МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Морских информационных систем

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(магистерская диссертация)

На тему: «Алгоритмы получения и расчета дополнительной навигационной информации для швартовки безэкипажного судна в режиме реального времени»

Исполнитель Солодовников Евгений Валерьевич

Руководитель профессор д.т.н. Сикарев И.А.

«К защите допускаю»	**«Согласовано»**
Руководитель ОПОП	Заведующий кафедрой
_____ Завгородний В.Н.	_____Сикарев И.А.
«___»_____2021 г.	«___»_____2021 г.

Санкт-Петербург

2021 год

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АИС – Автоматическая информационная система

АСУ – Автоматизированная система управления

БИНС – Бесплатформенная инерциальная навигационная система

ВОГ – Волоконно-оптические гироскопы

ВРК – Винто-рулевая колонка

ГЛОНАСС – глобальная навигационная спутниковая система РФ

ГНСС – Глобальная навигационная спутниковая система

ГЦСК – геоцентрической системы координат

ДПМС – Дистанционно пилотируемое морское судно

ДП – диаметральная плоскость

ИНС – Инерциальная навигационная система

КЛГ – Кольцевые лазерные гироскопы

ЛДПС – Локальные дифференциальные подсистемы

ММТ – Микромеханические гироскопы

МНК – метод наименьших квадратов

НАП – Навигационная аппаратура потребителей

НКА – Навигационные космические аппараты

РЛС – Радиолокационная станция

САРП – Средства автоматической радиолокационной прокладки

САШ – Система автоматической швартовки

СДУ – Система дистанционного управления

СДКМ – Система дифференциальной коррекции и мониторинга

СУДС – Система управления движением судов

СКМС – Система контроля мореходности судна

СРНС – Спутниковая радионавигационная система

ССУВРК – Следящая система управления винто-рулевой колонкой

ССУОВ – Следящая система управления оборотов винтов

ТПЦК – топоцентрическая система координат

ФК – фильтр Калмана

ШДПС – Широкозонные дифференциальные подсистемы

ЭКНИС – Электронная картографическая навигационно-информационная система

ABAS – Aircraftbased Augmentations Systems

DGPS – Differential global positioning system

GPS – Global positioning system

IMO – International maritime organization

INS – Inertial Navigation System

RTK – Real time kinematic

SBAS – Satellite based augmentation system

Введение

Рассматривая современные тенденции развития технологии в транспортной индустрии невозможно не отметить повышенный интерес к задачам внедрения беспилотных технологий. Также, необходимо отметить, что исследования состояния обеспечения безопасности судоходства говорят о необходимости более глубокой автоматизации процессов лоцманской проводки и швартовки крупнотоннажных судов в портовой зоне. Применение, в целях снижения влияния человеческого фактора на возникновение аварийных ситуаций, передовых беспилотных технологии при проводке и швартовке судов в условиях порта, несомненно, может привести к значительному экономическому эффекту.

На сегодняшний день, уровень развития техники позволяет в качестве одного из самых перспективных направлений в развитии безэкипажных технологий отнести дистанционное управление. В случае реализации указанной технологии на борту судна отсутствует экипаж, а управление осуществляется дистанционно. Оператор или группа операторов, получает все необходимые данные для принятия решений, направленных на обеспечение безопасности судоходства от различных датчиков, расположенных на борту судна в режиме реального времени.

Реализация такой задачи возможна только в случае организации процедур высокоточного местоопределения подвижного объекта, определения углов пространственной ориентации подвижного объекта, организации устойчивого канала управления и мониторинга, аутентификации и идентификации удаленно подключаемого оператора. Кроме того, необходимо разработать программу и провести испытания навигационной аппаратуры с использованием навигационных сигналов ГНСС ГЛОНАСС и ее функциональных дополнений.

Актуальность данной темы обусловлена повышенным интересам мирового сообщества в целях создания безэкипажных судов, на сегодняшний день современные технологии дают возможность для создания таких

проектов, в будущем безэкипажные суда должны если не вытеснить обычные суда, то взять под контроль большую часть морских и речных перевозок.

Целью данной работы является исследование алгоритмов получения и расчета дополнительной навигационной информации для швартовки безэкипажного судна в режиме реального времени.

Основные решаемые задачи данной дипломной работы:

- Обзор классификации безэкипажных судов
- Обзор спутникового навигационного оборудования
- Обзор структурной схемы СДУ ДПМС
- Исследование алгоритма получения и расчёта дополнительной навигационной информации для швартовки ДПМС в режиме реального времени

Глава 1 Классификация безэкипажных судов и основные элементы оборудования.

1.1 Классификация безэкипажных судов.

Безэкипажное судно – автономное судно, как совокупность модульных систем управления и коммуникационных технологий следующего поколения, которые позволяют осуществлять функции беспроводного мониторинга и управления как на борту, так и за его пределами.

На протяжении всей мировой истории человечество стремилось к изобретению и эксплуатации различных средств передвижения. В прошлом веке, в связи с развитием технологий, специалисты получили возможность разрабатывать автономные виды транспорта. На сегодняшний день существуют и активно используются автономные средства различного вида автотранспорта, мировой практике известны примеры автоматизированных метрополитенов и автоматических управляемых транспортных средств на современных контейнерных терминалах. Специалистами в сфере авиации разработаны различные подходы к концепции автономного управления. Указанное позволяет сделать вывод, что автономное управление транспортными средствами является межотраслевым и мировым трендом, в стороне которого не вправе оставаться и водный транспорт. Наработки по развитию безэкипажного флота ведутся во многих странах. Так, например, британский холдинг Rolls-Royce – один из ведущих мировых поставщиков коммерческой судоходной отрасли – занимается разработкой беспилотных грузовых морских судов. Специалисты компании утверждают, что судно без экипажа и с дистанционным управлением будет безопаснее и дешевле, чем обычное. В коллаборации компании YARA и KONGSBERG (Норвегия) ведут разработки в области создания экологичного контейнеровоза без экипажа. Разрабатываемое судно «YARA Birkeland» будет первым в мире автономным судном, работающим на электроэнергии, что позволит полностью исключить вредоносные для окружающей среды выбросы. Специалисты

классификационного общества Lloyd’s Register (LR) в сотрудничестве с компаниями ST Engineering Electronics, Mitsui & Co. и Smart City Solutions также разрабатывают автономные суда. На территории Европейского Союза уже несколько лет ведутся работы по разработке новой системы автономного управления судоходством, позволяющей грузовым судам совершать океанские переходы без экипажа на борту (проект Maritime Unmanned Navigation traugh Intelligence in Networks – MUNIN). Японские и китайские представители судостроительной отрасли внедряют различные технологии автономной навигации для морских судов. Предполагается, что эксплуатация автономных судов позволит снизить их себестоимость уже в процессе постройки, сократить стоимость грузоперевозок, при том, что грузовместимость увеличится, а также уменьшить потребление топлива. Несомненно, развитие безэкипажного управления позволит индустрии морского и речного транспорта решать существующие и будущие задачи в области конкурентоспособности, безопасности, стабильности и иных областях. Для Российской Федерации создание и опережающее развитие беспилотного судовождения является не только способом повысить эффективность судоходной отрасли, но жизненно важным вопросом влияния на будущие стандарты мировой транспортной системы. Между тем, технические разработки и реальная возможность эксплуатации автономного флота опережают степень разработанности правового регулирования данного феномена, ибо как международно – правовые, так и акты национального уровня подразумевают нахождение на борту судна живых людей – экипажа. Не будем вдаваться в перечисление множества действующих международных конвенций, касающихся судоходства, которые подвергнутся пересмотру, в связи с появлением автономных судов, но отметим, что эксплуатация таких судов, а в отдаленной перспективе и отказ от использования судов, управляемых экипажем, повлечет необходимость внесения существенных изменений в Международную конвенцию о подготовке и дипломировании моряков и несении вахты 1978 года.

Указанная конвенция является одной из трех основополагающих морских конвенций, принятых под эгидой Международной морской организации (International Maritime Organization (IMO), в которой участвуют более 70 стран, и которая закрепляет международные нормы подготовки и дипломирования моряков и несения вахты, и предусматривает положения, обеспечивающие охрану человеческой жизни и сохранность имущества на море, а также защиту морской среды.

На международном уровне уже ведется обсуждение будущего правового регулирования автономного судоходства. В плане развития IMO на 2018 - 2023 гг. одним из ключевых стратегических направлений указана «Интеграция новых и передовых технологий в нормативно – правовую базу». Указанное направление включает в себя нахождение баланса между преимуществами, полученными от новых и передовых технологий, которые развиваются стремительнее любого законодательства, и соображениями безопасности и защиты, воздействия на окружающую среду и упрощения процедур международной торговли, потенциальными затратами для отрасли и, наконец, их взаимодействия с «персоналом» как на борту, так и на берегу.

На национальном уровне также ведется работа по совершенствованию законодательства, в связи с появлением судов без экипажа. Так, например, в соответствии с поправками к Закону Финляндии об экипаже судов и безопасном управлении судов внесены изменения, касающиеся требований к составу экипажа для автономных судов и их тестированию. Ведется разработка закона о дистанционном управлении автономных судов.

Российская Федерация не остается в стороне актуального тренда и активно ведет работу по правовому регулированию возможной эксплуатации автономных судов. Распоряжением Правительства от 29.03.2018 года № 534-р (в ред. от 12.09.2019) утвержден план мероприятий («дорожная карта») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Маринет». В соответствии с утвержденной

дорожной картой на компетентные государственные органы возложена обязанность по разработке нормативных правовых актов, обеспечивающих опережающее внедрение новых технологий в морскую отрасль Российской Федерации. В соответствии с правилами юридической техники разработка правового регулирования любой сферы должна начинаться с определения дефиниций, в связи с чем потребуется закрепить само понятия безэкипажного судна. Разработчики уже указанного нами в настоящей статье проекта MUNIN предлагают определять автономное судно, как совокупность модульных систем управления и коммуникационных технологий следующего поколения, которые позволяют осуществлять функции беспроводного мониторинга и управления как на борту, так и за его пределами. Указанные технологии будут включать в себя передовые системы поддержки принятия решений для обеспечения возможности удаленной эксплуатации судов под частичным или полностью автономным управлением. Разработчики понятия постарались определить безэкипажное судно максимально широко, поскольку техническая степень разработанности таких судов предполагает различные уровни его автономности. Комитетом по безопасности IMO определены четыре таких уровня в зависимости от степени участия людей в управлении судном. Стоит отметить, что используемые в настоящее время экипажные суда относятся к так называемому нулевому уровню автономности, поскольку все необходимые управленческие решения принимаются экипажем. Следующие четыре уровня предполагают отказ от нахождения людей на борту в той или иной степени.

Суда первого уровня предусматривают частичную автоматизацию и возможность удаленного контроля при необходимости. На судах такого уровня судовые операции частично будут выполняться автоматически, но находящийся на борту экипаж будет контролировать судовые процессы и при необходимости сможет повлиять на управленческие решения системы. Соответственно, конструкция таких судов должна позволять управлять ими

как автономно, так и вручную. Предположительно, для экипажей судов данного уровня квалификационные требования не будут кардинально отличаться от имеющихся, однако потребуются изменения в части несения вахты и взаимодействия с автономной системой управления.

Суда второго уровня предполагают наличие частичного дистанционного управления, что подразумевает прохождение всех судовых процессов автоматически, включая управление движением судна и принятия решений по изменению режимов движения. Вместе с тем, подразумевается присутствие на таких судах экипажа, который будет иметь возможность вмешиваться в работу судна в крайних случаях. Последующие уровни автоматизации судов исключают нахождение людей на борту.

Третий уровень предусматривает автономное управление судном и принятие решений береговым персоналом. В свою очередь, на четвертом уровне или на уровне «полной автоматизации» судовая система полностью самостоятельна и принимает необходимые управленческие решения без участия судового и берегового персонала.

Появление автономных судов всех вышеупомянутых уровней повлечет необходимость пересмотра норм, устанавливающих требования к экипажу, а также его количественному и качественному составу. Потребуется разработка мероприятий по подготовке и дипломированию членов экипажей таких судов и берегового персонала. Несомненно, появятся новые судовые должности, например, внешний капитан или береговой экипаж. Кроме того, появление безэкипажных судов явится предпосылкой для изменения нормативно – правового регулирования трудовых правоотношений в судоходстве, ибо отпадет необходимость обеспечивания жизнедеятельности людей на судне, что в свою очередь предопределит внесение изменений в технические и организационные требования к судну, касающиеся его обитаемости.

Немаловажные изменения коснутся деятельности классификационных обществ по всему миру, которым потребуется разработать новые правила

постройки, классификации и освидетельствования безэкипажных судов, на основании которых таким судам будут выдаваться соответствующие свидетельства. Кроме того, эксплуатация автономных судов поставит перед отраслью вопрос о гражданской ответственности за негативные последствия при происшествиях (различного рода инцидентах и авариях) на море. Потребуется законодательное закрепление порядка определения лиц, ответственных за возможные столкновения судов, загрязнение окружающей среды вследствие происшествий, за причинение вреда инфраструктуре. Данный аспект непосредственно отразится на правилах различного страхования судов и гражданской ответственности, возможно изменениям подвергнутся подходы к определению уровня страхового риска.

Особое внимание законодателю предстоит уделить разработке правового регулирования «взаимодействия» автономного судна с портовыми властями на подходах к порту, с различными органами в процессе пограничного, таможенного и иных видах административного контроля, с агентами, грузовладельцами и иными лицами в период нахождения судна в порту. Особо отметим, что при подходе судна в порт береговые службы управления движением судов руководят судовым трафиком, принимая во внимание коммерческие, погодные и навигационные условия в порту. Существуют порты, на подходах к которым обязательна ледокольная проводка. В указанных случаях, береговые службы взаимодействую с экипажем судна, снабжая его рекомендациями, с учетом перечисленных особенностей. Соответственно, появление на водных пространствах автономных судов потребует законодательного решения взаимодействия с таким судами различного рода служб и государственных органов.

Допустимо предположить, что законодательные изменения коснутся перечня и состава судовых документов, поскольку довольно непоследовательно требовать нахождения на борту безэкипажного судна бумажной документации. Вероятно, что регистрационные и

классификационные документы, а также судовой и машинный журналы будут переведены в электронный вид и будут иметь «привязку» к судну.

Многие институты морского права, существующие на протяжении веков, подвергнутся существенным изменениям, в связи с появлением автономного флота. Например, потребуется законодательно урегулировать порядок выдачи коносаментов, которые в настоящее время выдаются капитаном судна, являющего представителем судовладельца и действующим от его имени. Каким образом в коносаменты будут вноситься оговорки относительно принимаемого к перевозке груза? Вопрос остается открытым[4]. Для категоризации дистанционно и автономно управляемых надводных судов вводится составное обозначение, характеризующее возможность управления судном в открытом море и при движении в стесненных условиях: узкостях, местах швартовки, в портах: . При движении судна в море: MC, MCDS, RCMC, RC, AC и при движении в стесненных условиях: MC, MCDS, RC MC, RC, AC. Пояснения для составных обозначений приведены в Таблице 1.

Таблица 1.

MC	Ручное управление	человек на борту
MC_{DS}	Ручное управление с поддержкой принятия решения	человек на борту
RC_{MC}	Дистанционное управление с возможностью перехода на ручное	человек на борту
RC	Дистанционное управление	нет человека на борту
AC	Автономное управление	нет человека на борту

Примеры составного обозначения категории судна: AC-MC (AC – автономное при движении в море и MC – ручное управление при проходе узкостей и при входе в порт), или RC_{MC}-MC_{DS} (RC_{MC} – дистанционное

управление с возможностью перехода на ручное при движении в море и MC_{DS} – и при входе в порт)[5].

1.2 Обзор спутникового навигационного оборудования для позиционирования судна в акватории порта и на прилегающих территориях.

Для высокоточного позиционирования корпуса морского судна, необходим оптимальный выбор датчиков, позволяющих с требуемой точностью и надежностью определять позицию дистанционно пилотируемого морского судна (ДПМС) и его параметры движения. Для высокоточного позиционирования корпуса ДПМС в акватории порта и на прилегающих районах наиболее целесообразно использовать комбинацию из спутникового компаса, работающего с использованием глобальной навигационной спутниковой системы (ГНСС) ГЛОНАСС и ее функциональных дополнений, и волоконно-оптического гирокомпаса, имеющего возможность работать в режиме инерциальной навигационной системы.

В настоящее время на рынке представлены спутниковые компасы, как отечественного, так и зарубежного производства, позволяющие автоматически в режиме реального времени отслеживать курс, скорость и пространственные углы ориентации судна и своевременно информировать судоводителя об изменении указанных параметров.

В данной главе рассмотрены параметры шести наиболее интересных с технической и функциональной точки зрения моделей: японские Furuno SC–30 и JLR– 30 компании JRC, канадский Hemisphere V111, Comet LT компании Azimuth Technologies и российские модели: Бриз-КМ-РНК и СН-5703 – навигационная аппаратура потребителей (НАП) ГНСС ГЛОНАСС/GPS/GALILEO в комплекте с системой угломерной КБ «НАВИС».

Спутниковый компас Furuno SC– 30 представлен на рисунке 1 [28].

Рисунок 1 – Спутниковый компас Furuno SC-30

Спутниковый компас FURUNO SC-30 – навигационный прибор для определения координат судна и передачи этих данных другому судовому оборудованию, включая приборы автоматической информационной системы (АИС). Спутниковый компас FURUNO SC-30 предназначен к использованию на всех видах судов, в том числе и высокоскоростных. Прибор имеет сертификат Российского Речного Регистра.

Спутниковый компас FURUNO SC-30 состоит из двух GPS-антенн (для расчета первого вектора), трехосевого скоростного гироскопа, датчиков ускорения (для определения второго вектора) и процессора. Сигналы, поступающие от датчиков, подвергаются цифровой обработке, по результатам которой вычисляются параметры судна, в т. ч. курс по отношению к грунту, данные о бортовой и килевой качке, рыскании, скорости по отношению к грунту, скорости поворота, координатах судна по GPS-данным. Эти параметры могут передаваться другому навигационному оборудованию судна – РЛС, эхолотам, плоттерам, приборам систем АИС, САРП, ЭКНИС.

