходит в режим повторной синхронизации.

5. Отсутствие возможности верификации цепочки доверия.

Протоколы, основанные на PKI (например, TLS), требуют проверки цепочки сертификатов. [2] В судовых условиях, особенно в изоляции (СМП, Арктика), отсутствует физический доступ к онлайн-реестрам и серверам состояния сертификатов. Это делает невозможной проверку актуальности ключа — в результате даже при перехваченной сессии злоумышленник может использовать устаревший, но действительный сертификат.

Таким образом, анализ уязвимостей, связанных с использованием стандартных протоколов аутентификации в условиях нестабильных радиоканалов, позволяет утверждать, что их непосредственная реализация в судовых КВ-сетях без адаптации технически и концептуально нецелесообразна. Высокая вероятность атак подмены, внедрения ложных сообщений, повторной передачи валидных фреймов, а также перегрузки коммуникационного стека требует применения альтернативных схем, построенных по принципу минимализма и устойчивости к сбоям.

Выявленные угрозы напрямую диктуют архитектурные требования к системам аутентификации: низкий объём, отказ от зависимостей от внешних PKI-серверов, встроенные средства защиты от повторных атак и возможность локальной верификации источника. Эти принципы и становятся основой при формировании облегчённого протокола, рассмотрение которого будет представлено в следующих разделах главы.

2.3 Теоретические основы построения лёгкого и устойчивого протокола обмена

Разработка протокола аутентификации и идентификации, пригодного для использования в условиях низкоскоростной, нестабильной и энергоограниченной среды (например, в КВ-диапазоне или при работе в высокоширотных районах Арктики), требует отказа от классических тяжёлых моделей, основанных на инфраструктуре публичных ключей (PKI), и перехода к компактным, автономным схемам обмена. Целью является создание протокола, который одновременно обеспечивает минимальный трафик, стойкость к атакам типа spoofing и replay, а также возможность локальной проверки подлинности сообщения без обращения к внешним доверенным центрам. [7]

В качестве криптографической основы для облегчённой аутентификации логично использовать схему HMAC (Hash-based Message Authentication Code). Она позволяет при наличии заранее известного

симметричного ключа сгенерировать короткую, криптографически стойкую метку целостности для произвольного сообщения. В отличие от RSA или TLS, HMAC и не зависит от третьей стороны.

Типовая структура передаваемого сообщения может включать следующие поля:

- Данные — полезная нагрузка (например, координаты, флаг статуса, команда управления), длиной 160-200 байт;
- Временная метка — 4-байтная метка времени (unix-time или синхронизированное «окно» в пределах 1–5 мин);
- HMAC — 20 байт (для SHA-1) или 32 байта (для SHA-256), вычисляется как HMAC (ключ, данные || временная метка).

Такая структура сообщения позволяет уместить один аутентифицированный пакет в диапазоне 150–300 байт, что соответствует техническим возможностям КВ-модемов и другим узкополосным каналам связи.

Для защиты от повторных атак используется метка времени, сверяемая с допустимым диапазоном. Например, при отклонении на более чем ±180 секунд пакет отбрасывается. Такой механизм не требует строгой синхронизации времени между отправителем и получателем, но обеспечивает базовую защиту при дрейфе часов до ±3 минут.

Передача ключей предполагается однократной при установке соединения или вшитой при регистрации судна. Ключ может быть жёстко связан с MMSI или другим идентификатором (например, Ключ = H(MMSI || Случайное число)), что обеспечивает уникальность и исключает повторное использование.

Наконец, в целях повышения устойчивости к отказам, протокол допускает фрагментацию сообщений по длине (например, по 64 байта с пересборкой на приёмной стороне), а также повторную отправку ключевых пакетов (например, каждые 10 минут дублируется актуальное состояние).

Итоговые свойства проектируемого протокола:

- Объём одного сообщения: 160-200 байт
- Стойкость к подмене и повторным атакам за счёт HMAC и Временной метки
- Независимость от PKI и онлайн-сертификации
- Простота реализации в микроконтроллерах и DSP-модемах
- Совместимость с нестабильными и прерывистыми каналами
- Поддержка фрагментации и повторной передачи без сессий.

В совокупности, перечисленные принципы образуют основу будущей реализации схемы аутентификации, отвечающей требованиям как к надёжности, так и к экономичности в ресурсно-ограниченной морской среде. Конкретная архитектура реализации будет подробно рассмотрена в третьей главе настоящей работы.

2.4 Выбор технологий: TCP/IP, контроль целостности, упрощённая аутентификация

Разработка систем идентификации и аутентификации, предназначенных для функционирования в условиях низкоскоростной и нестабильной связи, требует не только корректного выбора криптографических механизмов, но и обоснованного применения сетевых и транспортных технологий. Наиболее целесообразным подходом в этом контексте представляется адаптация существующих и проверенных технологических стеков, таких как TCP/IP, с соответствующей модификацией их применения для специфических задач судоходной связи. Такой подход позволяет сохранить преемственность с существующими средствами связи, снизить порог внедрения и обеспечить совместимость с различными аппаратными и программными платформами, применяемыми на морских судах.

2.4.1 Модель взаимодействия открытых систем

Сетевая модель OSI (The Open Systems Interconnection model**)** — сетевая модель стека (магазина) сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с

другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO). Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашёл отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF).

2.4.2 Транспортный уровень

Протокол TCP, входящий в базовую архитектуру модели взаимодействия открытых систем, несмотря на его широкое распространение в условиях устойчивых каналов (например, в проводных и беспроводных сетях общего назначения), представляет интерес и для задач судоходной радиосвязи. Его архитектура предполагает наличие встроенного механизма контроля целостности данных, обеспечиваемого за счёт контрольной суммы, вычисляемой для каждого TCP-сегмента. Эта особенность делает возможным использование TCP не только в качестве транспортного слоя, но и как средства базового обеспечения надёжности передачи данных в условиях, когда канальный уровень не гарантирует достоверности связи. [8]

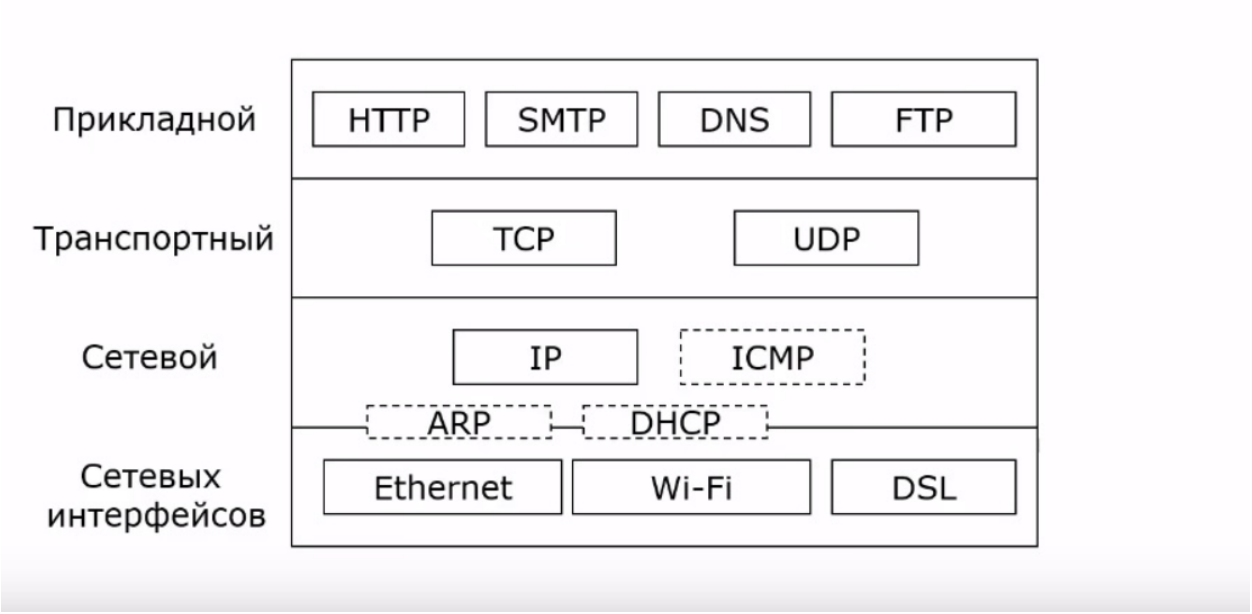

Рисунок 2.4.1. Модель протокола TCP/IP

2.4.2.1 Заголовок сегмента TCP

- Порт источника, Порт назначения

Порт источника идентифицирует приложение клиента, с которого отправлены пакеты. Ответные данные передаются клиенту на основании этого номера. Порт назначения идентифицирует порт, на который отправлен пакет.

- Порядковый номер

Порядковый номер - измеряется в байтах, и каждый переданный байт полезных данных увеличивает это значение на 1. Если установлен флаг SYN (идёт установление сессии), то поле содержит изначальный порядковый номер — ISN (Initial Sequence Number). В целях безопасности это значение генерируется случайным образом и может быть равно от 0 до 232−1 (4294967295). Первый байт полезных данных в устанавливающейся сессии будет иметь номер ISN+1.

- Номер подтверждения(ACK SN)

Если установлен флаг ACK, то это поле содержит порядковый номер октета, который отправитель данного сегмента желает получить. Это означает, что все

предыдущие октеты (с номерами от ISN+1 до ACK-1 включительно) были успешно получены.

- Длина заголовка (смещение данных)

Длина заголовка (Data offset) занимает 4 бита и указывает значение длины заголовка, измеренное в 32-битовых словах. Минимальный размер составляет 20 байт (пять 32-битовых слов), а максимальный — 60 байт (пятнадцать 32-битовых слов). Длина заголовка определяет смещение полезных данных относительно начала сегмента.

- Зарезервировано

Зарезервировано (3 бита) для будущего использования и должно устанавливаться в ноль.

- Флаги (управляющие биты)

Это поле содержит 9 битовых флагов:

NS (ECN-nonce) — Устойчивый механизм сигнализации насыщения с помощью ECN-nonce;

CWR (Congestion Window Reduced) — Поле «Окно перегрузки уменьшено» — флаг установлен отправителем, чтобы указать, что получен пакет с установленным флагом ECE;

ECE (ECN-Echo) — Поле «Эхо ECN» — указывает, что данный узел способен на ECN (явное уведомление перегрузки) и для указания отправителю о перегрузках в сети. URG — поле *«Указатель важности»* задействовано. Когда узел отправляет сегмент с URG флагом, то узел-получатель принимает его на отдельном канале. ACK — поле *«Номер подтверждения»* задействовано (англ. *Acknowledgement field is significant*)

PSH — (англ. *Push function*) инструктирует получателя протолкнуть данные, накопившиеся в приёмном буфере, в приложение пользователя. Обычно он устанавливается ядром, когда оно очищает буфер. Если узел отправляет сегмент с PSH флагом, это значит, что он отправил все, что было нужно.

RST — оборвать соединения, сбросить буфер (очистка буфера)

SYN — синхронизация номеров последовательности

FIN (англ. *final*, бит) — флаг, будучи установлен, указывает на завершение соединения

- Размер окна

Window Size самостоятельно определяет количество байт данных (payload), после передачи которых отправитель ожидает подтверждения от получателя, что данные получены.

- Контрольная сумма (Checksum)

Поле контрольной суммы — это 16-битное дополнение к сумме всех 16-битных слов заголовка и данных. Если сегмент, по которому вычисляется контрольная сумма, имеет длину не кратную 16-битам, то длина сегмента увеличивается до кратной 16-ти за счёт добавления к нему справа нулевых битов заполнения. Биты заполнения (0) не передаются в сообщении и служат только для расчёта контрольной суммы. При расчёте контрольной суммы значение самого поля контрольной суммы принимается равным 0.

В условиях работы через нестабильные каналы, особенно характерные для КВ-связи, возможность восстановления повреждённых или потерянных сегментов по инициативе приёмной стороны с использованием стандартного механизма подтверждения доставки (ACK) может служить дополнительным уровнем защиты целостности передаваемой информации. Однако важно отметить, что при разработке систем, ориентированных на минимизацию объёма служебных данных, реализация TCP должна быть адаптирована: следует исключить избыточные поля заголовков, отключить нерелевантные опции (например, масштабирование окна или избыточную сегментацию), а также ограничить размеры буферов для обеспечения устойчивой работы при высоких задержках и нестабильной пропускной способности.