Компас FURUNO SC-30 обеспечивает вычисление курса с погрешностью до 1,0°, с такой же погрешностью определяется

бортовая/килевая качка. Погрешность вычисления координат в системе GPS составляет 10 м (95%), а в системе WAAS 3 м (95%).

Скорость поворота судна, которую позволяет отслеживать прибор составляет 45°/сек., что позволяет использовать его даже на высокоскоростных судах. Кроме того этот компас может выполнять функции приемника GPS. Готовность к работе составляет три минуты после подключения питания. Питание осуществляется от сети напряжением 12-24 В DC, рабочий ток 1,2-0,5 А.

Следующим рассматриваемым оборудованием будет прибор фирмы JRC модель JLR-30 (Рисунок 2).

Рисунок 2 – Устройство дистанционной передачи курса JRC модель JLR-30

JRC JLR-30 представляет собой устройство дистанционной передачи курса (на базе ГНСС GPS). Имеет сертификат одобрения Российского Морского Регистра Судоходства. Предназначен для использования на судах валовой вместимостью менее 500. GPS компас JRC JLR-30 определяет направление, местоположение, скорость и курс с высокой точностью, в любой точке плавания и при любых погодных условиях.

Технические характеристики:

- диаметр антенны: NNN-30: 1152 мм;

- дисплей: 5.7", LED, 320x240 точек (с 4х позиционным диммером подсветки);
- питание: 10.8 – 31.2 VDC, <12 Вт.
- Количество каналов: 12+1 для SBAS;
- Частота: 1575.42 МГц ±1 МГц;
- Точность: 0.3° rms (для JLR-30);
- Четкость отображения данных: 0.1°;
- Четкость выходных данных: 0.01° (для JLR-30);
- Отслеживание поворота: 45°/сек;
- Отслеживание ускорения: 1 G;
- Температура эксплуатации: от -25°C до +70°C;
- Пыле/влагозащищенность: дисплей – IPX4, сенсор – IPX6.

Следующим рассматриваемым устройством данного класса является V111 канадской фирмы Hemisphere (Рисунок 3).

Рисунок 3 – Hemisphere V111 GPS Compass

Несмотря на разницу в цене по сравнению с Furuno SC-30, данный прибор обладает существенно лучшими заявленными характеристиками как, например, по весу – 1,5 кг против 2,5 кг, так и по точности, что является, безусловно, основной характеристикой при сравнении данного типа

оборудования: 2.5 м в обычном режиме и 0.6 м при использовании DGPS. Одновременно устройство обеспечивает и хорошие показатели времени получения первого отсчета навигационных определений: «теплый старт» (основной режим) - (20+10) с и «холодный старт» (первое включение) - (60+10)с.

Последним из рассматриваемых приборов иностранного производства будет Comet LT компании Azimuth Technologies (Рисунок 4).

Рисунок 4 – Azimuth Technologies Comet LT

По своим характеристикам данный прибор попадает между Hemisphere V111 GPS Compass и Furuno SC-30. Обладая аналогичным с изделием фирмы Furuno весом (2,5 кг) прибор обеспечивает более высокую точность определения координат - среднеквадратичное отклонение измерений координат местоположения составляет: 5 м (в стандартном режиме точности), 1.5 м (в режиме DGPS), углов - 0.5º.

Отечественным прибором, позволяющим решать подобные задачи является «Бриз-КМ-РНК» производства КБ «Навис» (Рисунок 5).

Рисунок 5 – Аппаратура «Бриз-КМ-РНК» в различных вариантах исполнения

Аппаратура «Бриз-КМ-РНК» предназначена для автоматического определения текущих координат места, времени, путевой скорости, текущих углов пространственной ориентации потребителя в реальном масштабе времени по сигналам космических навигационных систем ГЛОНАСС, GPS и их средств функциональных дополнений в любой точке земного шара, в любой момент времени и независимо от метеоусловий, выдачи их на устройство индикации и по стандартному интерфейсу внешним потребителям, а также для решения сервисных задач.

Аппаратура «Бриз-КМ-РНК» обеспечивает решение следующих задач:

- выработка углов ориентации основана на принципе мультиантенного фазового интерферометра. В состав аппаратуры входит 3 (опционально 4) спутниковые антенны, которые могут быть произвольно размещены на объекте с учетом его конструктивных особенностей (т.н. «свободная база»). Антенны снабжены защитными отражателями, подавляющими негативное влияние переотраженных сигналов на точность решения;
- выбор оператором и индикацию следующих режимов работы: абсолютные определения по сигналам НКА КНС ГЛОНАСС, GPS, ГЛОНАСС/GPS, дифференциальный режим с учетом поправок от широкозонных дифференциальных систем (SBAS), дифференциальный режим с учетом корректирующей информации МДПС, дифференциальный режим с учетом поправок от широкозонных дифференциальных систем (SBAS) и корректирующей информации МДПС;
- автоматическое определение текущих координат места (широты, долготы, высоты), текущего вектора путевой скорости (путевого угла, путевой скорости) фиксированной точки (фазового центра антенны), текущих углов ориентации (курса, крена, дифферента), выдачу на индикацию данных навигационных

определений и времени, к которому они относятся в режиме абсолютных определений и в дифференциальном режиме;

- Ввод корректирующей информации МДПС по интерфейсу RS-232 и ее учет при решении навигационной задачи;
- распределение аппаратных каналов приема сигналов НКА КНС и SBAS, выдачу на индикацию и во внешние устройства информации о состоянии каналов приема;
- решение навигационной задачи по минимальному созвездию из трех НКА одной КНС;
- автоматический самоконтроль технического состояния аппаратуры «Бриз-КМ-РНК» с индикацией информации об отказавшем узле (блоке);
- выдачу кода оцифровки метки времени и значения поправки на расхождение ШВ КНС и ШВ UTC (SU) или UTC в зависимости от рабочей КНС;
- выдачу на индикацию текущего времени в формате часы, минуты, секунды.
- счисление пути корабля при отсутствии навигационных определений по данным от НК, последнего определения или по данным, вводимым вручную.
- выдачу на индикацию и во внешние устройства навигационных параметров в системах координат WGS-84, ПЗ-90, СК-95, СК-42 или пользовательская;
- сопряжение с внешними устройствами по интерфейсу RS-232/422 в соответствии с IEC 1162 (NMEA 0183);
- автоматическое обновление и хранение альманахов КНС ГЛОНАСС и GPS в течение не менее 30 суток после выключения аппаратуры «Бриз-КМ-РНК»;
- автоматический учет превышения геоида над эллипсоидом;

- автономный контроль достоверности навигационных определений (RAIM);
- определение ионосферной задержки и коррекцию измерений при приеме сигналов НКА КНС ГЛОНАСС;

Точность определения углов ориентации зависит от расстояния между антеннами. Заявленные характеристики обеспечиваются в следующих диапазонах изменения параметров движения корабля:

качке и рыскании корабля со следующими параметрами:

- бортовая качка с амплитудой от -25° до +25°, периодом 5 с и радиусом не более 10 м;
- килевая качка с амплитудой от -10° до +10°, периодом 4 с и радиусом не более 10 м.

Другим отечественным спутниковым компасом, взятым для сравнения, является НАП ГНСС ГЛОНАСС/GPS/GALILEO СН-5703 в комплекте с системой угломерной производства ЗАО «КБ Навис» (Рисунок 6).

Рисунок 6 – Спутниковый компас СН-5703 ЗАО «КБ Навис»

(1 - Разъемы для подключения антенн ГНСС/ДГНСС, GPRS, 2 - Слоты для SIM карты и карты памяти (под защитной крышкой), 3 - Цветной жидкокристаллический экран с резистивной сенсорной панелью, 4. -Кнопка «ТРЕВОГА», 5 - Светодиоды «АВАРИЯ», «ВНИМАНИЕ», «ПИТАНИЕ», 6 - Кнопочная клавиатура размером 3 на 4, 7 - Предохранитель и выключатель питания, 8 - Разъем подачи питания 24В, 9 - Функциональные кнопки, 10 - Разъемы на нижней панели для подключения внешних устройств)

НАП СН-5703 соответствует требованиям Технического регламента о безопасности объектов морского транспорта, утвержденного постановлением Правительства РФ от 12.08.2010 №620 и Правилам по оборудованию судов. РМРС 2012 г.

Данный прибор обеспечивает:

а) автоматическую непрерывную выработку привязанных ко времени навигационных параметров (режим ориентирования):

- текущих координат места;
- путевой скорости;
- курсового угла, угла места;
- углов пространственной ориентации;

б) информационно-техническое сопряжение с внешними устройствами:

- электронная картографическая система (ЭКС Тальвег В12);
- судовые радиостанции ПВ/КВ или УКВ (взаимоисключающе);
- Инмарсат мини-С (3026М);
- Инмарсат FleetBroadBand (FBB 250, 500);
- Инмарсат D+ (IsatM2M DMR-800L);
- терминал Глобалстар (GSP2800M1);
- терминал Иридиум (OpenPort);
- приемник АИС (Т300); по интерфейсу RS-232/422 в соответствии с протоколом NMEA-2000;

в) возможность перехода в ждущий режим (экономии энергии);

г) возможность перехода после получения первого отсчета навигационных параметров в режим осреднения угловых величин и значений текущих координат;

д) формирование признака прекращения обсерваций;

е) возможность регистрации, хранения (и отображения) углов и текущих координат местоположения во встроенной памяти;

ж) выбор оператором необходимой системой координат.

В отличие от предыдущей рассмотренной отечественной системы она обладает характеристиками более схожими с зарубежными аналогами как по массо-габаритным параметрам так и по техническим и эксплуатационным характеристикам.

К тому же этот компас может использовать антенную систему со свободной базой, что позволяет определять скорости не только центра тяжести, но и носа и кормы, что необходимо при швартовке ДПМС.

Кроме того, SC-30 может работать только от американской WAAS, которая не охватывает территорию РФ, в то время как CH-5703 может принимать сигналы, как от ЛДПС, так и от СДКМ. Поэтому в качестве спутникового компаса целесообразно выбрать модель CH-5703.

Существенным недостатком спутниковых компасов является его не автономность, то есть зависимость от сигнала ГНСС. Этот недостаток особенно критичен при плавании в узкостях и, в частности, в акватории порта, так как портовые сооружения могут вызывать кратковременное затенение приемных антенн спутникового компаса и, соответственно, потерю сигналов от спутников либо существенное увеличение HDOP. Для устранения этого недостатка используется комплексирование спутникового компаса с ИНС, имеющей возможность некоторое время работать в автономном режиме без коррекции, и определять координаты объекта, его курс и скорость[29].

Наиболее совершенными и автономными ИНС являются системы на гиростабилизированных платформах. В состав этих устройств входят: гиростабилизированная платформа; гировертикаль, стабилизирующая платформу в плоскости истинного горизонта; гирокомпас, установленный на платформе, ортогональные акселерометры и датчики углов крена и дифферента, также расположенные на гиростабилизированной платформе, а также вычислительное устройство. Благодаря наличию гиростабилизированной платформы, устройство позволяет, помимо

координат, курса и скорости объекта, определять также углы пространственной ориентации и угловые скорости поворота, бортовой и килевой качки.

Данные системы являются высокоточными, имеют длительное время автономной работы без коррекции. Однако эти параметры достигаются за счет высоких технических требований к элементам системы и сложных технологических решений, позволяющих компенсировать главную проблему ИНС – уход оси платформы. Поэтому данные ИНС чрезвычайно дороги и потому используются только в военной сфере, в первую очередь на подводных лодках и боевых кораблях.

Для гражданской сферы разработаны существенно менее автономные, но, соответственно, и более дешевые бесплатформенные инерциальные навигационные системы (БИНС). Эти системы для привязки к географической системе координат используют аналитическую плоскость истинного горизонта, получаемую в вычислительном устройстве по углам Эйлера и их производным, измеренным в местной системе координат.

В состав БИНС входят: три осевых гироскопа, жестко привязанные к осям местной системы координат; три акселерометра, также привязанные к этим осям и процессор, служащий для построения аналитической плоскости горизонта и вычисления навигационных параметров. БИНС может работать в двух режимах: корректируемом и автономном. В корректируемом режиме БИНС получает информацию о координатах объекта и его скорости от НАП ГНСС и с большой точностью вычисляет углы пространственной ориентации (курс K, крен θ, дифферент ψ), угловую скорость поворота ω_z, угловые скорости бортовой ω_x и килевой качки ω_y. В автономном режиме БИНС, помимо вышеуказанных параметров, вырабатывает также координаты объекта и его скорость. Однако точность определения навигационных параметров в этом режиме будет значительно меньше, а погрешность определения координат будет непрерывно накапливаться. Поэтому

автономный режим в этих системах можно использовать лишь весьма кратковременно.

Скорость нарастания ошибки определения координат в автономном режиме в БИНС зависит в основном от качества и типа осевых гироскопов. В настоящее время в БИНС используется три основных типа гироскопов: микромеханические (ММГ), волоконно-оптические (ВОГ) и кольцевые лазерные (КЛГ). Также существенное влияние на точность работы в автономном режиме оказывает и качество акселерометров.

Современные бесплатформенные инерциальные навигационные системы подразделяются по уровню точности. Существуют системы низкой, средней и высокой точности.

Согласно общепринятой классификации [6] к БИНС низкой точности относятся системы, точность определения координат в которых колеблется в диапазоне от 5,5 км/ч до 37 км/ч. В качестве чувствительных элементов в системах с низкой точностью в основном применяются микромеханические гироскопы (ММГ) и микромеханические акселерометры (ММА). Данные системы применяются только для систем стабилизации или интегрирования с НАП ГНСС. Так же существуют достаточно точные зарубежные MEMS датчики (микроэлектромеханические системы, объединяющие гироскоп и акселерометр), но данные типы датчиков существенно дороже имеющихся на рынке датчиков широкого потребления.

Системы средней и высокой точности в ряде случаев уже могут быть использованы для решения задач автономной навигации. Точность определения координат в случае систем средней точности находится в интервале от 1,85 км/ч (1 м.миля/ч) до 5,5 км/ч, а для систем высокой точности от 0,4 км/ч до 1,85 км/ч.

БИНС средней точности строятся на базе ВОГ, высокой точности – в основном на базе КЛГ. Данные гироскопы не содержат сложных механических деталей, имеют высокую надежность и обеспечивают высокую точность измерения. Так инструментальный дрейф ЛГ не превышает 0,01°/ч.

В системах, в которых требуется обеспечивать высокую точность при работе в широком диапазоне ускорений, применяются компенсационные акселерометры. Наибольшее распространение получили компенсационные акселерометры (АК) с маятниками из кварца или кремния, так как их характеристики близки к требованиям, предъявляемым к акселерометрам для высокоточных БИНС.

Наиболее дешевыми являются БИНС на ММГ. Но они же имеют и наименьшую автономность. Так, например, БИНЦ ОАО «Концерн «Электроприбор» на базе микромеханических гироскопов и акселерометров, изображенная на рисунке 7, имеет следующие технические характеристики:

- время готовности к выдаче углов качки (с погрешностью ±0,07°) – не боле е 1 минуты;
- выходной интерфейс – RS-232 (RS-422, RS-485);
- потребляемая мощность не более 10 Вт;
- габаритные размеры 120x122x80 мм, масса 1 кг.

Рисунок 7 – Внешний вид БИНЦ ОАО «Электроприбор»

БИНС Компа-Нав-3 ООО ТЕКНОЛ, изображен на рисунке 8.

Рисунок 8 – Внешний вид БИНЦ Компа-Нав-3 корпорации «ТеКнол»

БИНС Компа-Нав-3 в автономном режиме имеет накапливаемую погрешность в определении координат 25 м за 15 с. Данные цифры вполне приемлемы для большинства режимов работы морских судов. Поэтому многие модели спутниковых компасов уже имеют встроенные БИНС на ММГ, например, компас SC-30 Furuno. При кратковременных потерях сигнала от ГНСС, например, при прохождении под мостом, использование подобных БИНС вполне приемлемо. Однако при буксировке методом «на укол», когда ДПМС будет длительное время находиться в тени высокого борта крупнотоннажного судна, а требования к точности позиционирования велики, БИНС на ММГ не смогут поддерживать требуемую точность позиционирования.

Более совершенными, но и более дорогими являются БИНС на ВОГ. К ним относятся российские БИНС GL-SVG-03 компании «ООО ГИРОЛАБ», БИНС-501 НПК «Оптолинк», БИНС-ТЭК и Компа-Нав-3 «ООО ТЕКНОЛ», а также БИНС LN251 американской компании «Northrop Grumman». Акселерометры всех этих приборов выполнены по технологии MEMS. Внешний вид и габариты некоторых БИНС представлены на рисунке 9.

Рисунок 9 – БИНС GL-SVG-03

БИНС на ВОГ относятся к классу инерциальных систем средней точности и находятся в среднем ценовом диапазоне. Накапливаемая погрешность в автономном режиме у лучших из них больше 1 мили/час, что соответствует 8 и более метрам за 15 с. Данная погрешность удовлетворительна для большинства режимов эксплуатации судов, однако для буксировочных операций эта погрешность также слишком велика.

Самыми совершенными и, соответственно, самыми дорогими на сегодняшний день являются БИНС на КЛГ, относящиеся к классу инерциальных систем высокой точности. К ним относятся российские системы БИНС-СП-2 НИИ «МИЭА», БИНС 18-М-ОС НПК «Электрооптика», БИНС GL-150 «ООО ГИРОЛАБ», LN120G «Northrop Grumman», Sigma-95N французской компании «Safran» и другие. В этих системах используются в основном высокоточные кварцевые акселерометры. Внешний вид некоторых лазерных БИНС представлен на рисунке 10.

Рисунок 10 – БИНС-18М-ОС (слева, без крышек) и БИНС Sigma-95N (справа)

Исходя из всего выше сказанного в качестве БИНС в комплект к ГНСС целесообразно использовать российскую БИНС GL-150 на лазерных гироскопах.

Таким образом, модуль датчиков и его интерфейс с блоком обработки информации окончательно примет вид, изображенный на рисунке 11.