Помимо встроенного контроля целостности, архитектура TCP/IP позволяет интеграцию пользовательских механизмов проверки данных, в частности — криптографически стойких контрольных сумм, реализуемых средствами, такими как HMAC. В этом контексте транспортный уровень обеспечивает надёжную передачу, в то время как прикладной уровень

отвечает за подлинность и непротиворечивость содержимого сообщения. Разделение этих функций позволяет добиться модульности и отказоустойчивости всей системы, при этом сохраняется гибкость в выборе алгоритмов аутентификации без необходимости вмешательства в базовые сетевые механизмы. [15]

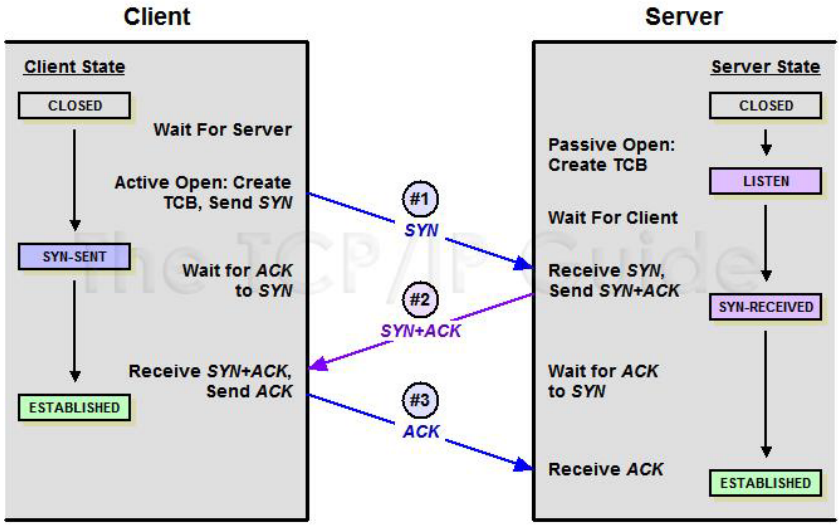

Рисунок 2.4.2 Контроль целостности данных в протоколе TCP

Одним из ключевых требований к предлагаемым схемам аутентификации является их упрощённость как с точки зрения алгоритмической сложности, так и с точки зрения объёма передаваемой информации. В условиях, когда судовые системы связи функционируют на ограниченном энергетическом ресурсе, а радиоканал характеризуется высокой вероятностью потери данных и крайне низкой пропускной способностью, становится необходимым отказаться от сложных процедур согласования (handshake), характерных для протоколов, таких как TLS, и перейти к модели, в которой аутентификация осуществляется односторонне и без установления состояния соединения. Такая модель позволяет свести к минимуму количество обменов между сторонами и исключить необходимость в постоянном взаимодействии для поддержания доверительной сессии.

Важным преимуществом подобной архитектуры является её независимость от внешних инфраструктур доверия. Протоколы на базе PKI, несмотря на высокую степень защищённости, оказываются непригодными в

условиях изоляции судна от глобальных сетей и невозможности обращения к внешним центрам сертификации. В условиях Севморпути и других арктических регионов такая изоляция является не только вероятной, но и систематической. Таким образом, наиболее рациональным решением является использование статически заданных ключей, связанных с уникальными идентификаторами судна и распределяемых при его регистрации. Такая схема обеспечивает автономность и позволяет проводить верификацию полученных сообщений без необходимости обращения к третьим сторонам. [20]

При этом отказ от шифрования как механизма сокрытия информации не противоречит целям аутентификации. В условиях, когда приоритетом является не конфиденциальность, а достоверность и подлинность сообщения, применение открытого текста (plaintext) с HMAC-подписью обеспечивает оптимальный баланс между лёгкостью обработки, прозрачностью протокола и защитой от внешнего вмешательства. Шифрование, как правило, требует значительного вычислительного ресурса, а также сложной процедуры обмена ключами, что делает его применение неоправданным в заданных условиях. Подпись же HMAC, напротив, может быть верифицирована за миллисекунды даже на ограниченных аппаратных ресурсах, обеспечивая при этом защиту от наиболее распространённых угроз, включая подделку сообщений и повторную передачу перехваченного пакета.

Выбор архитектурных и технологических решений для протокола обмена и аутентификации должен базироваться на принципах отказоустойчивости, минимализма, модульности и автономности. Комбинация проверенной сетевой архитектуры TCP, встроенных механизмов контроля целостности, и упрощённой аутентификации на базе HMAC формирует теоретически обоснованную и практически применимую платформу для разработки отказоустойчивых коммуникационных систем, адаптированных к специфике судоходной связи в условиях Северного морского пути и аналогичных арктических маршрутов.

Глава 3. Разработка алгоритма идентификации и аутентификации для корабельной связи в условиях ограниченных ресурсов

3.1 Постановка задачи: ограничения по скорости, надёжности и объёму трафика

Современные системы дистанционной автоматизации судов предъявляют комплексные требования к качеству, безопасности и устойчивости информационного обмена между морскими объектами и инфраструктурой управления. При этом эксплуатация судов в условиях высокоширотных регионов, включая акватории Северного морского пути (СМП), сопряжена с серьёзными ограничениями, напрямую влияющими на эффективность средств связи и реализуемых поверх них протоколов идентификации и аутентификации.

Система, подлежащая разработке в рамках данной работы, должна функционировать в условиях:

- низкой пропускной способности канала: до 300–3600 бит/с для КВ-связи), причём без гарантии устойчивой полосы пропускания в течение длительных периодов;
- жёстких ограничений на объём одного сообщения: включая технические лимиты КВ-модемов (например, 256–512 байт на кадр);
- невозможности постоянного использования PKI-инфраструктуры: из-за отсутствия доступа к центрам сертификации и отсутствия глобального соединения с Интернетом;
- ограничений по вычислительным ресурсам: микроконтроллеры и низкопроизводительные ЦПУ на борту судна не в состоянии выполнять ресурсоёмкие операции, такие как асимметричное шифрование в реальном времени;
- жёстких требований к надёжности и автономности: в силу критичности передачи управляющих, телеметрических и аварийных сообщений.