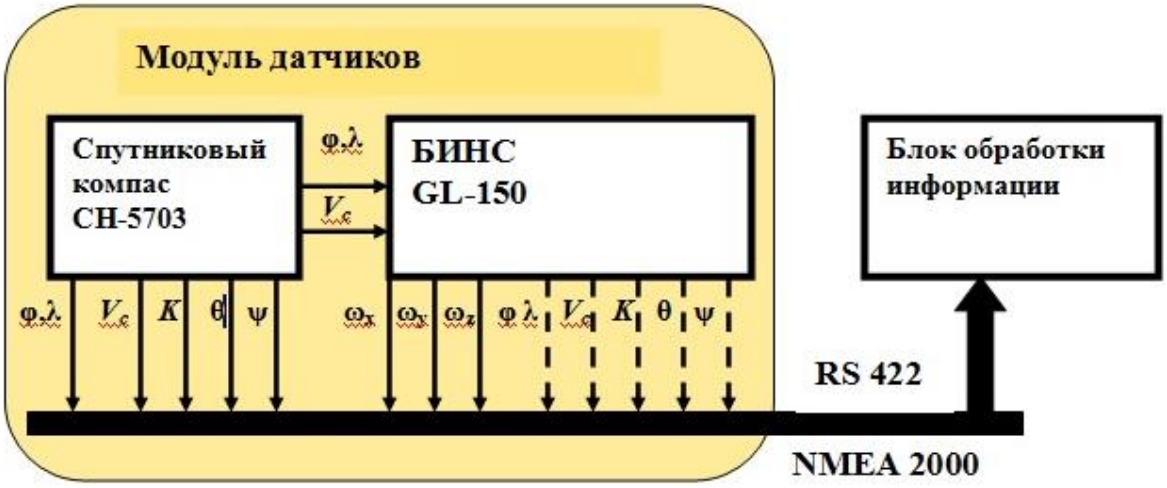


Рисунок 11 – Состав датчиков ДПМС и их интерфейс с блоком обработки

Как видно из рисунка, в режиме интеграции спутниковый компас будет выдавать высокоточные координаты и скорость ДПМС, а также углы его пространственной ориентации. Также компас будет передавать сигнал

коррекции (координаты и скорость ДПМС) в БИНС, которая будет вырабатывать угловые скорости поворота и бортовой и килевой качки. Эта информация через интерфейс RS 422 по протоколу NMEA 2000 будет поступать в блок обработки информации. При потере сигнала от ГНСС, БИНС переходит в режим инерциальной навигации и, помимо угловых скоростей, будет выдавать другие навигационные параметры вместо компаса.

1.3 Структуры основных элементов оборудования системы управления движением безэкипажного судна.

Помимо систем позиционирования и навигации, необходимо предусмотреть следующие элементы:

- блок управления;
- передатчик/приемник команд;
- приемник/передатчик данных телеметрии;
- транспондер АИС;
- морская УКВ-радиостанция;
- электронная картографическая навигационно-информационная система;
- модуль аутентификации.

Состав и распределение элементов по сегментам представлено на рисунке 12.

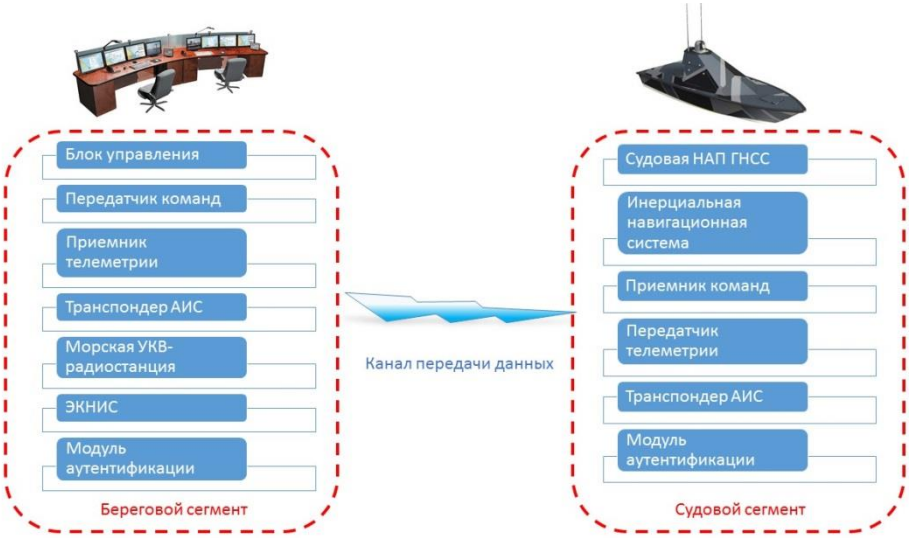


Рисунок 12 – Состав и распределение элементов системы управления движением дистанционно пилотируемого морского судна

Модуль управления. Модуль управления рабочего места оператора СДУ будет состоять из блока управления, преобразующего управляющее воздействие оператора в сигналы управления, и передатчика команд, посылающего сигналы управления по каналу управления в модуль обработки информации ДПМС.

Передатчик команд. Основной функцией передатчика команд является посылка сигналов управления по каналу управления в модуль обработки информации ДПМС. На борту ДПМС они будут приниматься соответствующим приемником.

Приемник телеметрии. Приемник телеметрии установлен в береговом сегменте системы управления движением дистанционно пилотируемого морского судна и предназначен для приема навигационных параметров ДПМС. Навигационные параметры ДПМС формируются набором датчиков, установленных на борту дистанционно пилотируемого судна, далее информация от них комплексируется и через передатчик направляется в приемник телеметрии. Оба набора устройств (передатчик/приемник команд и передатчик/приемник телеметрии) представляют собой СВЧ радиомодемы.

Транспондер АИС. Транспондер АИС предназначен для контроля оператором СДУ за передвижением судов в акватории порта и способен обеспечивать другие суда и компетентные органы информацией о судне в автоматическом режиме с заданной точностью и частотой, способствуя точному отслеживанию. Таким образом транспондером АИС должно быть оборудовано как ДПМС, так и рабочее место оператора. Он должен иметь исполнение класса А, иметь возможность отображения контролируемых целей на электронной карте ЭКНИС и передавать следующую информацию[29]:

1. Статическая:
    - Тип плавсредства;
    - Местонахождение антенны;
    - Основные габариты судна;
    - Позывной судна;
    - Название судна;
    - Номер Международной морской организации (МО);
    - Номер MMSI судна, полученный в радиочастотном центре.
2. Динамическая:
    - Координаты судна;
    - Время передачи посыла;
    - Время последнего обновления информации;
    - Истинный курс и курсовой угол;
    - Скорость;
    - Углы наклона по крену и дифференту;
    - Угол килевой качки;
    - Угловая скорость поворота и прочая информация от репитеров и датчиков электрорадионавигационных приборов и систем/
3. Информацию о рейсе:
    - Порт назначения

- Расчетное время прибытия судна в порт
- Осадка
- Сведения о характере и типе груза (при наличии)
- Информация об экипаже и пассажирах (при наличии)
- Иные информационные сведения

УКВ-радиостанция. Морская УКВ-радиостанция предназначена для оперативной связи оператора СДУ с лоцманом, а также с оператором СУДС на одном из международных каналов портовой службы и службы движения. Правила радиосвязи аналогичны правилам радиообмена между лоцманом, оператором СУДС и капитанами буксиров.

Электронная картографическая навигационно-информационная система. Сертифицированная ЭКНИС предназначена для наблюдения за движением ДПМС и других судов в акватории порта относительно обозначенных на карте навигационных опасностей, линий разделения движения и фарватеров. ЭКНИС обеспечивает безопасность судовождения и является альтернативой традиционным бумажным картам. Компьютерная система отображает информацию из электронных навигационных карт, интегрирует её с данными глобальных навигационных спутниковых систем, данными радаров и систем автоматической идентификации судов[29]. ЭКНИС должна выполнять следующие функции:

- вывод данных от приемоиндикатора местоположения судна, а также лага гирокомпаса на электронную карту и непрерывное ведение исполнительной прокладки;
- запись траектории пройденного пути;
- ведение электронного судового журнала и вывод его данных на печать;
- восстановление отображения траектории пути судна и записей судового журнала любого рейса;

- составление предварительной электронной прокладки предстоящего рейса с проведением расчетов скорости, расстояний, времени;
- избирательное управление составом отображаемой картографической информации;
- слежение за исполнительной электронной прокладкой и параметрами движения судна по маршруту;
- измерение географических координат дистанций и пеленгов любых объектов карты;
- сигнализация о приближении к путевой поворотной точке, отклонениях от установленных параметров движения судна и неисправностях самой системы;
- отображение карты в удобном масштабе (масштабирование) и врезка электронной карты;
- отображение электронной карты в режимах ориентации «Север вверху» и «Курс вверху»;
- получение дополнительной справочной информации о картографических объектах, средствах навигационного оборудования, гидрографических и других сведений из базы данных электронной карты;
- возможность слежения за изменением местоположения захваченных неподвижных объектов относительно движения собственного судна;
- вывод на экран изображения карт в различных форматах, в том числе стандарте ЭКНИС, утвержденном IMO;
- автоматическая, полуавтоматическая и ручная корректура электронных карт;
- подбор цвета экрана в зависимости от освещенности помещения рубки;

- мгновенная запись местоположения судна (человек за бортом);
- отображение на электронной карте целей, захваченных САРП/РЛС;
- запись (архивация) траекторий целей на диск и возможность их отображения вместе с соответствующей траекторией собственного судна и записями судового журнала[30].

Модуль аутентификации. Служит для обеспечения безопасности и предотвращения нелегального использования системы. Аутентификацию оператора СДУ целесообразно производить через сервер российской системы аутентификации и контроля (ЗИТ) по сети Интернет. Модуль аутентификации рабочего места оператора СДУ будет состоять из блока аутентификации, в который будет вставляться уникальный электронный ключ оператора, и маршрутизатора сети Интернет[29].

Вывод:

В данной главе рассмотрены классификация безэкипажных судов, произведен обзор приборов спутниковой навигации, а так же рассмотрена структура основных элементов оборудования системы управления движением безэкипажного судна.

Глава 2 Основные требования к программному обеспечению, идентификации и аутентификации. Концепция СДУ ДПМС

2.1 Эксплуатационные требования к программному обеспечению и организации обмена данными в СДУ ДПМС

Для того, чтобы сформулировать эксплуатационные требования к программному обеспечению СДУ ДПМС необходимо, в первую очередь, провести классификацию требований. В настоящее время чаще всего требования к программному обеспечению подразделят на функциональные и нефункциональные [20].

Функциональные требования регламентируют функционирование или поведение системы.

В отношении СДУ ДПМС функциональными требованиями являются следующие:

- обеспечение оператору возможности дистанционного управления ДПМС;
- обеспечение оператора всей полнотой данных телеметрии, поступающей от ДПМС;
- обеспечение функционирования механизма идентификации и аутентификации оператора ДПМС с использованием удостоверяющего центра.

Нефункциональные требования, соответственно, регламентируют внутренние и внешние условия или атрибуты функционирования системы. Выделяют следующие основные группы нефункциональных требований [21]:

- внешние интерфейсы;
- атрибуты качества;
- ограничения.

Основными атрибутами качества согласно модели FURPS являются следующие:

- функциональность
- удобство использования
- надежность
- производительность
- удобство сопровождения

Для создания интегрированного рабочего места оператора, СДУ необходимо рассматривать как интегрированную систему, из чего следует необходимость рассмотреть вопрос организации и требований к шинам и протоколам связи между ее оборудованием. Для выбора типа протокола, необходимо оценить объем передаваемой в единицу времени информации. Объем цифровой информации, снимаемой с типовых параметрических датчиков со встроенным вычислителем (контроллером) определяется словом, длина которого не превышает 80 байт для одного измеряемого параметра, в том числе с учетом контрольной суммы. Очевидно, что объем всей возможной обрабатываемой информации применительно к целям СДУ, особенно с учетом передачи изображения в реальном масштабе времени, является весьма значительным. Традиционным для организации сопряжения морского оборудования на судах является протокол обмена NMEA-0183 (IEC 61162-1), разработанный Национальной Ассоциацией Морской Электроники (National Marine Electronics Association) для поддержания совместимости морского навигационного оборудования различных производителей. NMEA-0183 представляет собой текстовый протокол и применяется для обмена данными навигационных устройств, использующихся на морских судах, таких как сонаров, радаров, электронных компасов, барометров. Протокол NMEA-0183 расширяемый, т.е. помимо описанных стандартом, он может быть дополнен проприетарными сообщениями на усмотрение разработчика.

Если приёмник или датчик с вычислителем имеет последовательный интерфейс RS-232 (COM-порт) и формирует текстовые сообщения в стандарте NMEA-0183, то обработку его данных легко реализовать в блоке

обработки первичных измерений с применением уже отработанных технических и программных решений.

Основной недостаток стандарта NMEA-0183 – относительно низкая скорость передачи (4800 бод) и преимущественно односторонняя направленность, т.е. все источники передают (и принимают) безадресные данные. При такой организации обмена данными существуют трудности в организации единой системы обмена данными, например возможны коллизии при посылке управляющих сигналов, которые могут истолкованы различным оборудованием по-разному. Поэтому на смену этому протоколу сегодня приходит протокол NMEA-2000, позволяющий объединять в единую сеть различные источники (датчики) и приемники.

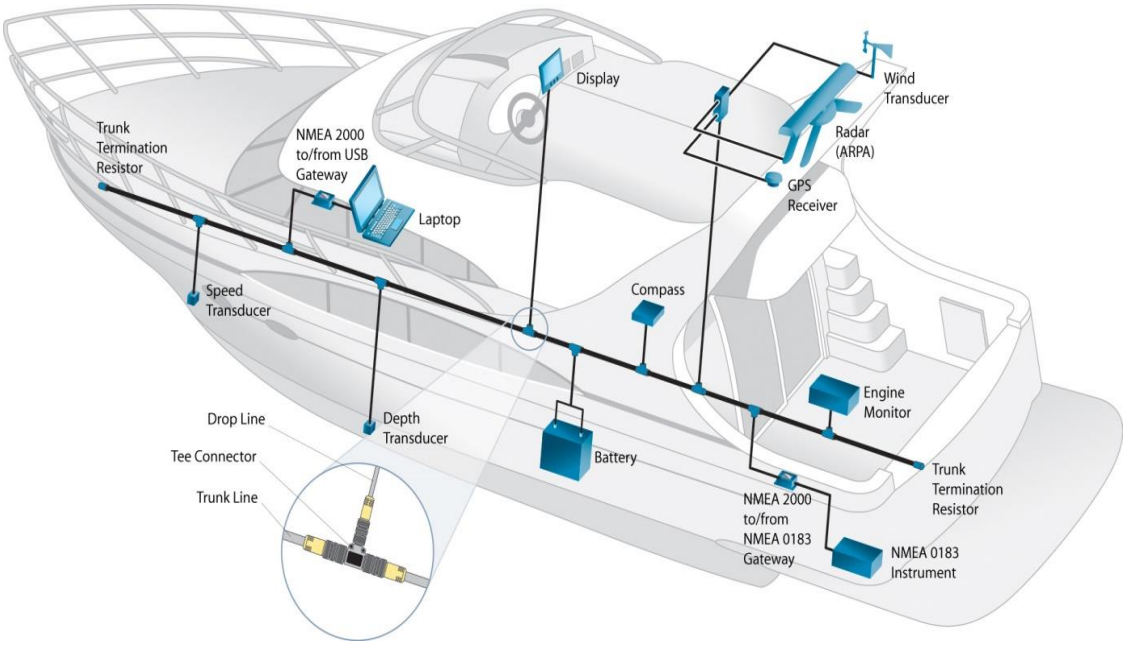


Рисунок 13 – NMEA-2000

NMEA 2000 (IEC 61162-3) является сетевым протоколом верхнего уровня, использующим стандарт передачи Controller Area Network (CAN). Этот протокол, в отличие от использовавшегося ранее NMEA 0183 (IEC 61162-1), позволяет объединить множество приборов в одну сеть и передавать информацию одновременно. Для подключения используются, как

правило, разъёмы стандартов Mini-c и Micro-c. Кроме того, NMEA-2000 предусматривает применение специальных кабелей стандарта DeviceNet.

Обмен данными осуществляется со скоростью 250 кбит/с и позволяет любому датчику общаться с любым приемником, совместимым с протоколами NMEA-2000. По электрическим параметрам, NMEA-2000 совместим с сетевыми контроллерами ("CAN Bus"), используемыми на дорожных транспортных средствах. Формат протокола более высокого уровня основан на SAE J1939 , с конкретными сообщениями для морской среды.

При работе с активными датчиками, то есть датчиками, которые могут принимать управляющие команды по цифровому интерфейсу, аппаратура среднего уровня должна уметь формировать управляющие команды и/или позволять другим управляющим устройствам передавать такие команды на активные датчики. Управляющие команды часто используются в навигационных приемниках для переключения режимов работы и тонкой настройки портов и протоколов обмена. Передача данных осуществляется по последовательному асинхронному цифровому интерфейсу RS232/422/485 (последовательный порт). Аналогичный интерфейс поддерживают сегодня подавляющее большинство датчиков, используемых для получения параметров движения судна.

При необходимости сопряжения с сетью Интернет разработан стандартный преобразователь интерфейсов RS232/422/485 – Ethernet. Данные преобразователи исполняются в виде отдельных и законченных устройств, включаемых в разрыв коммутируемых соединений, поэтому при необходимости его применения для передачи данных в судовую локальную вычислительную сеть или подключении внешних устройств по протоколу Ethernet, в аппаратуре СДУ достаточно организовать свободный последовательный порт.

Устройство и технические характеристики передатчика сигнала визуализации должны рассматриваться на этапе НИОКР при создании опытного образца СДУ.

Блок преобразования и обработки информации предназначен для преобразования команд управления, вырабатываемых в блоке управления рабочего места оператора посредством его соответствующих манипуляций, в сигналы управляющего воздействия, поступающие в блок управления движительной установки, а также для пакетирования навигационной информации, одновременно поступающей от различных датчиков по протоколу NMEA-2000.

Большое значение при создании эффективной СДУ ДПМС имеет выбор каналов управления и контроля. С одной стороны эти каналы должны обладать высокой пропускной способностью и помехозащищенностью, а с другой – не создавать помехи в работе радиосистем, используемых в СУДС.

Для построения информационных каналов оператор – ДПМС возможно использование всего двух видов линий связи: наземные радиолинии или линии спутниковой связи.

Минимальные эксплуатационные требования к программному обеспечению приведены в таблице 2.

Таблица 2 Минимальные эксплуатационные требования к программному обеспечению

Параметр	Значение
Ввод данных	Поддержка современных устройств ввода данных, аналогичных установленным в рубке судна, электронный ключ пользователя
Передача данных	Поддержка двух радиомодемов стандарта WiMAX, модема стандарта GSM с технологией MVNO

Продолжение таблицы 2

Обработка данных	В режиме реального времени
Отображение данных	Подключение трех мониторов диагональю 22 дюйма с разрешением 1920*1080
Протокол шифрования данных	Kerberos
Длина ключа шифрования, бит	128
Базовая ОС	Unix

В рассматриваемой СДУ ДПМС обмен данными будет происходить по трем основным направлениям:

- Оператор – СДУ ДПМС;
- Оператор – удостоверяющий центр;
- Удостоверяющий центр –ДПМС

Основные направления для обмена данными в СДУ ДПМС показаны на рисунке 14.

Рисунок 14 – Основные направления для обмена данными в СДУ ДПМС

Для организации обмена данными между береговым и судовым сегментами СДУ ДПМС (между оператором и СДУ ДПМС) возможным видится использование спутниковой системы Гонец третьего поколения.

Однако, третье поколение системы будет развернуто еще не очень скоро и остается ограничение скорости передачи информации (10 кбит/с).

Поэтому для реализации каналов визуализации целесообразно использовать технологию WiMAX стандарта IEEE 802.16 m, использующие СВЧ диапазон частот. Эта технология предназначена для обеспечения широкополосного беспроводного доступа к стационарной сети интернет. В нашем случае с помощью технологии WiMAX будет реализовываться сеть точка - многоточка, где точкой будет являться опорная станция, а многоточками – модемы WiMAX, установленные на ДПМС. Через опорную станцию WiMAX, видеоизображение по высокоскоростным выделенным линиям сети интернет будет поступать на рабочие места операторов СДУ.

Оборудование WiMAX стандарта IEEE 802.16 m предназначено для работы в полосе частот 3.5 – 5.0 ГГц. Согласно Постановлению Правительства РФ, полоса частот 3.4 – 3.6 ГГц предназначена для новых средств фиксированной службы «точка – многоточка», поэтому именно эту полосу целесообразно использовать при создании радиоканалов WiMAX стандарта IEEE 802.16 m.

Радиус действия одной опорной станции WiMAX в данном частотном диапазоне составляет порядка 100 км, что вполне достаточно, чтобы покрыть акваторию любого морского порта РФ. Пропускная способность – до 150 Мбит/с, что также может обеспечить одновременную передачу изображения с 5-6 ДПМС[31]. Таким образом, для получения телеметрических данных от ДПМС на пульт оператора и передачи управляющих команд оператора на ДПМС планируется использовать канал передачи данных WiMAX.

Но перед началом работы необходимо провести проверки, что ДПМС находится в состоянии, пригодном для эксплуатации, а оператор имеет право на управление им.

Данная схема приведена на рисунке 15.

Рисунок 15 – Схема проверки, реализуемая в СДУ ДПМС

Для решения поставленных задач на борту ДПМС находится уникальный электронный ключ «1», который устанавливает туда специалист, ответственный за техническую подготовку флота. После установки данного ключа по каналу передачи данных «4» происходит передача данных в отраслевую организацию «2», являющуюся системным интегратором транспортной и информационной безопасности (удостоверяющий центр), предполагается что данную роль можно возложить на ФГУП «ЗИТ». После прохождения процедуры подтверждения на пульт управления оператора СДУ ДПМС «3» от удостоверяющего центра «2» поступает информация о готовности к эксплуатации данного ДПМС.

Организацию допуска к работе оператора с ДПМС предполагается реализовать с помощью следующего алгоритма. Оператор СДУ ДПМС

подключает свой уникальный электронный ключ к пульту управления «3» (рабочему месту оператора).

От пульта управления «3» по каналу связи «4» данные уникального электронного ключа передаются на сервер, расположенный в отраслевой организации, являющейся системным интегратором транспортной и информационной безопасности «2» (ФГУП «ЗИТ»), где происходит идентификация оператора «3». Если идентификация оператора прошла успешно, тогда отправляется сообщение от системного интегратора транспортной и информационной безопасности на ДПМС «1», что данный оператор имеет право на управление.

В рассматриваемом алгоритме одна из значимых ролей отведена каналу передачи данных между устройством мониторинга, размещенном на борту контролируемого объекта, и сервером отраслевой организации, являющейся системным интегратором транспортной и информационной безопасности. С точки зрения удобства передачи данных конструктивным представляется использовать для данной цели канал связи, предоставляемый государственной автоматизированной информационной системой «ЭРА-ГЛОНАСС» (ГАИС «ЭРА-ГЛОНАСС»). Это согласуется с законодательством Российской Федерации, а именно п.5.1 Федерального закона от 28 декабря 2013 г. № 395-ФЗ «О ГАИС «ЭРА-ГЛОНАСС»: «Создание в сфере транспорта и в иных сферах, определенных Правительством Российской Федерации, государственных информационных систем, а также информационных систем, входящих в состав объектов концессионных соглашений, при функционировании которых предполагается использование навигационной информации (далее - информационные системы), осуществляется в соответствии с законодательством Российской Федерации и на основе обязательного использования информационного ресурса, и (или) программно-технических средств, и (или) технологической инфраструктуры системы (далее - составные части системы) в создаваемой информационной системе при наличии технической возможности такого

использования». Так как разрабатываемая система является информационной и предполагает непосредственное использование навигационной информации, то она подпадает под действие указанного закона.

Одновременно, необходимо отметить, что использование ресурса ГАИС ЭРА-ГЛОНАСС тем более оправдано технически, так как подразумевает передачу данных по каналу связи сотового оператора, чей сигнал обладает лучшими характеристиками приема в указанном районе (технология MVNO), а главное, при данной реализации отсутствует зависимость от частного лица, которым является оператор сотовой связи, так как АО «ГЛОНАСС», управляющее ГАИС «ЭРА-ГЛОНАСС» и предоставляющее услугу передачи данных, является АО с государственным участием (контрольный пакет у Правительства России).

Таким образом, в результате проведенного анализа получена схема организации обмена данными в СДУ ДПМС, приведенная на рисунке 16.

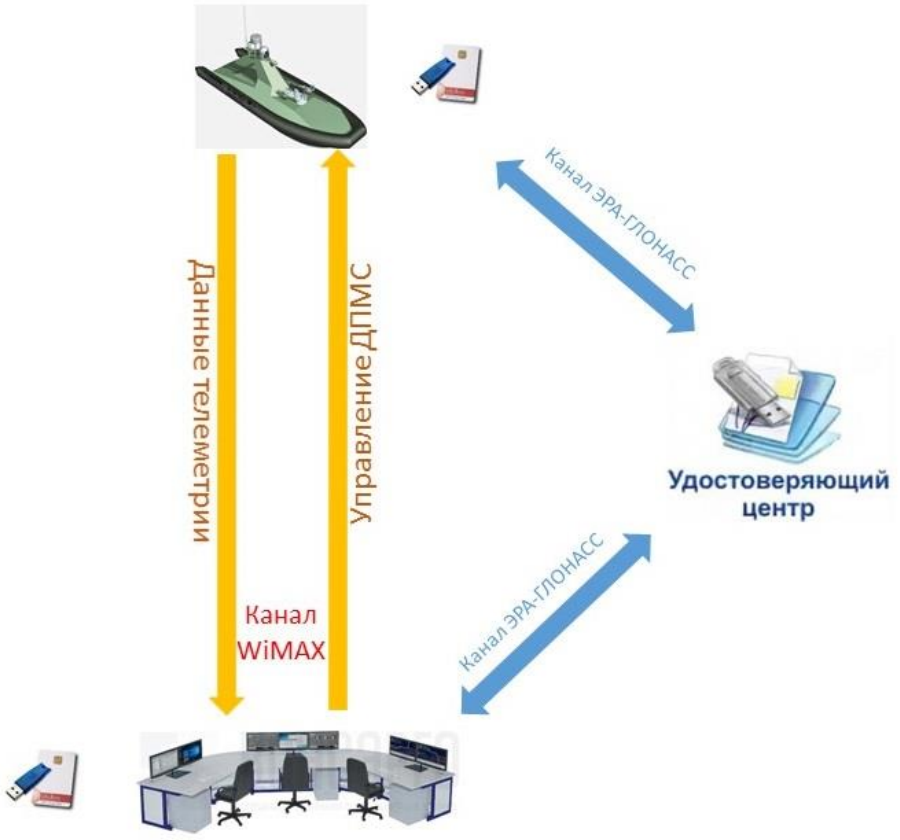


Рисунок 16 – Схема организации обмена данными, реализуемая в СДУ ДПМС

2.2 Методы идентификации, аутентификации управления доступом и функционирование системы управления движением морского судна

При установлении связи между оператором и дистанционно управляемым морским судном (СДУ ДПМС) могут возникать следующие угрозы информационной безопасности:

- Подмена оператора (злоумышленник выдает себя за оператора).
- Подмена (СДУ ДПМС) (злоумышленник выдает себя за (СДУ ДПМС).
- Несанкционированное изменение команд оператора.
- Несанкционированное изменение ответов (СДУ ДПМС).
- Несанкционированный доступ к командам со стороны злоумышленника (чтение команд).
- Принудительный разрыв соединения злоумышленником.

Для борьбы с первыми двумя угрозами используются протоколы аутентификации, позволяющие абонентам быть уверенными в подлинности собеседника. Для борьбы с несанционированным доступом и несанкционированными изменениями применяются, как правило, шифрование и методы аутентификации сообщений (электронная подпись, имитовставка, т.д.). Шестой пункт подразумевает физическое прекращение связи и в данном разделе, посвященном алгоритмическим методам обеспечения информационной безопасности, рассматриваться не будет[32].

Рассмотрим методы аутентификации, которые могли бы быть применены для решения указанных проблем подмены абонентов. Следует отметить, что односторонние методы аутентификации (когда только одна из сторон подтверждает свою подлинность перед другой) рассматриваться не будут, так как не позволяют решить одновременно и угрозу подмены оператора, и угрозу подмены (СДУ ДПМС). Следовательно, для решения поставленной задачи подходят только методы двусторонней (взаимной)

аутентификации, позволяющие обоим сторонам убедиться в подлинности друг друга[32].

Дополнительным фактором является обязательная аутентификация оператора в системе, которая выполняется в первую очередь при входе в нее и в случае успешного прохождения позволит ему исполнять свои функции. При этом подлинность операторов проверяет специализированный сервер аутентификации. Кроме того, при попытке оператора начать работу с ДУМС необходимо проверять его полномочия на выполнение данных действий[32].

Для выбора из существующих способов взаимной аутентификации необходимо также учитывать угрозы несанкционированного доступа к передаваемым командам или внесения в них изменений. Как упоминалось выше, данные проблемы могут быть решены применением шифрования[32].

Таким образом, можно выделить следующие требования к рассматриваемой системе:

- Аутентификация операторов при входе в систему.
- Проверка полномочий оператора на осуществление запрошенных действий с (СДУ ДПМС).
- Аутентификация оператора перед (СДУ ДПМС).
- Аутентификация (СДУ ДПМС) перед оператором.
- Обеспечение защиты от несанкционированного доступа к каналу связи.
- Обеспечение защиты от несанкционированного внесения изменений в передаваемую по каналу связи информацию[32]

Симметричные алгоритмы шифрования используют один и тот же секретный ключ для зашифрования и расшифрования, и этот секретный ключ должны хранить в тайне все абоненты. Собственно, в основу аутентификации в этом случае положено предположение, что если секретный ключ знают только условные абоненты А и В, то либо зашифровать некоторые данные, либо расшифровать полученный шифртекст может только абонент,

посвященный в общий секрет, то есть или абонент А, или абонент В. Избежать атак, связанных, например, с перехватом злоумышленником аутентификационного сообщения и последующей попыткой злоумышленника использовать полученные зашифрованные данные для, например, внедрения в систему от имени легального пользователя, помогают метки времени, случайные числа, числовые последовательности, т.п.

В асимметричных алгоритмах один из пары ключей является открытым и может быть предоставлен всем заинтересованным сторонам, а второй – закрытым, и должен храниться в тайне от всех. В асимметричном шифровании, получив доступный всем открытый ключ пользователя, любой желающий может зашифровать информацию на этом ключе. Расшифровать же полученный шифртекст сможет только владелец второго ключа – закрытого. Именно возможность расшифровать полученный шифртекст и будет являться доказательством подлинности абонента. Электронную же подпись может поставить только владелец закрытого ключа с его помощью, а вот проверить – любой, кто возьмет доступный открытый ключ. Соответственно, именно возможность поставить электронную подпись, которую потом сможет проверить любой желающий, и является доказательством подлинности абонента. При использовании асимметричных алгоритмов для защиты от ряда атак также используются метки времени, случайные числа и т.д. Кроме того, применение асимметричной криптографии подводит еще к одной проблеме – как убедиться, что выложенный открытый ключ принадлежит именно заявленному пользователю? Один из наиболее распространённых подходов – это использование некоторой независимой доверенной третьей стороны, которая сможет гарантировать принадлежность открытого ключа абонента. В качестве этой третьей стороны может выступать удостоверяющей центр, создающий так называемые цифровые сертификаты, представляющие собой фактически открытый ключ абонента, подписанный электронной подписью удостоверяющего центра.

Для аутентификации традиционно используется логин и многоразовый пароль пользователя, однако данная схема имеет целый ряд недостатков, начиная от проблем хранения и заканчивая проблемами передачи паролей. Более безопасный подход предполагает применение одноразовых паролей или аутентификацию на основе цифровых сертификатов.

Задачи защиты от несанкционированного доступа к передаваемой информации и защиты от внесения изменений в нее решаются прежде всего шифрованием передаваемой информации. Шифрование осуществляется симметричным алгоритмом шифрования, что требует знания обоими абонентами (ДУМС и оператора) одного секретного ключа. Секретный ключ, применяемый для шифрования сеанса связи, называется сеансовым, и должен меняться как минимум от сеанса к сеансу. Это накладывает требования по получению данного ключа обоими абонентами до начала сеанса связи. Существует большое количество криптографических протоколов распределения ключей, однако в целях уменьшения объема передаваемых служебных данных и в целях своевременной доставки сеансовых ключей обоим абонентам наибольший интерес представляет протокол аутентификации, совмещенный с протоколом распределения ключей. Своевременность доставки ключей означает отсутствие ситуаций, когда один из абонентов уже ключ шифрования имеет и высылает зашифрованную на нем информацию другому абоненту, а тот еще ключ шифрования не получил[33].

Примером такого совмещенного протокола является протокол Kerberos (изначально описан в стандарте RFC 1510). Kerberos прошел многочисленные исследования на тему поиска уязвимостей, и в настоящее время считается одним из лучших решений при построении схем типа SSO – Single Sign-On – схем однократного входа с авторизацией, позволяющих пользователям всего один раз проходить аутентификацию при входе в систему, но получать доступ ко всем необходимым сервисам сети. Достоинством Kerberos (5 версии) является также гибкость при выборе

алгоритма шифрования и возможность использовать различные виды аутентификаторов пользователей (смарт-карты, USB-токены, одноразовые пароли (OTP токены) и так далее[33].

Kerberos является трехсторонним протоколом, т.е. в процессе аутентификации участвуют пользователь (клиент), сервер аутентификации Kerberos и собственно требуемый клиенту сервер (сервис, служба). Классический Kerberos основан на одном из упоминавшихся выше видов аутентификации – аутентификации на основе симметричного шифрования, т.е. подлинность участников аутентификации доказывается знанием ими общего для обоих сторон секретного ключа, выдаваемого сервером Kerberos. Участники протокола Kerberos по умолчанию работают в незащищенной среде, и поэтому на всех этапах протокола не обмениваются никакой конфиденциальной информацией в незащищенном виде, все данные шифруются и не могут быть прочитаны или изменены злоумышленником[33].

Обмен данными происходит по принципу клиент-сервер, причем все рабочие станции пользователей и все сервера сети оснащаются клиентской частью Kerberos, а сервер Kerberos может быть установлен либо на одном компьютере, либо разнесен по нескольким. Так или иначе, сервер Kerberos должен быть хорошо защищен с точки зрения информационной безопасности, т.к. именно на безопасности и доверенности этого сервера и держится безопасность всей системы в целом. Сервер Kerberos называют также KDC – Key Distribution Center, центр распределения ключей. В дальнейшем будем называть оператора «пользователь», если надо будет подчеркнуть участие человека в каких-либо процедурах, или «клиент», если необходимые действия выполняются клиентской программой без непосредственного участия человека. Простым «сервером» сети, с которым необходимо будет связаться клиенту, же фактически выступает (СДУ ДПМС), выполняющий команды оператора.

В классическом протоколе Kerberos подразумевается использование двух серверов – сервера аутентификации и сервера выдачи билетов. Сервер аутентификации (Authentication server, AS) позволяет подтвердить подлинность клиента при первом же входе пользователя в систему. Если аутентификация прошла успешно, сервер аутентификации выдает клиенту так называемый билет (ticket, иногда переводят как мандат, разрешение) на получение билетов, с которым клиент будет обращаться на сервер выдачи билетов (TGS, Ticket-Granting Server) каждый раз, когда ему надо будет связаться с новым сервером сети. Возникает вопрос, не является ли избыточным такое количество защищенных серверов Kerberos, и можно ли просто возложить обязанности по выдаче билетов на работу с различными серверами сети на сервер аутентификации. Делать так в общем случае нежелательно, так как протокол Kerberos требует использования долговременного мастер-ключа пользователя собственно при прохождении аутентификации пользователя. Мастер-ключ генерируется на основе пароля пользователя, и при частом использовании надо либо постоянно держать в памяти устройства собственно мастер-ключ, либо постоянно запрашивать пароль у пользователя для генерации мастер-ключа в случае необходимости. Соответственно, использование значения мастер-ключа при работе с обычными серверами сети существенно увеличивает риск его компрометации. Традиционное решение подобных проблем – создание временных сеансовых ключей, действительных только в течение определенного периода времени, чем, собственно, и занимается сервер выдачи билетов. Следовательно, разделение службы аутентификации пользователя в системе и службы получения разрешений на доступ к серверам сети позволяет повысить уровень защищенности всей системы в целом. В 5 версии протокола Kerberos в ряде случаев возможно использовать сервер аутентификации для выдачи билетов, но злоупотреблять этой возможностью не следует.