Сформулированные ограничения обуславливают следующие прикладные требования к разрабатываемому алгоритму идентификации и аутентификации:

- Минимальный объём передаваемых данных — полный цикл аутентификации не должен превышать предельные возможности радиосредств, включая все поля сообщения и контрольные структуры. Это ограничение обусловлено возможностями канала, а также необходимостью обеспечить быструю передачу при первом доступном сеансе.
- Наличие встроенной защиты от подмены и повторных атак — каждое сообщение должно быть привязано к уникальному временному контексту и сопровождаться подтверждением подлинности источника (например, HMAC).
- Использование только симметричных ключей, согласованных заранее — ключи могут быть предварительно встроены в программное обеспечение. Обновление ключей возможно в плановом порядке, вне связи.
- Разделение логики обмена по типам информации — необходимо реализовать различную частоту передачи и приоритетность сообщений: телеметрия должна отправляться чаще, чем управляющие команды, а второстепенные данные — с ещё меньшей частотой. Это позволяет оптимизировать использование канала и избежать перегрузки.
- Контроль целостности и подтверждение доставки (если возможно) — каждая сторона должна иметь возможность определить, была ли передача успешной, либо предпринять повторную отправку. В условиях однонаправленной связи предпочтение отдаётся верификации по контрольной сумме и времени приёма.

На основании изложенных требований можно заключить, что разрабатываемая система должна обеспечивать надёжную, компактную и энергетически экономичную процедуру аутентификации, применимую в судовых условиях, без зависимости от глобальных сетевых инфраструктур и с учётом физико-технической специфики радиосреды Арктики.

3.2 Разработка формата сообщения: структура, контрольная сумма, метки, HMAC

Эффективное функционирование системы аутентификации и идентификации в условиях ограниченной радиосреды предполагает строго регламентированный, минималистичный и при этом функционально завершённый формат передаваемого сообщения. В отличие от стандартных протоколов, применяемых в условиях широкополосной сети, предлагаемая структура должна быть рассчитана на передачу в условиях узкополосного канала, при этом обеспечивая базовые свойства — верифицируемую идентичность отправителя, неизменность данных и защиту от атак повторной передачи.

Формат сообщения должен быть универсальным для всех категорий данных (телеметрия, управление, общая служебная информация), но при этом сохранять возможность логического разделения по типу и назначению. Основной подход — «всё в одном пакете»: вся необходимая информация, включая подтверждение подлинности, должна быть включена в одно сообщение, без необходимости запрашивать дополнительные данные.

3.2.1 Базовая структура сообщения

Таблица 3.2.1.1. Структура сообщения и размер данных

Поле	Размер(в байтах)	Назначение
Тип	1	Телеметрия – 1 Управление – 2 Полезные данные(аудио, видео) -3
Позывной	5	Радиопозывной, присвоенный судну
MMSI	9	Идентификатор судна
Счетчик пакета	4	Определяет порядковый номер передаваемых пакетов данных
Временная метка	4	Метка времени(в Unix-time формате)

Данные	От 100байт до нескольких сотен Мбайт	данные в зависимости от типа(телеметрия, управление, полезная информация)
Контрольная сумма	4	Контрольная сумма, вычисленная на основе значений предыдущих полей.
HMAC	32	Аутентификационный код (на базе симметричного ключа SHA-256)

Общий объём сообщения: до 250 до нескольких мегабайт в зависимости от размера полезной части.

3.2.2 Роль и назначение полей

Поле Тип определяет, как будет обрабатываться сообщение.

Поле Позывной и MMSI обеспечивает логическую привязку к конкретному судну.

Счетчик пакета используется как дополнительная мера против повторов и для упрощения восстановления последовательности сообщений на приёмной стороне. При ограниченных ресурсах его значение сбрасывается каждый день в 00:00.

Временная метка критически важна для предотвращения повторных атак. Верификация выполняется с допуском ±3 минут (в зависимости от конфигурации оборудования и точности часов). Отправитель обязан синхронизировать время хотя бы раз в сутки — например, через спутник или при заходе в порт.

Поле Данные содержит всю прикладную информацию. Её формат может варьироваться, но максимальный размер ограничивается техническими возможностями радиоканала.

CRC32 применяется для быстрой проверки целостности данных ещё до проверки HMAC. Это позволяет сразу отбрасывать искажённые сообщения.

HMAC (например, HMAC-SHA256) рассчитывается по всей информации, включая Тип, Позывной, MMSI, Счетчик пакета, Временная метка и Данные. Использование симметричного ключа, исключает возможность подмены даже при перехвате трафика.

3.2.3 Свойства предложенного формата

1. Минимизация объёма: сообщение в полной форме умещается в ≈ 300 байт, что позволяет передавать его даже в условиях КВ-связи.
2. Универсальность: структура едина для всех типов сообщений и может быть обрабатываема одинаковыми процедурами на приёмной и передающей стороне.
3. Автономность: приёмник, имея ключ и допуск по времени, может проверить подлинность и целостность сообщения локально.
4. Безопасность: комбинация временной метки, счётчика и HMAC обеспечивает защиту от атак подмены, повторов, вставок и искажений.

Таким образом, формализованная структура сообщения отвечает, как эксплуатационным требованиям, так и архитектурным ограничениям судовых радиоканалов. Следующий этап заключается в адаптации логики обмена к реальной структуре данных и моделированию частотной передачи разных категорий сообщений в соответствии с их приоритетом.

3.3 Логика разделения данных по приоритетам: телеметрия, управление, полезная информация

Одной из ключевых задач при построении коммуникационной подсистемы в условиях ограниченного и нестабильного радиоканала является эффективное распределение пропускной способности между различными типами данных. В случае дистанционной автоматизации судов в условиях Арктики и Севморпути целесообразно реализовать систему логического приоритезации сообщений, основанную на функциональной значимости передаваемой информации и критичности её своевременной доставки.

В рамках предлагаемого подхода вся информация, передаваемая в систему, делится на три логических категории:

Телеметрические данные — регулярные, изменяющиеся во времени параметры, фиксирующие техническое состояние судна, включая курс, скорость, положение, температуру систем, состояние электропитания и связи. Эти данные, как правило, не несут критически важной нагрузки в каждый конкретный момент времени, но необходимы для построения полной динамической картины функционирования судна.

Управляющие команды — сообщения, содержащие инструкции, направленные на активацию или деактивацию подсистем, изменение маршрута, восстановление связи или инициализацию аварийного режима. Эти данные являются высокоприоритетными и требуют гарантированной доставки в максимально сжатые сроки.

Полезные данные — передача данных, не имеющих значения в реальном времени, но представляющих интерес для анализа (например, периодические видеокадры, аудиофрагменты, научная или навигационная информация). Эти данные могут передаваться с большой задержкой, при отсутствии спутникового канала.

3.3.1 Принципы организации логики обмена

Каждая категория данных обслуживается в соответствии с заранее установленной политикой интервалов передачи и допустимых задержек. Обмен осуществляется с использованием общего формата сообщения, но со специфическим значением поля Тип, определяющим приоритет обработки и политику хранения на стороне приёмника.

- Телеметрия передаётся каждые 10 минут. Это позволяет обеспечить необходимую детализацию для последующего анализа без перегрузки канала. Объём одного сообщения ограничивается 160-200 байтами данных.
- Управляющие команды передаются по запросу или при изменении состояния. Такие сообщения должны обрабатываться с немедленным

приоритетом. Они могут инициироваться автоматически (например, при обнаружении отклонений) или вручную через центр управления. Повторная передача команды допускается каждые 10 секунд до получения подтверждения или таймаута.

- Полезная нагрузка передаются при необходимости, по возможности — в периоды наименьшей загруженности канала. Такие сообщения могут быть сегментированы и распределены по частям. Передача не требует немедленной обработки и может откладываться без потери критичности.

3.3.2 Алгоритмическая схема обработки

На передающей стороне реализуется планировщик сообщений, формирующий очередь передачи на основе таймеров и приоритетных флагов. Телеметрия ставится в очередь автоматически по таймеру. Управляющие команды, появляясь в буфере, вытесняют менее приоритетные данные. Служебная информация занимает остаточную ёмкость буфера, не влияя на работу остальных компонентов.

На принимающей стороне используется таблица обработки по типу с обязательной верификацией *HMAC* и проверкой допустимого интервала по временной метке. Приёмник имеет право игнорировать устаревшие или повреждённые телеметрические пакеты, но всегда должен обрабатывать команды и подтверждённые служебные фреймы.

Предлагаемая логика обмена основана на допущении, что в условиях нестабильной связи невозможна передача всех типов данных с одинаковой частотой и приоритетом. Попытка равномерного распределения ресурса приведёт к неоптимальному использованию пропускной способности и задержкам в критичных ситуациях. Реализация приоритетов позволяет соблюсти баланс между технической осведомлённостью, реакцией на угрозы и экономией ресурса канала.

Таким образом, разделение данных по типу и реализация соответствующих правил их отправки обеспечивают адаптацию системы обмена к ограниченной и неустойчивой среде. Следующий этап заключается в

моделировании и расчёте фактического времени передачи сообщений с учётом выбранной архитектуры и предполагаемой загруженности канала.

3.3.3 Алгоритм интервалов передачи: оптимизация под реальную пропускную способность

Оптимизация интервалов передачи сообщений является ключевым элементом проектирования эффективной системы обмена данными в условиях ограниченной и нестабильной радиосреды. В случае судоходной связи, особенно в арктических и приполярных регионах, где используются узкополосные каналы (КВ, УКВ, узкополосные спутниковые протоколы), задачей становится обеспечение максимальной пропускной эффективности при сохранении требуемой семантики данных, а также минимизации вероятности потери критически важной информации.

Процесс оптимизации интервалов должен учитывать следующие фундаментальные факторы:

- доступную пропускную способность канала (бит/с), которая может варьироваться от 300 бит/с для КВ-связи до 9600 бит/с в некоторых спутниковых системах;
- размеры сообщений, определённые таблице 3.2.1.1;
- приоритет и критичность каждого типа данных;
- стратегию повторной передачи в случае потерь;
- возможность фрагментации и сборки сообщений (для полезной нагрузки);
- ограничения приёмной стороны по буферизации и обработке.

3.3.3 Введение алгоритма приоритетной очереди

Для адаптации алгоритма под переменные условия, вводится система приоритетной передачи с динамическим подавлением низкоприоритетных сообщений в случае перегрузки. Очередь реализуется как трёхуровневая:

- Уровень 1: управляющие команды - передаются при необходимости.

- Уровень 2: телеметрия - передаётся с фиксированной периодичностью, но может подавляться при обнаружении команды или ухудшении канала.
- Уровень 3: полезная нагрузка — передаётся только при наличии свободного канала и подтверждённой доставки более приоритетных данных.

3.4 Расчёт временных затрат на передачу в КВ-диапазоне

Функционирование протоколов аутентификации и обмена в условиях коротковолновой (КВ) связи предъявляет строгие требования к временным характеристикам передачи сообщений. В связи с этим расчёт фактического времени, необходимого для передачи одного или нескольких пакетов, представляет собой важнейший этап в обосновании практической реализуемости разработанного алгоритма.

КВ-связь, особенно в арктических широтах, характеризуется узкой полосой пропускания, значительными флуктуациями уровня сигнала, непредсказуемой ионосферной рефракцией, а также высокой вероятностью возникновения устойчивых помех и замираний. Для расчётов в настоящей работе принимаются усреднённые параметры для КВ-модемов, работающих по протоколам, на которых построены многие современные системы судовой связи.

3.4.1 Расчёт временных задержек

Формула расчета времени приёма-передачи (1) при использовании TCP протокола в КВ-диапазоне, где tп– подготовка, tс – соединение, to – обработка, tк – потенциальные задержки при передаче.

$$t_{\text{впп}} = t_{\text{п}} + t_{c} + t_{\text{о}} + t_{\text{к}} \quad (1)$$

tп = 2с + 1с + 20с + 180с ≈ 203с ≈ 3 мин 23с – потенциальные задержки при работе протокола TCP в КВ-диапазоне

Время передачи пакета

Базовые параметры расчёта

- Средняя скорость передачи: R = 300 бит/с (устойчивая работа при минимальном уровне сигнала);
- Максимальный размер сообщения телеметрии и управления: 300 байт = 1280 бит (сообщение с ключом аутентификации, телеметрией и временной меткой);
- Средний размер телеметрического сообщения: 160-200 байт = 1600 бит;
- Управляющее сообщение: 100 байт = 800 бит;
- Служебная информация (служебные префиксы, стартовые символы, синхронизация): ~10% от объёма полезных данных;
- Перерывы на подтверждение, контроль частоты, переключение каналов: до 1–2 сек между пакетами.