В общем случае, любой билет в Kerberos содержит в себе идентификаторы тех, кто хочет установить между собой связь, и сеансовый ключ для этой связи. Содержащаяся в билете информация зашифрована на ключе того сервера, которому предназначена, и это шифрование с одной стороны, защитит содержимое от несанкционированного доступа, а с другой стороны – позволит аутентифицировать как отправителя (если он смог зашифровать, значит, знает общий секрет и является тем, за кого себя выдает), так и получателя (если расшифровал и получил передаваемый сеансовый ключ, значит, опять-таки знает общий секрет и является тем, за кого себя выдает).

Билет на выдачу билетов, соответственно, является своеобразным подтверждением подлинности пользователя для получения доступа к сетевым ресурсам, так как создается сервером аутентификации Kerberos для сервера выдачи билетов Kerberos (т.е. в доверенной защищенной среде для доверенной защищенной среды). Зашифрован он на секретном ключе, общем для этих двух серверов, что, как и в случае обычного билета, служит одновременно и для подтверждения подлинности абонента, и для защиты от несанкционированного доступа. Даже если данный билет на выдачу билетов будет перехвачен злоумышленником, прочитать содержащуюся в нем информацию он не сможет, а для защиты от атак, когда злоумышленник, выдавая себя за легального пользователя, может попытаться использовать перехваченный билет на выдачу билетов для получения доступа в сеть (атаки воспроизведением), применяются такие дополнительные средства, как указание срока действия билета, адрес пользователя, и т.д. Клиент будет каждый раз при необходимости обратиться к новому серверу сети предъявлять билет на выдачу билетов серверу выдачи билетов Kerberos. При этом, так как обращения к серверу аутентификации не происходит, пользователю не надо будет каждый раз проходить процедуру аутентификации – наличие билета на выдачу билетов косвенно подтверждает

успешное прохождение проверки на подлинность клиентом на первом этапе протокола Kerberos.

Помимо билетов, в протоколе Kerberos вводится понятие аутентификаторов клиентов. Аутентификатор клиента в общем случае содержит в себе идентификатор клиента и временную метку, зашифрован на сеансовом ключе клиента и сервера, передаваемом в билете, и имеет очень небольшой срок действия (для противодействия атакам воспроизведения). Аутентификатор генерируется самим клиентом. Его основное назначение – подтверждение того, что предъявитель билета и тот, кому этот билет был выдан – одно и тоже лицо.

Упрощенная схема работы протокола Kerberos показана на рисунке 17.

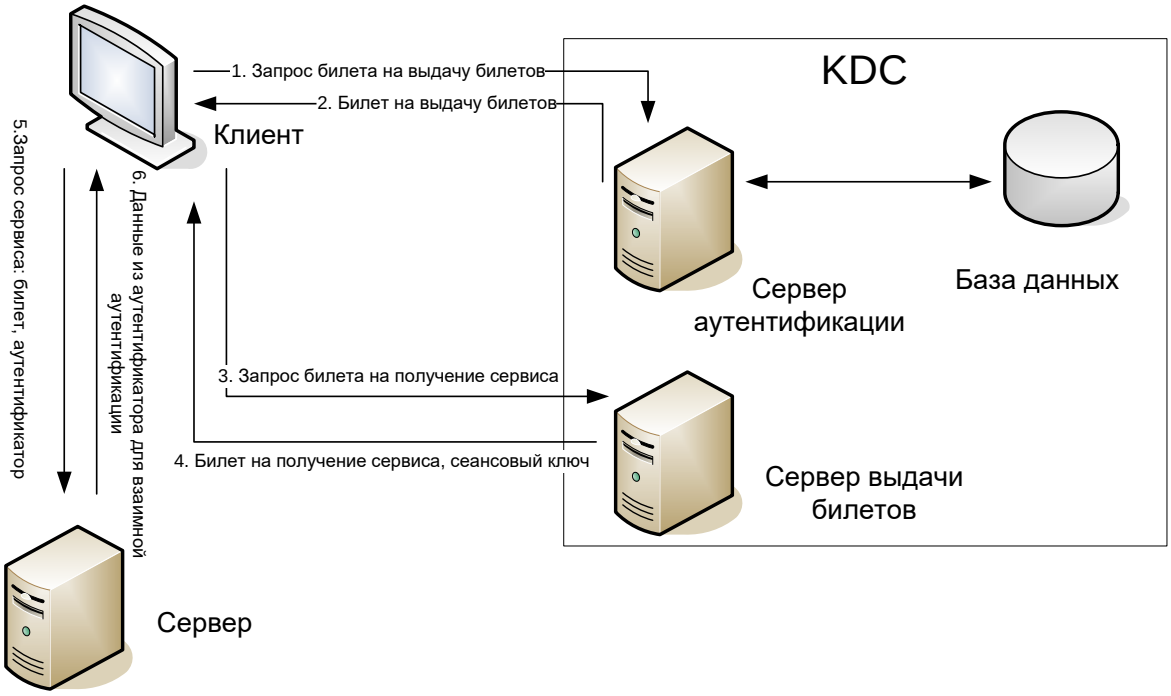


Рисунок 17 – Упрощенная схема протокола Kerberos

Таким образом, протокол Kerberos можно условно разделить на три основные этапа:

1) Аутентификация пользователя в системе.

2) Получение пользователем возможности доступа к необходимым сервисам.

3) Доступ пользователя к необходимым сервисам.

За первые два пункта отвечают специальные сервера Kerberos, реализация последнего пункта возлагается на самого пользователя с учетом данных, полученных на втором этапе.

1) Сервер аутентификации

Пользователь использует свой аутентификатор (пароль, токен, цифровой сертификат, т.д.) для входа в систему. На основании значения аутентификатора клиент генерирует мастер-ключ пользователя, которым будет в дальнейшем зашифрован сеансовый ключ для работы с сервером выдачи билетов. Далее

Шаг 1.

Клиент запрашивает билет на получение билета. Для этого клиент высылает серверу аутентификации следующее сообщение:

{Опции || ID_C || *Область клиента* || ID_{TGS} || *Период действия* || *Случайное значение*$_1$*},*

где Опции – флаги, которые могут включаться в билет. Например, в начальном запросе могут стоять флаги, сигнализирующие о необходимости предварительной аутентификации, возможном перенаправлении и т.д.

ID_C - идентификатор клиента. Идентифицирует пользователя перед сервером аутентификации;

ID_{TGS} - идентификатор сервера выдачи билетов. Обозначает для сервера аутентификации, с кем хочет связаться клиент.

Область (realm) – сеть, использующая протокол Kerberos, состоящая из серверов KDC и множества клиентов и серверов сети. Сети различных административных подразделений организации обычно образуют различные области. Клиент и сервер из разных областей могут связываться между собой при условии, что их сервера KDC являются доверенными друг для друга, для чего они должны иметь общие секретные ключи.

Период действия – в общем случае время начала и окончания действия билета, а также крайний срок для возобновления действия билета (если в процессе работы понадобиться продлить его срок действия).

Случайное значение – защита от атаки воспроизведения. Сервер аутентификации должен будет на следующем шаге вернуть это число, чтобы доказать, что это не злоумышленник направляет клиенту перехваченное ранее сообщение, а настоящий сервер аутентификации выслал ему соответствующие данные.

Следует обратить внимание, что никаких конфиденциальных данных типа значения пароля клиент не пересылает. Кроме того, клиент не посылает вообще никаких аутентифицирующих себя данных (только свой идентификатор). Фактически сессия начинается с запроса клиента с указанием сервиса, который он хочет получить.

Шаг 2.

Получив сообщение клиента, сервер аутентификации проверяет в своей базе данных наличие клиента с указанным идентификатором. Если все в порядке, сервер аутентификации высылает клиенту билет на выдачу билетов для доступа на сервер выдачи билетов:

{Область клиента || ID_C || $Билет_{TGS}$ ||

|| $E_{Kc}[K_{C,TGS}$|| *Период действия* || $Случайное\ значение_1$|| $Область_{TGS}$ || $ID_{TGS}]$ *}*

где $Билет_{TGS} = E_{KTGS}$[Флаги || $K_{C,TGS}$ || Область клиента || ID_C || AD_C || Период действия]

E_{Kc} – шифрование на мастер-ключе К клиента С. Данный секретный ключ является общим для сервера аутентификации и клиента и в общем случае создается из значения аутентификатора пользователя (пароля, некоторого секретного значения, т.д.). Как упоминалось выше, для защиты от атаки воспроизведения сервер аутентификации возвращает в данном зашифрованном сообщении полученное на предыдущем шаге случайное значение.

Область$_{TGS}$ – так как в общем случае клиент и запрашиваемый им сервер могут находиться в разных областях, то их область явно указывается в сообщении.

Билет$_{TGS}$ - билет на выдачу билетов, предназначенный для пересылки на сервер выдачи билетов. Клиент или злоумышленник не смогут получить доступ к содержимому билета, так как он зашифрован секретным ключом, известным только серверу аутентификации и серверу выдачи билетов.

AD_C – адрес клиента. Нужен для предотвращения использования билета с рабочей станции, отличной от той, с которой билет был запрошен. Часто используется для проверки совпадения с адресом, включенным в билет, как часть аутентификации собственно билета.

E_{KTGS} – шифрование на долговременном секретном ключе К сервера выдачи билетов TGS. Данный ключ является общим для сервера аутентификации и сервера выдачи билетов.

$K_{C,TGS}$ – временный сеансовый секретный ключ, сгенерированный сервером аутентификации для клиента С и сервера выдачи билетов TGS. Каждая копия ключа передается в зашифрованном виде в сообщениях, предназначенных, соответственно, для клиента и для сервера. Даже если злоумышленник получит каким-либо образом доступ к содержимому одного из данных сообщений, второе он все равно ни модифицировать, ни прочитать не сможет, так как оно будет зашифровано на совершенно другом секретном ключе.

Крайне важным для протокола Kerberos является значение Периода действия. Значения времени на всех компьютерах всех участников протокола должны быть синхронизированы, и жёсткость данного требования – одно из немногих неудобств Kerberos.

Следует отметить, что в сообщении сервера аутентификации присутствует также информация в открытом виде – это полученные на предыдущем этапе область клиента и идентификатора клиента. Эти данные конфиденциальными не являются и служат лишь подтверждением получения

их из сообщения клиента на первом этапе и одновременно указанием, для кого предназначен передаваемый билет на выдачу билетов.

Доказательством успешного прохождения аутентификации служит то, что клиент сможет расшифровать предназначенную ему часть сообщения, зашифрованную на ключе, полученном из его пароля, и примет участие в дальнейших шагах протокола Kerberos.

Для усиления безопасности рекомендуется использовать так называемую «предварительную аутентификацию». Если сервер KDC настроен на предварительную аутентификацию, то после получения указанного в пункте 1 запроса клиента сервер аутентификации потребует у клиента перед шагом 2 аутентифицировать себя. Например, выслать серверу аутентификации случайное значение и метку времени, зашифрованные мастер-ключом пользователя. Если клиент сможет выслать подобное сообщение и после расшифровки сервером аутентификации данный сервер устроит значение метки времени, этап предварительной аутентификации признается успешным и начинается выполнение шага 2. Вместо метки времени в различных реализациях Kerberos могут использоваться одноразовые пароли, генерируемые на токеном или смарт-картой на основе пароля пользователя и т.д.

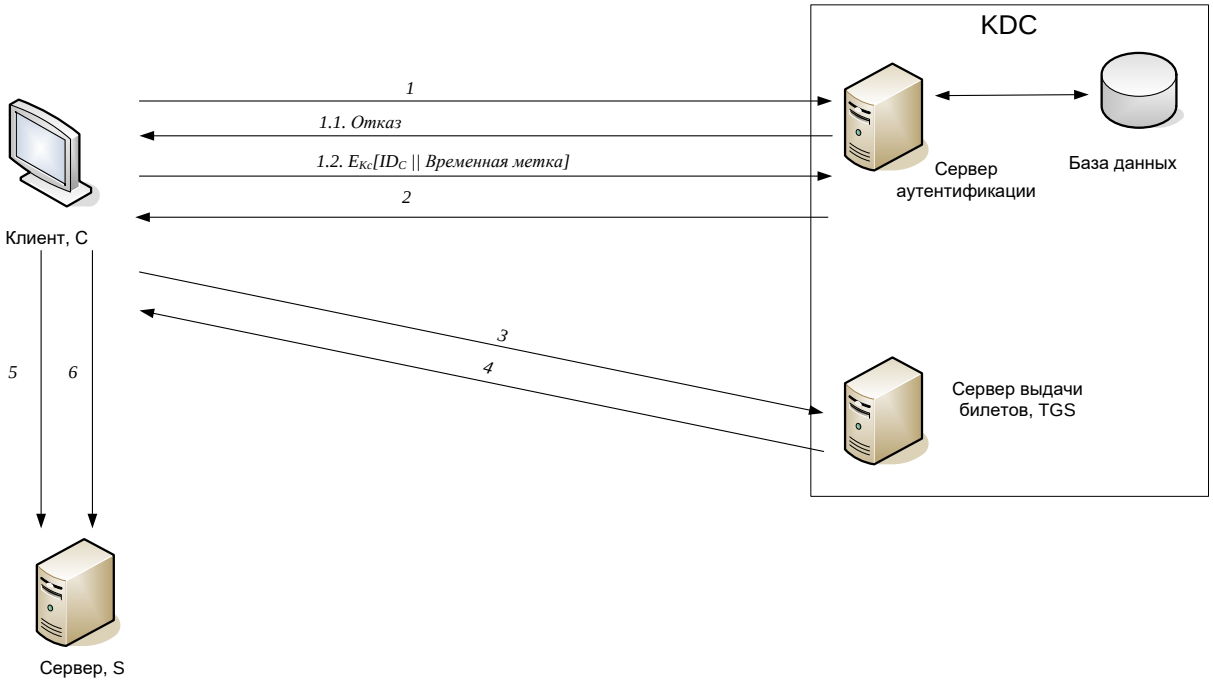


Рисунок 18 – Протокол Kerberos с вариантом предварительной аутентификации по метке времени

2) Сервер выдачи билетов

Получив сообщение от сервера аутентификации, клиент расшифровывает предназначенную ему информацию (т.е. ту, которая зашифрована на его секретном мастер-ключе) и получает таким образом $[K_{C,TGS}$|| Период действия || Случайное значение$_1$|| Область$_{TGS}$ || $ID_{TGS}]$.

Наибольший интерес для клиента здесь представляет $K_{C,TGS}$ – временный сеансовый ключ для связи с сервером выдачи билетов. Остальные расшифрованные поля либо нужны для еще одного уточнения, для соединения с кем данный ключ предназначен – идентификатор сервера выдачи билетов и область данного сервера, либо нужны для защиты от разнообразных угроз – период действия и случайное число.

Шаг 3.

Клиент, определившись с необходимым ему сервером сети, хочет получить возможность с ним связаться. Для этого клиент обращается к серверу выдачи билетов с просьбой предоставить ему данные, необходимые

для установления связи. Эти данные должны, с одной стороны, аутентифицировать клиента перед сервером сети, а с другой – содержать сеансовый ключ для данного соединения. Соответственно, клиент посылает на сервер выдачи билетов следующее сообщение:

{Опции || ID_S || *Период действия* || $Случайное\ значение_2$ || $Билет_{TGS}$ ||
|| *Аутентификатор клиента}*

где Опции – клиент запрашивает установку необходимых ему флагов в будущем билете;

ID_S – идентификатор того сервера сети, с которым клиент хочет установить соединение;

Период действия – клиент запрашивает для будущего билета для соединения с сервером сети срок действия: начало, окончание, срок для возможного продления действия будущего билета;

Случайное значение – случайное число, которое в дальнейшем послужит для защиты от атаки воспроизведением;

$Билет_{TGS}$ – билет на выдачу билетов, полученный на шаге 2 от сервера аутентификации. Так как он зашифрован на секретном ключе, который знает только сервер аутентификации и сервер выдачи билетов, то доступ к содержимому этого билета имеют только они, клиент же всего лишь пересылает некоторый зашифрованный пакет, прочитать или модифицировать который ни он, ни потенциальный злоумышленник не смогут. Билет на выдачу билетов служит для подтверждения успешной аутентификации клиента перед сервером выдачи билетов и подразумевает многократное использование в рамках период действия, чтобы пользователю не приходилось каждый раз проходить аутентификацию на сервере аутентификации, когда необходимо будет получить доступ к различным серверам и сервисам сети.

Аутентификатор клиента формируется самим клиентом для подтверждения своей подлинности перед тем, кому аутентификатор высылается, то есть аутентификатор фактически подтверждает подлинность

билета. Идея основана на том, что аутентификатор шифруется на общем сеансовом секретном ключе клиента и второго абонента, чтобы получить который клиенту понадобилось расшифровать сообщение соответствующего сервера KDC. Если он смог это сделать, извлек сеансовый ключ и, соответственно, затем им воспользовался, значит, тем самым он подтвердил свою подлинность. В данном случае, аутентификатор зашифрован на сеансовом секретном ключе клиента и сервера выдачи билетов.

Аутентификатор клиента = $E_{KC,TGS}$[ID_C || Область клиента || Метка времени].

Аутентификатор, как уже говорилось, имеет крайне ограниченный срок действия, поэтому наличие метки времени и синхронизация времени по всей сети Kerberos позволяют противостоять атакам воспроизведения.

Шаг 4.

Сервер выдачи билетов расшифровывает информацию, содержащуюся в пришедшем от клиента билете на выдачу билетов, т.е получает

[Флаги || $K_{C,TGS}$ || Область клиента || ID_C || AD_C || Период действия],

то есть все данные по клиенту, который к нему обращается.

Соответственно, после извлечения сеансового ключа $K_{C,TGS}$, сервер выдачи билетов сможет расшифровать аутентификатор и получить [ID_C || Область клиента || Метка времени].

Безусловно, идентификатор клиента из билета и идентификатор клиента из аутентификатора должны совпасть, а метка времени – уложиться в указанный интервал в Периоде действия (в противном случае сервер выдачи билетов посчитает пришедшее сообщение недействительным). Сервер также сверяет период действия билета для выдачи билетов с текущим временем.

Кроме того, сервер выдачи билетов по поступившим данным клиента проверяет, имеет ли он вообще право на доступ к запрашиваемому серверу.

После все проверок, сервер выдачи билетов создаст сеансовый секретный ключ для связи между клиентом и запрошенным им сервером S и

вышлет клиенту и этот сеансовый ключ в зашифрованном виде, и билет, предназначенный для передачи данного сеансового ключа указанному серверу:

{Область клиента || ID_C || $Билет_S$ ||

|| $E_{KC,TGS}[K_{C,S}$|| *Период действия* || $Случайное\ значение_2$ || *Область S* || $ID_S]\}$

где $Билет_S = E_{KS}$[Флаги || $K_{C,S}$ || Область клиента || ID_C|| AD_C|| Период действия]

Сообщение шага 4 имеет по сути ту же структуру, что и шага 2. В нем содержится билет, предназначенный для передачи серверу S, и зашифрованный на мастер-ключе сервера. В билете содержится сеансовый ключ $K_{C,S}$ для предоставления возможности защищенного обмена данными между клиентом и сервером при отсутствии общего постоянного ключа, срок действия данного билета, а также данные о клиенте, который хочет связаться с сервером (его идентификатор, сетевой адрес, область). Все упомянутые данные о клиенте сервер выдачи билетов берет из того билета для выдачи билетов, что прислал ему клиент на предыдущем шаге, и в дальнейшем получатель билета будет их сверять с теми, которые будут в аутентификаторе. Так как билет шифруется мастер-ключом сервера, который, естественно, знают и серверы KDC (но они, собственно, билет и формируют), то этим гарантируется его подлинность и неизменность.

Билет имеет ту же структуру, что и билет на выдачу билетов, и может быть использован многократно в рамках указанного срока действия. Тем самым клиент избавляется от необходимости при повторном обращении к серверу вновь обращаться к серверу выдачи билетов, что снижает как нагрузку на сервер выдачи билетов, так и общий объем передаваемой по сети служебной информации.

Кроме билета, который клиент прочитать не сможет и в дальнейшем передаст в неизменном виде на сервер, сервер выдачи билетов направит клиенту уже ему предназначенный экземпляр сеансового ключа для связи с сервером $K_{C,S}$, а также срок действия данного ключа, данные о сервере, с

которым клиент хочет установить соединение (его идентификатор и область), и случайное число, которое клиент прислал в незашифрованном виде на сервер выдачи билетов на шаге 3. Вся эта информация будет зашифрована на переданном в билете на выдачу билетов сеансовым ключом для связи между клиентом и сервером выдачи билетов $K_{C,TGS}$. Возврат случайного числа в зашифрованном сообщении нужен, чтобы клиент убедился, что данное сообщение является ответом на сообщение с шага 3, а не результатом повторной пересылки злоумышленником перехваченного ранее аналогичного сообщения.

Может возникнуть вопрос, почему обязанность передать серверу билет возлагается на клиента, почему это не может сделать сам сервер выдачи билетов. Разработчики Kerberos пошли именно по этому пути, чтобы гарантировать отсутствие ситуаций, когда клиент уже получил и обработал свой сеансовый ключ и пытается связаться с сервером, а до того сообщение от сервера выдачи билетов с его экземпляром сеансового ключа еще не дошло. В данном же случае служба KDC, отправив клиенту и информацию для него, и сообщение для сервера, снимает с себя обязанности по отслеживанию дальнейшей судьбы выданного билета.

Передаваемые в незашифрованном виде область клиента и его идентификатор нужны для правильной адресации передаваемого сообщения.

3) Аутентификация клиент/сервер

После получения сообщения от сервера выдачи билетов, клиент с помощью сеансового ключа $K_{C,TGS}$ расшифровывает следующее:

[$K_{C,S}$|| Период действия || Случайное значение$_2$ || Область S || ID_S].

Таким образом, он получает сеансовый ключ для создания защищённого соединения с сервером с определенным сроком действия, данные об этом сервере, для подтверждения предназначения ключа, а также случайное число, для подтверждения, что информация, содержащаяся в данном сообщении, является ответом на запрос данного клиента с шага 3.

Кроме той информации, которую клиент может расшифровать и использовать, в сообщении сервера выдачи билетов содержится также информация, доступа к которой у клиента нет, и которая предназначена, чтобы клиент переслал ее на соответствующий сервер, - $Билет_S$. Значение Период действия из расшифрованной клиентом части сообщения и Периода действия из билета (т.е. фактически срок действия билета) совпадают.

Шаг 5.

Получив всю необходимую для обращения на сервер информацию, клиент генерирует свой аутентификатор и высылает серверу следующее сообщение, сигнализируя о желании установить соединение:

Опции || $Билет_S$ || *Аутентификатор клиента*

где Аутентификатор клиента = $E_{KC,V}$[ID_C|| Область клиента|| Метка времени || Подключ || Порядковый номер]

Билет позволит серверу убедиться, что клиент был проверен и разрешение на допуск к серверу получил, а аутентификатор позволит убедиться в подлинности билета. Следует только еще раз подчеркнуть, что клиент будет каждый раз генерировать новый аутентификатор из-за краткосрочности его действия. Аутентификатор шифруется клиентом на сеансовом ключе $K_{C,S}$, полученном от сервера выдачи билетов на шаге 4.

Следует отметить, что в 5 версии протокола Kerberos клиент может запросить взаимную аутентификацию у сервера, а также вводятся поля сообщения Подключ и Порядковый номер, при этом вариант организации соединения с сервером из другой области представлен на рисунке 20.

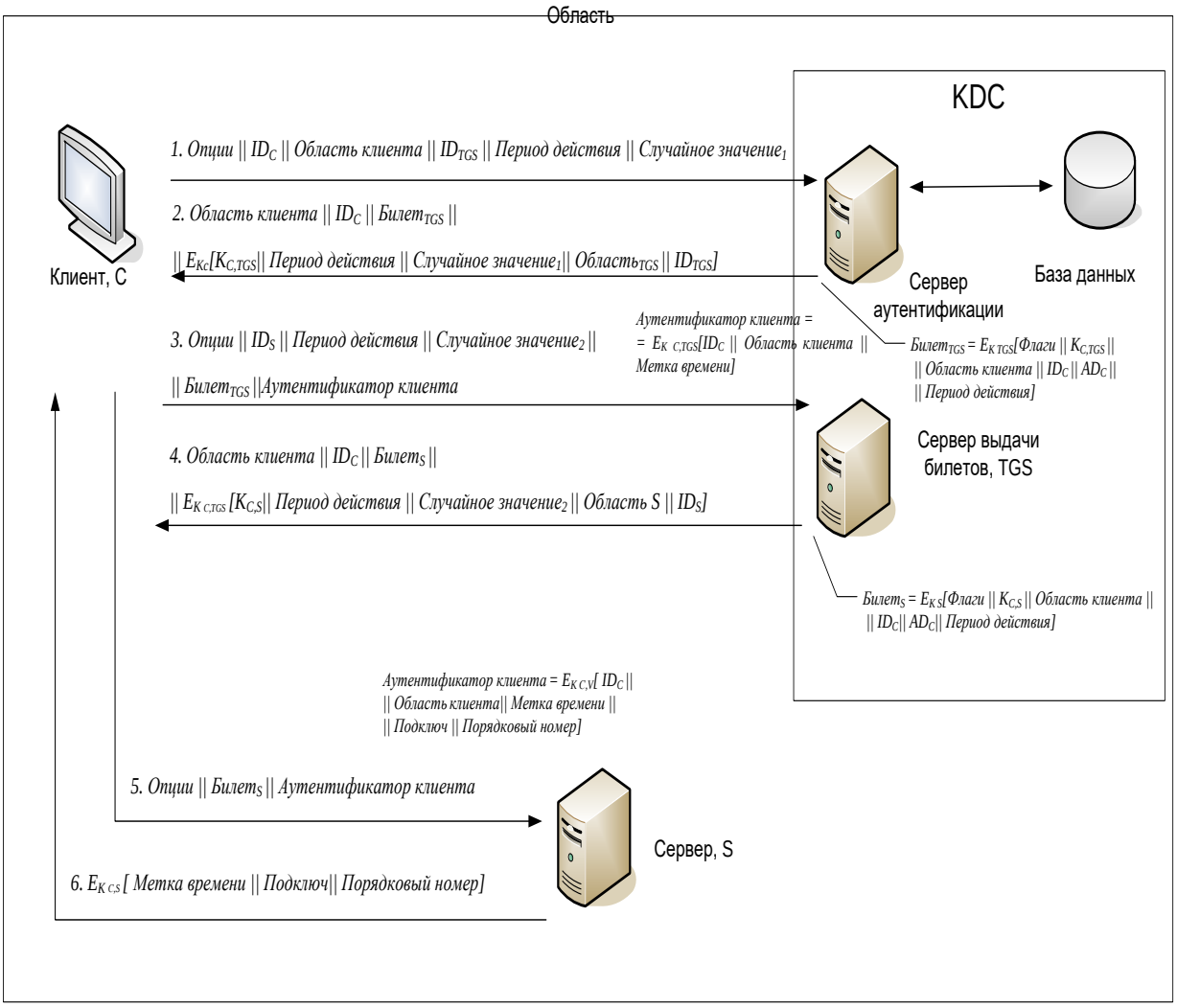


Рисунок 19 – Сообщения протокола Kerberos v5

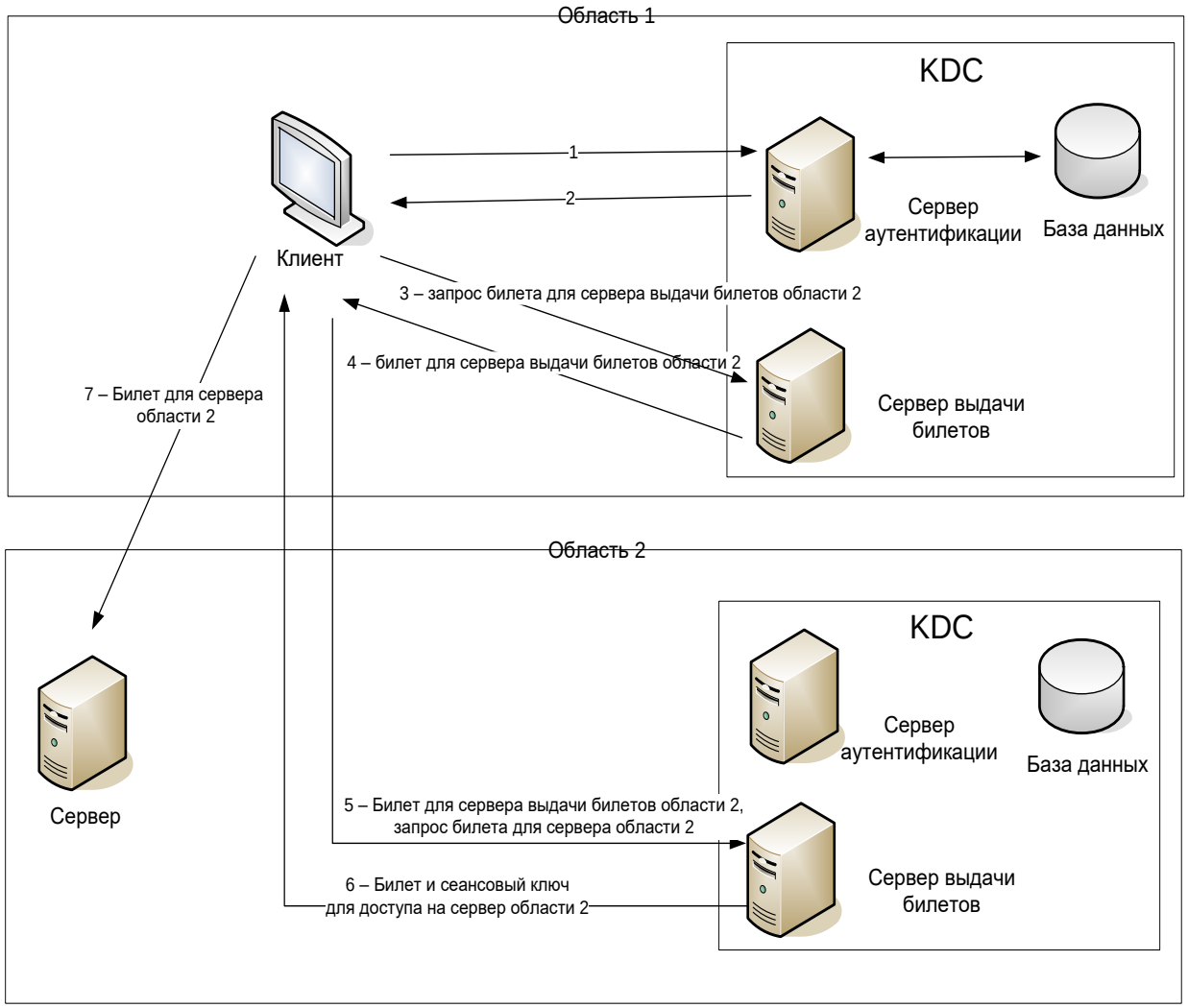


Рисунок 20 – Вариант организации соединения с сервером из другой области

Подключ. Если данное поле не используется, Kerberos будет применять сеансовый ключ билета $K_{C,S}$ для защиты всех сеансов связи по данному билету (а если на одном билете будет несколько сеансов связи, ведь он многократного использования? Злоумышленник может перехватить сообщения старого сеанса и предъявить его клиенту или серверу). Если же в данном поле будет некоторое другое значение, то именно это значение будет использовано в качестве сеансового ключа для конкретного сеанса работы, и, соответственно, для следующего сеанса работы по текущему билету должен будет сгенерирован другой сеансовый подключ.

Порядковый номер. Данное поле также является необязательным. Если оно присутствует, то тем самым указывается начальный порядковый номер, который должен применяться сервером для нумерации сообщений, посылаемых клиенту в ходе данного сеанса. Нумерация сообщений поможет в быстром обнаружении атаки воспроизведения[16].

Шаг 6.

Сервер, получив данное сообщение, в первую очередь расшифрует билет (так как знает ключ, на котором билет зашифрован). В результате он получит следующую информацию

Флаги || $K_{C,S}$ || Область клиента || ID_C|| AD_C|| Период действия.

Соответственно, после расшифровки серверу будет доступен сеансовый ключ $K_{C,S}$ для шифрования канала связи между клиентом сервером, время действия данного билета, данные о клиенте, включающие в себя идентификатор клиента, его адрес и область клиента.

Получив сеансовый ключ, сервер сможет расшифровать значение аутентификатора и получить

ID_C|| Область клиента|| Метка времени || Подключ || Порядковый номер

Далее сервер сверит данные о клиенте из аутентификатора и из билета, а также проверит допустимость метки времени аутентификатора. Если все проверки прошли успешно, то проводится процедура второй части взаимной аутентификации, т.е. теперь сервер должен аутентифицировать себя перед клиентом. Для этого он высылает клиенту следующее сообщение:

$E_{KC,S}$ *[Метка времени || Подключ|| Порядковый номер]*

Данное сообщение зашифровано на сеансовом ключе $K_{C,S}$, и содержит метку времени из аутентификатора, значение подключа для данного сеанса связи (если оно задается, конечно) и начальный порядковый номер, который должен использовать клиент для своих сообщений.

Следует отметить, что сервер, как правило, не хранит долговременно сеансовые ключи для связи с клиентом – эта обязанность возложена на клиента. Именно клиент будет направлять билет с сеансовым ключом на

сервер всякий раз, когда захочет с ним связаться (в пределах периода действия, конечно, потом надо будет либо продлять срок действия билета, либо обращаться на сервер выдачи билетов за новым билетом). Как правило, срок действия билетов не превышает 8 часов – продолжительности рабочего дня. При выходе пользователя из системы, все соответствующие аутентификаторы и билеты уничтожаются.

Реализации протокола Kerberos

Полное описание протокола Kerberos приведено в спецификациях RFC 4120 (5 версия Kerberos) [17]. Описания некоторых аспектов применения Kerberos и работы с ним описаны в таких спецификациях, как RFC 4121, RFC 3961 и других. Соответственно, существует достаточно большое количество реализованных версий протокола Kerberos, которые могут отличаться как по условиям распространения (свободно распространяемые, реализованные в коммерческих продуктах), так и по особенностям реализации.

Так, к свободно распространяемыми относятся MIT Kerberos, Heimdal Kerberos (реализации для Linux), а к коммерческим реализациям – ОС Windows, которая начиная с Windows 2000 применяет Kerberos в качестве механизма доменной аутентификации.

Возможные атаки на Kerberos и способы защиты от них [18]

Атака воспроизведением со старыми ключами. Цель: попытка выдать себя за другого пользователя. Общая идея атаки: злоумышленник пересылает серверу ранее перехваченные билет и сообщения клиента, которые были зашифрованы сеансовым ключом из билета. Решение: использование сеансовых подключей или, если это невозможно, посылка сервером клиенту запроса, который потребует зашифрованного на сеансовом ключе ответа, зависящего от данных клиента.

Автономный взлом и воспроизведение. Цель: повторное использование билета. Общая идея атаки: Злоумышленник автономно взламывает сеансовый ключ и использует его для повторного применения соответствующего билета. Решение: временная метка, используемая в

сообщениях протокола Kerberos, что позволяет обнаруживать попытки повторного использования билетов.

Автономный взлом мастер-ключа. Цель: выдать себя за легального пользователя для доступа к сервисам сети. Общая идея атаки: Злоумышленник запрашивает билеты от имени жертвы и использует их для взлома мастер-ключа методом грубой силы. Решение: предаутентификация, когда при попытке запроса к серверу аутентификации или серверу выдачи билетов клиент должен предоставлять аутентификационные данные.