1. Время передачи одного телеметрического сообщения

- Блок телеметрии: 200 байт = 1600 бит
- Служебные данные: 0,1 х 1600 = 160 бит
- Итого: 1600+160 = 1760 бит

$$t = \frac{1760}{300} \approx 5{,}87 \text{ сек}$$

С учётом возможной паузы и задержками между передачами, общее время одного цикла может достигать до 5 минут.

2. Время передачи управляющего сообщения

- Блок данных управления: 100 байт = 800 бит
- Служебные данные: 0,1 х 800 = 80 бит
- Итого: 800 + 80 = 880 бит

$$t = \frac{880}{300} = 2{,}93 \text{ сек}$$

В случае повторной передачи и задержек затраты возрастают кратно: до 4 минут

3. Время передачи одного сообщения с полезной информацией

- Полный размер: 50 Мбайт = 400 000 000 бит
- Итого: 400 000 000 бит

$$t \text{ нагрузка} = \frac{400\,000\,000}{300} \approx 1\,466\,666{,}67 \text{ сек} \approx 24444 \text{ минут}$$

Передача видео информации по КВ не целесообразна.

Результаты расчёта показывают, что разработанная структура сообщений и алгоритм интервальной передачи позволяют уверенно вписаться в допустимые временные рамки работы судовой КВ-связи даже в условиях ограниченной пропускной способности. Среднее время передачи одного сообщения телеметрии и управления составляет до 5 минут.

3.4.2 Расчёт временных задержек в УКВ-диапазоне

Исходя из преведенной формулы формулы расчёта времени приёма-передачи можно вывести потенциальную задержку в передаче данных в УКВ, по негативным прогнозам, такая задержка, может составлять до одной минуты. Приблизительная пропускная способность УКВ-диапазона равна ≈ 1200 бод

1. Время передачи одного телеметрического сообщения

- Блок телеметрии: 200 байт = 1600 бит
- Служебные данные: 0,1 х 1600 = 160 бит
- Итого: 1600+160 = 1760 бит

$$t = \frac{1760}{1200} \approx 1{,}47 \text{ сек}$$

С учётом возможной паузы и задержками между приёмом-передачей, общее время одного цикла может достигать до 2 минут.

2. Время передачи управляющего сообщения

- Блок данных управления: 100 байт = 800 бит
- Служебные данные: 0,1 х 800 = 80 бит
- Итого: 800 + 80 = 880 бит

$$t = \frac{880}{1200} = 0{,}02 \text{ сек}$$

В случае задержек приёма-передачи затраты возрастают кратно: до 1 минуты

Передача видеофрагментов по УКВ является по-прежнему не целесообразным, поскольку превышает в несколько раз пропускную способность данного диапазона.

3.4.3 Расчёт временных задержек при использовании спутниковых средств связи

Спутниковые средства связи обладают высокой пропускной способностью и в меньшей степени подвержен влиянию атмосферы, и воздействию от электромагнитных полей Земли. Спутники, работающие в Ku-диапазоне, обеспечивают пропускную способность порядка 14Мбит/с, что позволяет передавать телеметрию и команды управления практически без задержек (около 320мс). Использование спутниковых технологий позволяет обмениваться видеофрагментами с бэзэкипажного транспорта.

1. Время передачи видеофрагмента

$$t = \frac{400\,000\,000}{14\,000\,000} = 28 \text{ сек}$$

С учетом возможных задержек в работе протокола TCP, время доставки фрагмента может продлится до минуты.

3.5 Сравнительный анализ с использованием TLS: затраты, эффективность, применимость

В качестве одного из наиболее известных и формально защищённых протоколов аутентификации и шифрования, TLS (Transport Layer Security) представляет собой стандартное решение, широко применяемое в сетевых системах различного назначения — от веб-браузеров до промышленных SCADA-комплексов. [11] Он используется и в некоторых судовых ИТ-решениях, особенно при интеграции с береговыми центрами в условиях наличия устойчивого IP-соединения. Однако попытка применения TLS в условиях низкоскоростной связи, особенно через КВ-каналы, демонстрирует

резкое снижение эффективности и даже полную непригодность протокола для задач удалённой автоматизации судоходства в изолированных регионах.

TLS в своей классической реализации (версии 1.2 или 1.3) требует многошаговой процедуры установления сессии, включающей обмен приветственными сообщениями, передачу цифрового сертификата, генерацию ключей с помощью алгоритмов RSA или ECDHE, а также обмен завершающими служебными пакетами. Объём одного полного "рукопожатия" составляет от 4 до 7 КБ служебной информации, в зависимости от длины сертификатов, настроек безопасности и используемых алгоритмов. При типичной скорости КВ-связи в 300 бит/с передача только этой служебной части занимает до 80–100 секунд, без учёта потерь пакетов, задержек или ошибок канала. Фактическое время может увеличиваться в разы при наличии повторных попыток установления соединения.

Помимо объёма, критическим ограничением TLS является зависимость от инфраструктуры публичных ключей (PKI). Для полноценной верификации сертификатов требуется обращение к онлайн-службам — таким как OCSP или CRL — которые недоступны в условиях автономной навигации и отсутствия глобального соединения. Это делает невозможной актуальную проверку подлинности ключей. Кроме того, применение асимметричных алгоритмов с длиной ключа от 2048 бит создаёт значительную нагрузку на вычислительные ресурсы бортовых микроконтроллеров и радиомодемов, что противоречит принципу энергоэффективности и минимальной аппаратной зависимости.

Предложенная в рамках данной работы облегчённая схема, основанная на использовании HMAC с симметричными ключами обеспечивает одностороннюю верификацию источника сообщения без обращения к сторонним службам. Такая реализация позволяет достоверно передавать и проверять сообщения даже при высокой потере пакетов и прерывистой связи. Более того, весь цикл аутентификации укладывается в несколько минут, что делает его возможным для применения в КВ-диапазоне.