Поддельное изменение времени. Цель: сделать устаревшие билеты действующими. Общая идея атаки: злоумышленник посылает серверу запрос с поддельным временем суток, чтобы заставить его изменить время на системных часах. Решение: сообщения о времени должны аутентифицироваться.

Восстановление или модификация закрытых данных. Цель: заставить жертву принять поддельный сессионный ключ. Общая идея атаки: злоумышленник перехватывает запрос клиента KDC и возвращает другой набор ключей, которые ему неизвестны. Решение: включение случайных чисел в запросы и ответы KDC.

Как видно из приведенных примеров атак на Kerberos, наиболее часто встречается угроза перехвата злоумышленником некоторой легальной информации и последующей попыткой пересылки этой информации для тех или иных целей, т.е. разновидности атаки воспроизведением. Соответственно, в Kerberos учитываются существующие угрозы и в протокол вносятся дополнения. Так в 4 версии не было ни предаутентификации, ни подключей, ни возможности выбора алгоритма шифрования. Все это появилось в 5 версии, и, наряду с традиционными методами противодействия – случайными числами, метками времени – прекрасно решает задачу безопасности протокола Kerberos. Существенную угрозу для Kerberos может представлять фактически только рассинхронизация часов на серверах KDC, клиентах и серверах, сервисах и т.д. сети. Можно утверждать, что протокол

Kerberos будет выполнять свои защитные функции до тех пор, пока системные часы всех участников Kerberos будет синхронизованы.

2.3 Концепция СДУ ДПМС

Основным свойством СУДС или АСУ ДС в соответствие с требованиями IMO и MAMC является способность взаимодействовать с судоходством и осуществлять ответные воздействия на судоходные ситуации.

При использовании в акватории портов судов или объектов, реализованных на основе беспилотных технологий, необходимо принимать во внимание, что операторы таких судов или объектов, а также лица, ответственные за их безаварийную эксплуатацию, должны в обязательном порядке проходить соответствующую подготовку с последующей аттестацией. Указанная необходимость обусловлена тем, что эксплуатация судов должна осуществляться лицами, прошедшими подготовку в специализированных учебных заведениях с последующим дипломированием в квалификационной комиссии при Администрации порта. Кроме того, необходимо учитывать статью Гражданского кодекса №1079 «Ответственность за вред, причиненный деятельностью, создающей повышенную опасность для окружающих». Только в таком случае представляется возможным обеспечить в акватории порта достаточный уровень безопасности судоходства при эксплуатации судов или объектов, строящихся на применение беспилотных технологий.

Алгоритм подготовки операторов для безэкипажных судов или объектов, а также лица, ответственного за их безаварийную эксплуатацию, показан на рисунке 21.

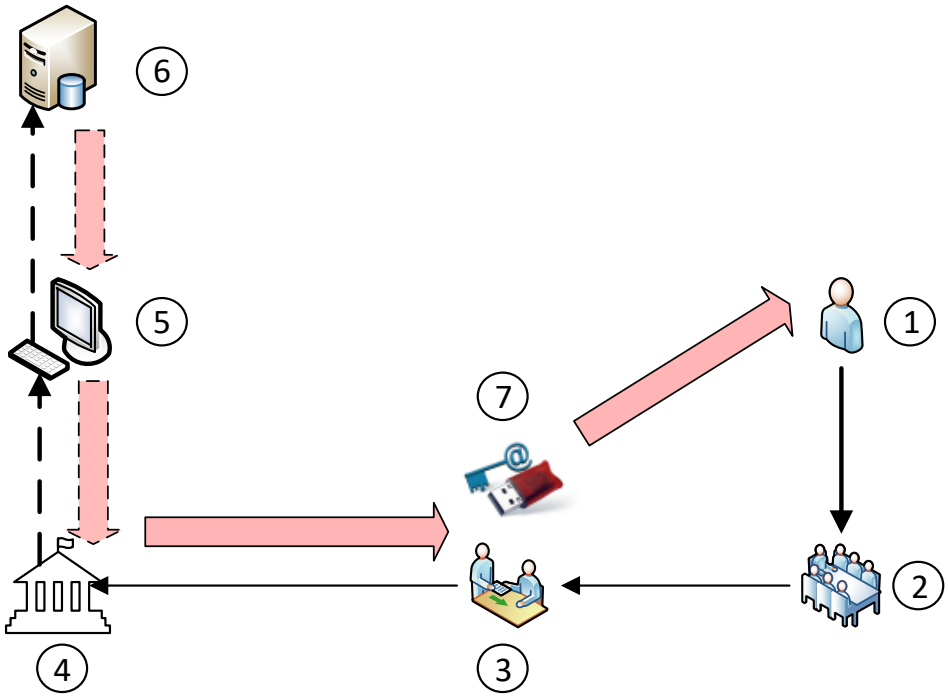


Рисунок 21 - Алгоритм подготовки операторов для безэкипажных судов или объектов, а также лица, ответственного за их безаварийную эксплуатацию

Реализовывать алгоритм предполагается следующим образом: потенциальный оператор или лицо, ответственное за безопасную эксплуатацию судна или объекта, строящегося на основе беспилотных технологий «1» должен обратиться в профильную образовательную организацию высшего профессионального образования, реализующую данный вид подготовки по программе, согласованной с Федеральным агентством морского и речного транспорта «2». После прохождения подготовки должна проводиться аттестация «3». Результаты аттестации должны передаваться в отраслевую организацию, являющуюся системным интегратором транспортной и информационной безопасности «4». Указанная организация должна осуществлять формирование и ведение базы данных операторов и лиц, ответственных за безопасную эксплуатацию судов или объектов, строящихся на основе беспилотных технологий «5» и «6». Далее будет формироваться уникальный электронный ключ «7», использование которого позволит сформировать процедуру контроля и учета безэкипажных роботизированных объектов и судов[34].

Учет и контроль безэкипажных роботизированных объектов и судов может быть реализован на основе алгоритма, показанного на рисунке 23. Здесь оператор или лицо, ответственное за безопасную эксплуатацию судов или объектов, строящихся на основе беспилотных технологий «1» подключает свой уникальный электронный ключ к устройству мониторинга, которое размещается на борту безэкипажного роботизированного объекта или судна «2». Указанное устройство по каналу связи «3» начинает передавать данные уникального электронного ключа, которые в дальнейшем поступают на сервер «4», расположенный в отраслевой организации, являющейся системным интегратором транспортной и информационной безопасности «5», где происходит идентификация оператора «1». Если идентификация оператора прошла успешно, тогда отправляется сообщение в систему управления движением судов (СУДС) «6»[34].

В рассматриваемом алгоритме одна из значимых ролей отведена каналу передачи данных между устройством мониторинга, размещенном на борту контролируемого объекта, и сервером отраслевой организации, являющейся системным интегратором транспортной и информационной безопасности[34]. С точки зрения удобства передачи данных конструктивным представляется использовать для данной цели канал связи, предоставляемый государственной автоматизированной информационной системой «ЭРА-ГЛОНАСС» (ГАИС «ЭРА-ГЛОНАСС»). Это согласуется с законодательством Российской Федерации, а именно п.5.1 Федерального закона от 28 декабря 2013 г. № 395-ФЗ «О ГАИС «ЭРА-ГЛОНАСС»: «Создание в сфере транспорта и в иных сферах, определенных Правительством Российской Федерации, государственных информационных систем, а также информационных систем, входящих в состав объектов концессионных соглашений, при функционировании которых предполагается использование навигационной информации, осуществляется в соответствии с законодательством Российской Федерации и на основе обязательного использования информационного ресурса, и программно-технических

средств, и технологической инфраструктуры системы в создаваемой информационной системе при наличии технической возможности такого использования». Так как разрабатываемая система является информационной и предполагает непосредственное использование навигационной информации, то она подпадает под действие указанного закона.

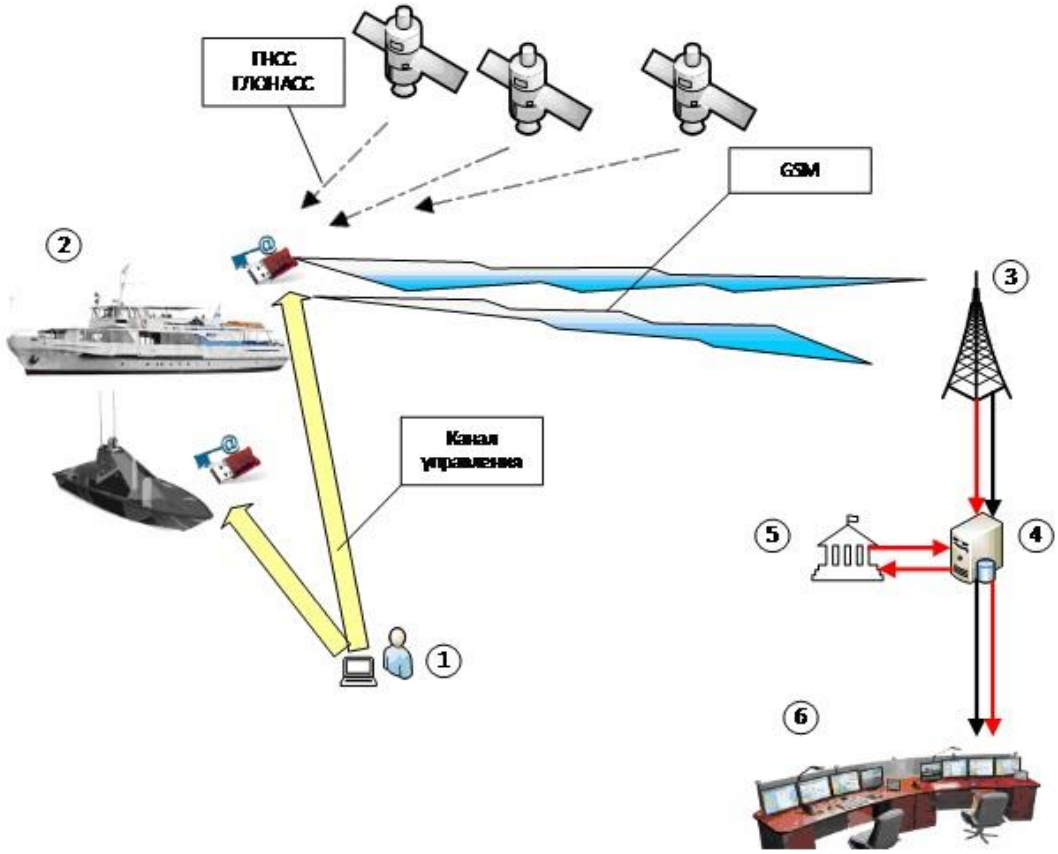


Рисунок 22 - Алгоритм учета и контроля безэкипажных роботизированных объектов и судов

Одновременно, необходимо отметить, что использование ресурса ГАИС ЭРА-ГЛОНАСС тем более оправдано технически, так как подразумевает передачу данных по каналу связи сотового оператора, чей сигнал обладает лучшими характеристиками приема в указанном районе (технология MVNO), а главное, при данной реализации отсутствует зависимость от частного лица, которым является оператор сотовой связи, так как АО «ГЛОНАСС», управляющее ГАИС «ЭРА-ГЛОНАСС» и предоставляющее услугу передачи данных, является АО с государственным участием (контрольный пакет у Правительства России).

Устройство мониторинга будет представлять собой блок, совмещенный с модулем «ЭРА-ГЛОНАСС», таким образом совместно с данными уникального электронного ключа будут передаваться сообщения, содержащие информацию о положении устройства мониторинга, вырабатываемые по сигналам ГНСС ГЛОНАСС/GPS.

Отраслевая организация, являющаяся системным интегратором транспортной и информационной безопасности, на основании полученных данных позиционирования и электронного ключа принимает решение о регионе использования безэкипажного роботизированного объекта или судна. Если будет выявлено, что такое судно или объект эксплуатируется в зоне ответственности СУДС или АСУ ДС, тогда данные мониторинга и информация об операторе должна быть незамедлительно перенаправлена в соответствующий СУДС. В таком случае СУДС будет проинформирован об использовании безэкипажного роботизированного объекта или судна в зоне своей ответственности. В случае выявленных нарушений оператор СУДС получит возможность связаться с оператором безэкипажного роботизированного объекта или судна так как контактная информация должна содержаться в сообщении от системного интегратора транспортной и информационной безопасности «5». Кроме того, оператор СУДС должен получить возможность фиксации нарушений оператором безэкипажного роботизированного объекта или судна с последующей их регистрацией в базе данных системного интегратора транспортной и информационной безопасности. При наличии значительного количества выявленных нарушений у оператора безэкипажного роботизированного объекта или судна, действие его уникального электронного ключа должно быть остановлено до последующей внеочередного обучения и аттестации оператора.

Разрабатываемая СДУ ДПМС реализует процесс контроля и дистанционного пилотирования безэкипажного морского буксира,

осуществляющего проводку по акватории порта и швартовку крупнотоннажных морских судов.

Для обеспечения процесса проводки оператор должен получать информацию о параметрах движения буксира: координаты (φ,λ), курс ψ, продольную V_x и поперечную V_y составляющие скорости относительно грунта и воды, углы крена θ и дифферента γ. скорость и направление ветра, скорость и направление течения).

Для обеспечения процесса швартовки самого буксира дополнительно необходимо получать информацию отдельно о скорости носа и кормы и угловой скорости поворота ω_z.

В нашем случае, под эффективностью предлагаемого варианта построения СДУ ДПМС подразумевается, во-первых, соблюдение ограничений, накладываемых на нее вышестоящей системой АСУ ДС, исходя из целеполагания последней. В этой связи на концептуальном уровне синтеза СДУ ДПМС необходимо выбрать такой вариант ее построения, который, как минимум, не приведет к снижению безопасности судоходства в зоне ответственности АСУ ДС. Кроме того, необходимо рассмотреть такие варианты построения каналов контроля и управления СДУ ДПМС, которые не привели бы к снижению электромагнитной защищенности радиоаппаратуры, используемой в АСУ ДС, а также к перегрузке радиоканалов, используемых для управления движением в ней.

Во-вторых, обеспечение необходимой пропускной способности каналов контроля и управления и оптимальных способов взаимодействия между основными элементами СДУ ДПМС.

В-третьих, обеспечение устойчивости автоматической подсистемы управления движением ДПМС, устойчивости алгоритмов управления, а также помехоустойчивости каналов контроля и управления СДУ и наиболее оптимальное обеспечение контроля мореходных качеств судна.

Контроль мореходных качеств безэкипажного судна, являющийся обязательным условием сохранения уровня безопасности судоходства в зоне

ответственности АСУ ДС, возлагается на оператора СДУ. Для этого он по каналу контроля должен дополнительно получать углы пространственной ориентации судна и их производные: скорость изменения углов рыскания, угловую скорость бортовой ω_x и килевой качки ω_y, а также определять период рыскания и периоды бортовой и килевой качки.

Алгоритм управления ДПМС будет зависеть от режима его движения. Можно выделить три основных режима управления ДПМС: режим движения по заданной траектории (движение в точку встречи буксируемого судна и возвращение от грузового терминала к стоянке); режим буксировки и швартовки буксируемого судна; швартовка самого ДПМС.

Режим движения по заданной траектории.

Траектория движения в акватории порта задается точками поворота, соединенными прямолинейными отрезками с заданным курсом и скоростью (Рисунок 23).

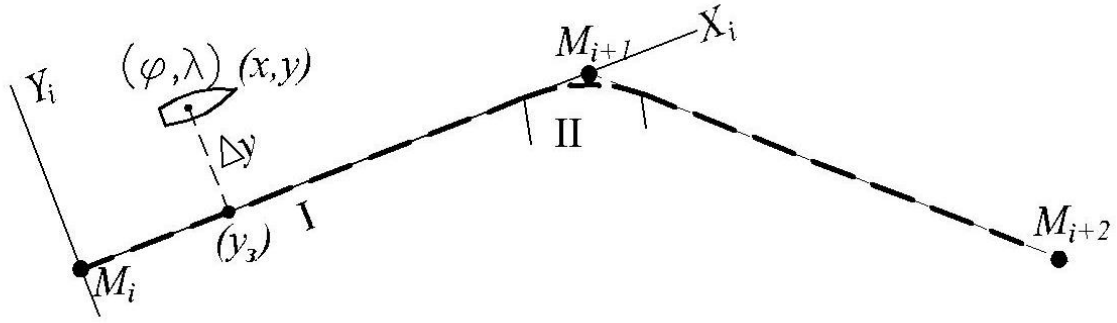


Рисунок 23 – Принцип управления движением по заданной траектории

Оператор загружает в ЭКНИС выбранный маршрут. На прямолинейном участке с помощью наложенной на электронную карту информации от НАП ГНСС и АИС, он контролирует отклонение ДПМС от маршрута и изменение его скорости под действием внешних возмущений (ветер, течение, волнение), а также движение относительно опасных целей и выдает команды на изменение оборотов винтов (n) и угла поворота винто-рулевой колонки (γ), поддерживая заданную скорость движения и курс. Эти команды на среднем уровне в блоке обработки преобразуются в сигналы

управления, поступающие в ССУОВ и ССУВРК, которые непосредственно воздействуют на ВРК и движитель. При достижении точки поворота, оператор с помощью тех же команд выводит ДПМС на новый курс и новую заданную скорость.

Режим буксировки и швартовки буксируемого судна

В этом режиме оператор СДУ с помощью тех же команд управляет ДПМС по командам от лоцмана, руководствуясь видеоизображением и данными от АИС.

Режим швартовки ДПМС

Швартовка ДПМС осуществляется с помощью системы автоматической швартовки (САШ). Так как размер электромагнитного устройства, с которым должна состыковываться ответная часть ДПМС, невелик, а его визуальное наблюдение невозможно, то при швартовке с помощью инструментальных методов точность позиционирования пятна контакта должна составлять десятки сантиметров. Для достижения подобной точности в СДУ ДПМС необходимо использовать технологию RTK.