Таким образом, несмотря на признанный уровень защищённости и широкое распространение, протокол TLS не адаптирован для эксплуатации в условиях КВ-связи, характеризующихся низкой пропускной способностью, высокой латентностью и отсутствием инфраструктурной поддержки. Разработанный в настоящей работе протокол, напротив, ориентирован на специфические эксплуатационные ограничения судовой связи в арктических регионах, обладает высокой устойчивостью к внешним сбоям и обеспечивает критически важную функциональность — идентификацию и аутентификацию — при минимальных затратах ресурса. Это подтверждает его превосходство в условиях, где TLS либо неработоспособен, либо неэффективен без радикального упрощения.

3.5.1 Сравнительный анализ с АИС: применимость и ограничения

Автоматическая система идентификации (АИС) является одной из наиболее массово применяемых в судоходстве технологий обмена идентификационной и навигационной информацией между судами и береговыми службами. Её основное назначение — повышение безопасности мореплавания за счёт автоматического вещания координат, курса, скорости и уникального идентификатора судна (MMSI). На первый взгляд, АИС выполняет функцию идентификации, однако с точки зрения требований, предъявляемых к системам надёжной и криптографически защищённой идентификации и аутентификации, система АИС имеет фундаментальные ограничения, делающие её непригодной в условиях высоких требований к верифицируемой безопасности.

С технической точки зрения, АИС работает в УКВ-диапазоне (161.975 и 162.025 МГц), используя TDMA (Time Division Multiple Access). Сообщения передаются с периодичностью от 2 до 10 секунд в зависимости от класса оборудования и скорости судна. Длина стандартного АИС-пакета составляет 168 бит (21 байт), в который включены поля MMSI, текущие координаты, скорость, курс, навигационный статус и дополнительная служебная информация. Обмен осуществляется в режиме открытой трансляции, без

установления сеанса, подтверждений или какой-либо криптографической обработки данных.

Ключевым недостатком АИС в контексте задач аутентификации является полное отсутствие механизма проверки подлинности источника сообщений. Любой приёмник АИС безусловно принимает и отображает данные, исходя только из указанного в сообщении MMSI. В результате становится возможна подмена идентификатора, координат и статуса судна. Этот тип атаки доказан в практических условиях и широко рассматривается как серьёзная угроза морской кибербезопасности. Более того, поскольку АИС не использует ни симметричное, ни асимметричное шифрование, сообщения могут быть легко перехвачены, проанализированы и воспроизведены в другом месте — что создаёт эффект «клонированного» судна.

Кроме уязвимости к подмене и повторным атакам, АИС не обеспечивает адаптивности к условиям радиосреды. В приполярных районах, где УКВ-сигналы затруднены из-за рельефа, ледового покрова и метеоусловий, стабильная работа АИС невозможна без прямой видимости между антеннами. Это делает технологию малопригодной для использования в районах Севморпути, где дистанции между судами и инфраструктурой достигают сотен километров, а береговые станции часто отсутствуют. [15]

Наконец, АИС не предназначен для передачи произвольной полезной информации или управляющих команд. Формат сообщений жёстко стандартизирован, и возможность вставки команд управления отсутствует. Это делает невозможным использование АИС как транспорта для интеграции в автоматизированные системы дистанционного контроля и управления.

В противоположность этому, предложенная в данной работе система аутентификации:

- реализует верифицируемую подлинность источника на основе HMAC с меткой времени;
- устойчива к атаке повторной передачи (replay);

- допускает передачу произвольной полезной нагрузки, включая телеметрию, управление, ;
- адаптирована к нестабильной и низкоскоростной связи, с полной автономностью и без требований к внешним доверенным службам.

Таблица 3.5.1.1 Сравнение разработанного протокола с АИС

Параметр	АИС	Предлагаемое решение
Аутентификация	Отсутствует	Ключ аутентификации, контрольная сумма, временная метка
Устойчивость к подмене	Слабая	Повышенная
Объем данных	Статичен	Гибкий
Передача управляющих команд	Отсутствует	Возможна
Адаптация к слабому каналу	Отсутствует	Реализована

Таким образом, АИС, несмотря на свою значимость в обеспечении общей навигационной информированности, не соответствует требованиям систем аутентификации и идентификации в техническом и криптографическом смысле. Её использование допустимо только как дополнительный источник открытых данных, но не как средство подтверждения подлинности или защищённого обмена. Разработанный в данной работе протокол не заменяет АИС, а восполняет его ключевые недостатки, адаптируясь к условиям, в которых АИС не функционирует или даёт искажённую картину, особенно в удалённых арктических районах.

3.6 Выводы по результатам моделирования, рекомендации и итоги разработки

Проведённое моделирование и сравнительный анализ, основанные на разработанном адаптивном алгоритме идентификации и аутентификации, подтверждают его высокую применимость в условиях судовой связи с ограниченной пропускной способностью, характерной для эксплуатации на Северном морском пути и в арктических широтах. В рамках построенной архитектуры были реализованы принципы компактности, автономности и устойчивости к сбоям, что обеспечивает полное соответствие разработанной схемы специфике эксплуатационной среды.

Моделирование временных затрат при передаче сообщений различных типов (телеметрия, управление, полезная нагрузка) показало, что даже в условиях КВ-канала с пропускной способностью 300 бит/с возможно функционирование системы с общей нагрузкой до 5 минут от доступного эфирного времени. Временные характеристики полной передачи одного сообщения (включая аутентификацию на базе HMAC, временные метки и контрольные суммы) обеспечивает возможность реакции на критичные события.

Разработка единого формата сообщения, ориентированного на 3 категории данных, позволила обеспечить унификацию обмена, при этом сохранив гибкость настройки интервалов и приоритетов. Введённый механизм приоритезации передачи, адаптируемых к текущим характеристикам радиосреды, продемонстрировал высокую устойчивость к нестабильности канала, включая потери сообщений. Повторная передача управляющих сообщений, показала надёжность восстановления даже при ухудшении связи.

Сравнительный анализ с двумя доминирующими в практике подходами — протоколом TLS и системой АИС — наглядно продемонстрировал преимущества предложенного метода. В случае TLS, несмотря на высокий уровень криптографической стойкости, системные и инфраструктурные ограничения делают его фактически неприменимым в условиях КВ-связи,

требующей высокой автономности и компактности сообщений. АИС, в свою очередь, не реализует аутентификацию в принципе, не устойчив к подделке данных и не допускает расширения формата для передачи управляющей или технической информации. Разработанный протокол восполняет эти пробелы за счёт включения HMAC-аутентификации, временных меток, минимального объёма служебных данных.

3.7 Рекомендации по применению

Внедрение разработанного протокола рекомендуется на судах, работающих в условиях Севморпути, Арктики и других изолированных морских регионов, где невозможно обеспечить устойчивое спутниковое соединение или доступ к инфраструктурам PKI. Протокол может быть встроен в системы судовой связи на базе КВ-модемов, совместимых с стандартами шифрования, путём прошивки модуля прикладного уровня.

Использование протокола допустимо как в режиме прямой связи судно–центр, так и в схеме судно–судно, с минимальной необходимостью конфигурации. Ключи могут быть предварительно установлены при регистрации судна, либо обновляться через защищённый канал во время портового обслуживания. Для дальнейшего повышения безопасности возможно введение "одноразовых ключей" или временных окон синхронизации с ограничением по числу попыток верификации.

Однако для получения возможности передавать видео и аудио фрагменты, необходимо увеличение покрытия акватории Северного Морского Пути средствами спутниковой связи с повышенной пропускной способностью.

ЗАКЛЮЧЕНИЕ

В результате исследования, проведенного в рамках данной ВКР были изучены процессы идентификации и аутентификации, их аспекты применимо судоходству и применению безэкипажного водного транспорта в Северных условиях, рассмотрены стандартизированные методы международной идентификации. Также были рассмотрены современные подходы к реализации защищенных каналов связи на основе аутентификационных ключей и контрольных сумм передаваемой информации. Была произведён анализ особенностей радиосреды, которые позволяют наладить бесперебойную коммуникацию, как судно-судно, судно-берег.

Для построения системы были подобраны алгоритмы и протоколы, которые являются основой для построения устойчивых и надёжных систем идентификации и аутентификации. Выбранный стек технологий позволяет настраивать транспортный уровень с поддержкой сохранения целостности информации на основе процедур цифрового “рукопожатия” и проверке контрольных сумм на стороне приёмника(TCP). Использование механизмов обмена данными на использовании секретных ключей(HMAC-SHA256) обеспечивает конфиденциальность данных, даже в тех случаях, когда произошёл перехват пакетов связи.

Для обеспечения постоянной связи с безэкипажных судном были концептуально описаны формат служебных сообщений, которые делятся на три группы: телеметрические данные(номер судна, позывной, его скорость, направление, местоположение и прочие технические данные полученные с установленных датчиков), данные управления(команды движения, стоп движения, изменения курса, включение/выключение установленного в транспорте оборудования), полезные данные(аудио-, видеоданные, которые позволяют произвести наблюдение в экспериментальных целях, или в случае возникновения чрезвычайной ситуации). Форматы были разработаны с учетом пропускных способностей каналов связи для минимизации задержек в данном регионе, поэтому была проведена работа по устранению избыточности

сигнала. Однако для обеспечения бесперебойной передачи данных и увеличения скорости радиообмена, необходимо увеличение покрытия связи спутниковыми средствами связи, которые позволяют производить обмен с повышенной пропускной способностью, это позволит сократить время передачи данных до нескольких сотен миллисекунд, а также позволит передавать видеоинформацию, определенные в блоке полезной информации.

Список литературы

1. Афанасьев А.А.,Веденьев Л.Т.,Воронцов А.А. Теория и практика обеспечения безопасного доступа к информационным системам. – Москва, 2009 – с.40;
2. Иванов В. В., Лубова Е. С., Черкасов Д. Ю. Аутентификация и авторизация // ФГБОУ “МТУ” – Москва: - с.31;
3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях. - Москва : Издательство Юрайт, 2025. — с.42-50.
4. В. В. Никольский, Т. И. Никольская. Электродинамика и распространение радиоволн. — М.: Наука, 1989. — С. 467
5. "Кодекс внутреннего водного транспорта Российской Федерации" от 07.03.2001 №24-ФЗ (ред. от 08.08.2024)
6. Блэк У. Интернет: протоколы безопасности. СПб.: Питер, 2001. – с.120.:
7. Ступницкий М.М., Лучин Д.В. Потенциал КВ-радиосвязи - для создания цифровой экосистемы России // Электросвязь. 2018. №5. С. 49-54.
8. Семенов Ю.А. Протоколы Интернет. Энциклопедия. М.: Горячая линия - Телеком, 2001.
9. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г. М., Сергеев И. В. // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых : сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др.. — М. : ИИУ МГОУ, 2016
10. Андреев Е.Б., Куцевич Н.А., Синенко О.В.
11. Е.Б. Андреев, Н.А. Куцевич, О.В. Синенко SCADA-системы: взгляд изнутри - М.: Издательство «РТСофт», 2004. - 176 с.: ISBN 5-9900271-1-7\

12. IEC 62320-1:2009 Оборудование и системы морской навигации и радиосвязи. Автоматические системы идентификации (АИС).
13. Полянская О.Ю., Горбатов В.С. Инфраструктуры открытых ключей Москва, 2007 – с. 368;
14. Нестеренко А.Ю. О подходе к построению защищенных соединений // Математические вопросы криптографии. 2013. С. 101-111.
15. Стандарт МЭК 61993-2 Часть 2 «Судовое оборудование универсальной автоматической идентификационной системы (АИС) класса А. Технические и эксплуатационные требования, методы и требуемые результаты испытаний».
16. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. - Москва.: ДМК Пресс, 2008.
17. Мониторинг судоходства в системе АИС [Электронный ресурс]. Режим доступа: https://www.marinetraffic.com/en/АИС/home/centerx:88.8/centery:60.1/zoom:3(дата обращения 19.05.2025)
18. Смит Ричард Э. Аутентификация: от паролей до открытых ключей.: - М.: Издательский дом "Вильямс", 2002. - 432 с. ISBN 5-8459-0341-6
19. Гатчин, Ю.А. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.А. Гатчин, В.В.Сухостат. - СПб.: СПбГУ ИТМО, 2010.
20. Gary R. Wright, W.Richard Stevens TCP/IP Illustrated. Volume 2. The implementation. Addison-Wesly Professional, 1995. 1194 c.
21. A Thomas. Arthur D. Enabling TCP/IP Communications Over High Frequency Communication Links. School of Electrical Engineering and Robotics Faculty of Engineering QUT University, 2024, c.45.