Во всех режимах плавания ДПМС в блоке обработки информации вырабатываются значения периодов рыскания и качки, которые сравниваются с заданными. При существенных отклонениях этих параметров от заданных, свидетельствующих об ухудшении мореходности ДПМС, в блоке обработки вырабатывается дополнительный сигнал, передаваемый по каналу телеметрии на верхний уровень и вызывающий срабатывание сигнализации. При срабатывании сигнализации, оператор СДУ должен немедленно отвести ДПМС к месту стоянки и оповестить об этом лоцмана, оператора СУДС и диспетчера буксирной компании.

Команды нижнего и среднего уровня передаются по защищенным от помех каналам межприборного интерфейса RS 422 по протоколу NMEA 2000. Команды же управления и сигналы верхнего уровня передаются по радиоканалам, подверженным воздействию различных помех. Так как в акватории порта одновременно могут использоваться несколько ДПМС, то

может возникнуть проблема воздействия взаимных помех. Однако в нашем случае, при передаче узкополосных сигналов телеметрии и команд управления выделенная полоса в 10 МГц позволяет разнести информационные каналы достаточного числа ДПМС так, чтобы они не создавали помех друг другу. И даже для широкополосных видеосигналов в очень широкой гигогерцовой полосе это условие также может быть выполнено. Наибольшее влияние на радиоканалы команд управления и телеметрии будут оказывать индустриальные помехи. На рисунке 24 представлен график замеров среднего уровня помех в городском индустриальном районе. Как видно из рисунка, влияние индустриальных помех будут заметно на частотах ниже 1 ГГц. Следовательно, видеосигналы, излучаемые в диапазоне 3.5 ГГц, не будут подвержены влиянию индустриальных помех.

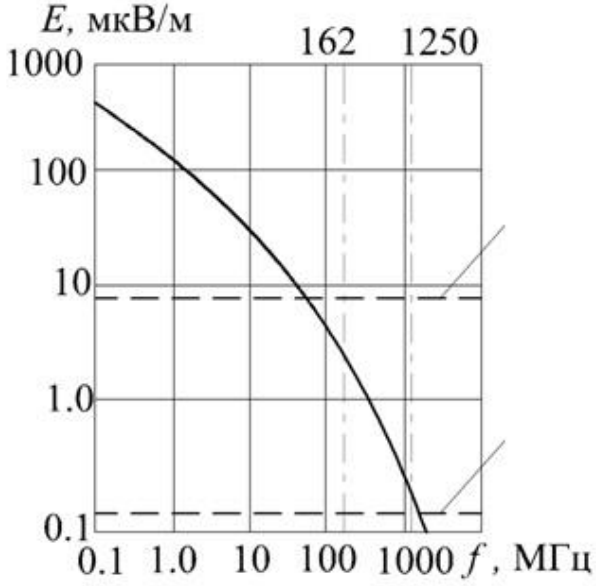


Рисунок 24 – Распределение статистических уровней напряженности поля помех по частоте

В нашем случае, в портовой зоне наиболее существенными будут помехи от контактной сети портовых кранов и от сварочных аппаратов, концентрирующихся в сухих доках. Аппаратура дуговой сварки создает помехи очень высокого уровня. Поэтому на предприятиях с интенсивным

использованием сварочной техники суммарных уровень помех достаточно высок. Так напряжённость поля на расстоянии 300 м от источника может составлять порядка 20 дБмкВ/м, убывая с увеличением расстояния со скоростью 1/R1.5. Спектр помех, возникающих при работе аппаратуры различной конструкции, очень широк. Результаты измерений, проведенных с большим числом аппаратов разной конструкции, показали наличие трёх широких резонансных полос, центры которых соответствуют частотам 750 кГц, 3 МГц и 20 МГц. Эти максимумы далеки от полосы 440-450 МГц, в которой работают информационные радиоканалы СДУ ДПМС, поэтому сварка не будет оказывать на них существенного воздействия.

Напряженность поля помех от контактной сети портового крана на расстоянии 10 м от оси пути определяется эмпирической формулой [7]:

$$E = E_0 - 11.3 \lg \frac{f}{0.15} \tag{1.1}$$

где E_0 – базовая напряженность поля помехи на частоте 0.15 МГц [дБмкВ/м]. Для портового крана E_0 = 66 дБмкВ/м.

Затухание этих помех определяется эмпирическим выражением:

$$E(r) = E_0 + 20k \lg\left(\frac{r_0}{r}\right) \tag{1.2}$$

где E – напряженность поля помехи в расчетной точке, дБмкв/м;

E_0 – напряженность поля помехи в базовой точке, дБмкв/м;

k – коэффициент затухания в поперечном направлении;

r – расстояние от оси пути до расчетной точки, м;

r_0 – расстояние от оси пути до базовой точки, м.

Для оценки влияния помех можно воспользоваться методикой, основанной на оценке вероятности ошибки поэлементного приема цифрового сообщения [8].

При отсутствии взаимной помехи вероятность ошибки $p_{ош}$ в канале с шумами будет определяться выражением:

$$p_{\text{ош}} = -0.5\exp\left[-\frac{h^2}{2}\right], \qquad (1.3)$$

где h – энергетика помехи.

Так как спектральная плотность индустриальной помехи меняется достаточно медленно, то в полосе частот узкополосного сигнала данную помеху можно рассматривать как белый гауссовский шум $\xi_к(t)$ с плотностью вероятности $\nu_{\text{к}}^2$. Тогда ее можно сложить с основным флуктуационным белым шумом с плотностью вероятности ν^2. В этом случае энергетика шумовой помехи будет определяться выражением:

$$h^2(r) = \frac{P_{\text{с}} T_{\text{с}}}{\nu_{\text{к}}^2(r) + \nu^2}, \qquad (1.4)$$

где $P_{\text{с.}}$ – мощность сигнала на входе приемника;

$T_{\text{с}}$ – длительность единичного импульса сигнала;

r – расстояние от источника помехи до приемника.

Так как спектральная плотность помехи от коронного разряда в полосе частот полезного сигнала практически постоянна, то ее величина будет определяться выражением:

$$\nu_{\text{к}}^2(r) = P_к / F, \qquad (1.5)$$

где F - полоса частот сигнала;

$P_{\text{к}}$ - мощность. помехи от контактной сети портового крана на входе приемника, определяемая по напряженности поля помехи по формуле (1.2).

Тогда помехозащищенность информационных каналов СДУ ДПМС будет определяться условием:

$$p_{\text{ош}} < p_{\text{ош.доп.}}, \qquad (1.6)$$

Величина допустимой вероятности ошибки поэлементного приема цифрового сообщения $p_{\text{ош.доп}}$ будет зависеть от количества бит информации, передаваемой по каналу в единицу времени. Так, в случае передачи 10-ти тыс. бит информации в секунду, $p_{\text{ош.доп}}$ будет равна 10^{-4}.

Окончательно величина допустимой вероятности ошибки поэлементного приема цифрового сообщения может быть получена после проектирования СДУ ДПМС на этапе НИОКР.

Операция по управлению ДПМС со стороны СДУ подразделяется на пять этапов, имеющих определенную специфику:

1) отход от причальной стенки и подход к буксируемому судну;

2) буксировка крупнотоннажного морского судна от входа в порт до грузового терминала;

3) швартовка буксируемого судна к причальной стенке грузового терминала;

4) отшвартовка буксируемого судна от причальной стенки грузового терминала;

5) подход к причальной стенке и швартовка самого ДПМС.

СДУ ДПМС относится к классу автоматизированных систем, поэтому ее функционирование происходит под управлением оператора.

На первом и пятом этапах оперативного управления ДПСМ оператор СДУ поддерживает связь только с диспетчером АСУ ДС или СУДС, получая от них разрешение на отход ДПСМ от причальной стенки и указания, связанные с безопасностью движения по акватории порта (в случае возникновения нештатных ситуаций). Кроме того, он получает задание на буксировку от диспетчера буксирной компании. При этом он осуществляет проводку ДПСМ по акватории порта, руководствуясь только соответствующими международными, национальными и местными документами и указаниями диспетчера СУДС. Для связи с диспетчером СУДС целесообразно использовать существующие международные УКВ каналы службы движения, используемые диспетчерами СУДС для связи с судами, находящимися в зоне их ответственности.

Особенностью второго этапа оперативного управления ДПСМ является то, что оператор СДУ управляет ДПСМ, руководствуясь командами лоцмана, находящегося на борту буксируемого крупнотоннажного морского судна.

При этом оператор СДУ, также как и капитан обычного буксира, несет ответственность за последствия аварийных ситуаций с участием ДПМС, которые могут возникнуть в процессе выполнения этих команд. Поэтому он обязан предпринимать все необходимые действия, чтобы этих ситуаций избежать и руководствоваться положениями соответствующих документов в случаях, если команды лоцмана им противоречат. Для связи оператора ДПСМ с лоцманом целесообразно использовать те же международные УКВ каналы портовой службы, которые используют лоцманы для связи с капитанами обычных буксиров.

Особенностью третьего этапа оперативного управления ДПСМ является то, что швартовка крупнотоннажного судна производиться не только под руководством лоцмана, но и ответственного представителя терминала (мастера погрузки), с которым оператор СДУ также должен поддерживать связь на тех же каналах, что и с лоцманом.

Важное значение для поддержания уровня безопасности судоходства на акватории порта имеет обязательная аутентификация операторов СДУ и самих ДПМС, исключающая возможность использования системы неподготовленными лицами, а также использование технически неисправных, не имеющих допуска к эксплуатации ДПМС.

Для обеспечения безопасности судоходства в акватории порта рабочее место оператора СДУ должен быть оборудовано техническим средствами для контроля не только за своим ДПМС, но и за другими судами, находящимися в акватории порта.

Для повышения безопасности буксировочных операций с использованием ДПМС целесообразно использовать систему визуализации, работающую в реальном масштабе времени.

Для передачи телеметрии (параметров движения ДПМС) в направлении ДПМС - оператор и команд управления в направлении оператор–ДПМС необходимо обеспечить надежные, помехозащищенные радиоканалы с пропускной способностью, достаточной для передачи больших объемов

информации, снимаемой с датчиков ДПМС, а также сигнала визуализации. При этом трафик ДПМС – оператор не должен создавать помех радиообмену и работе радиосистем, входящих в СУДС. Выбор конкретного частотного диапазона, конкретных схем реализации приемопередатчиков осуществляется на четвертом (элементарном) уровне анализа системы после завершения концептуальных исследований.

При буксировке крупнотоннажных морских судов, а также при их швартовке и отшвартовке, как правило используются комбинированные методы буксировки (активные и пассивные). Разрабатываемые ДПМС целесообразно использовать только для пассивного метода буксировки, когда для обеспечения маневрирования крупнотоннажного морского судна в пределах зон следования буксир осуществляет сопровождение в готовности работать на укол без подачи буксирного троса на борт буксируемого судна. Кроме того, буксировка способом «на укол» является обязательной при швартовке и отшвартовке крупнотоннажного судна согласно нормативных документов большинства портов.

Исходя из анализа требований, содержащихся в портовых нормативных документов, для построения ДПМС, осуществляющих буксировку «на укол», необходимо использовать буксиры с крыльчатым движителем или азимутальными винто-рулевыми колонками (азиподами), позволяющими буксиру разворачиваться на месте на 360^0. Мощность таких буксиров должна быть не менее 3500 л.с.

Построение СДУ ДПМС приведет к повышению безопасности при проведении буксировочных операций вследствие существенного уменьшения влияния человеческого фактора. Во-первых, вместо экипажа управление буксирами будет осуществляться береговым оператором, физическое и эмоциональное состояние которого гораздо легче контролировать. Во-вторых, используемые для создания СДУ технические средства позволят лоцману использовать графический способ указания места «укола», более

надежный и оперативный, чем голосовой, к тому же не допускающий неоднозначного толкования.

Критерием эффективности подобных систем является минимизация расходов на их создание и эксплуатацию, при обеспечении заданных технических характеристик и уровня безопасности. Поэтому предлагаемое концептуальное решение СДУ ДПМС должно удовлетворять именно этому критерию эффективности.

Благодаря отсутствию рубки, помещения для экипажа, системы жизнеобеспечения и спасательных средства, ДПМС будет более компактен и, следовательно, будет иметь лучшую управляемость по сравнению с обычным буксиром аналогичной мощности. И, несмотря на появление дополнительной «электроники», постройка его обойдется дешевле, так как стоимость электроники значительно ниже стоимости вышеперечисленных элементов, исключаемых из конструкции ДПМС.

Замена трехсменных экипажей каждого из буксиров группой дежурных операторов, численность которых будет варьироваться в соответствии с оперативным планом буксировочных работ, составляемым по заявкам морских агентов, а также снижение расхода топлива вследствие уменьшения массы ДПМС по сравнению с обычным буксиром той же мощности, приведет к существенному сокращению эксплуатационных расходов.

Исходя из вышеизложенного, на системном уровне анализа окончательно сформулируем принципы построения СДУ ДПМС, являющейся операционной подсистемой S_0-системы АСУ ДС. Исходя из рассмотренной концепции построения СДУ ДПМС, ее структура должна содержать следующие элементы (Рисунок 25):

1) рабочее место оператора, включающее в себя:

- модуль управления,
- модуль контроля,
- модуль аутентификации,
- интерфейс обмена между модулями;

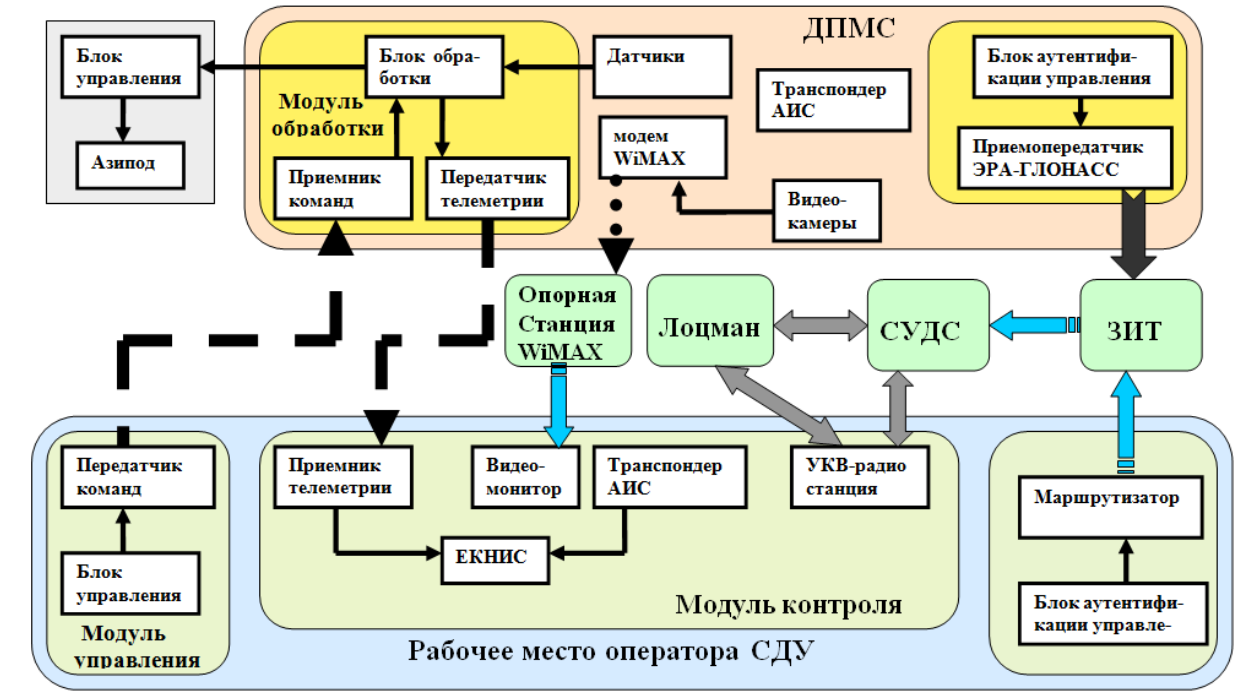
2) объект управления (ДПМС), включающий в себя:

- движительную систему,
- модуль датчиков параметров движения,
- модуль визуализации,
- модуль обработки и передачи информации,
- модуль аутентификации,
- интерфейс обмена между модулями;

3) радиоканалы связи с лоцманом, диспетчером СУДС;

4) радиоканалы визуализации, контроля и управления ДПМС;

5) каналы передачи данных электронного ключа оператора и электронного ключа ДПМС на сервер Российской системы аутентификации и контроля («ЗИТ»), а также диспетчеру СУДС.



высокоскоростные линии сети интернет;

каналы связи системы ЭРА-ГЛОНАСС

каналы WiMAX АСС;

межприборный интерфейс RS232/422/485 (NMEA 2000)

Рисунок 25 - Концептуальная структура СДУ ДПМС

Вывод:

В данной главе были рассмотрены: Эксплуатационные требования к программному обеспечению и организации обмена данными в СДУ ДПМС, Методы идентификации, аутентификации управления доступом и обеспечения целостности функционирования всей системы дистанционного управления движением морского судна, а так же была приведена концепция синтеза СДУ ДПСМ.

Глава 3 Алгоритмы определения движения ДПМС

3.1 Алгоритм получения и расчета дополнительной навигационной информации для швартовки дистанционно пилотируемого морского судна в режиме реального времени.

Швартовка ДПМС осуществляется с помощью системы автоматической швартовки (САШ). Так как размер электромагнитного устройства, с которым должна состыковываться ответная часть ДПМС, невелик, а его визуальное наблюдение невозможно, то при швартовке с помощью инструментальных методов точность позиционирования пятна контакта должна составлять несколько сантиметров. При этом оператор СДУ по каналу телеметрии, помимо координат и векторов скорости носа и кормы, а также угловой скорости поворота судна, должен дополнительно получать координаты ответной части САШ, установленной на судне, с указанной выше точностью.

Для достижения подобной точности в СДУ ДПМС необходимо использовать технологию RTK (Real Time Kinematic) – кинематика реального масштаба времени, на основе приемника спутниковой навигации GPS/ГЛОНАСС (Рисунок 26). Данная технология получила широкое распространение в геодезии, топосъемке, сельском хозяйстве при управлении автоматическими агрегатами (тракторами, комбайнами и т.д.).

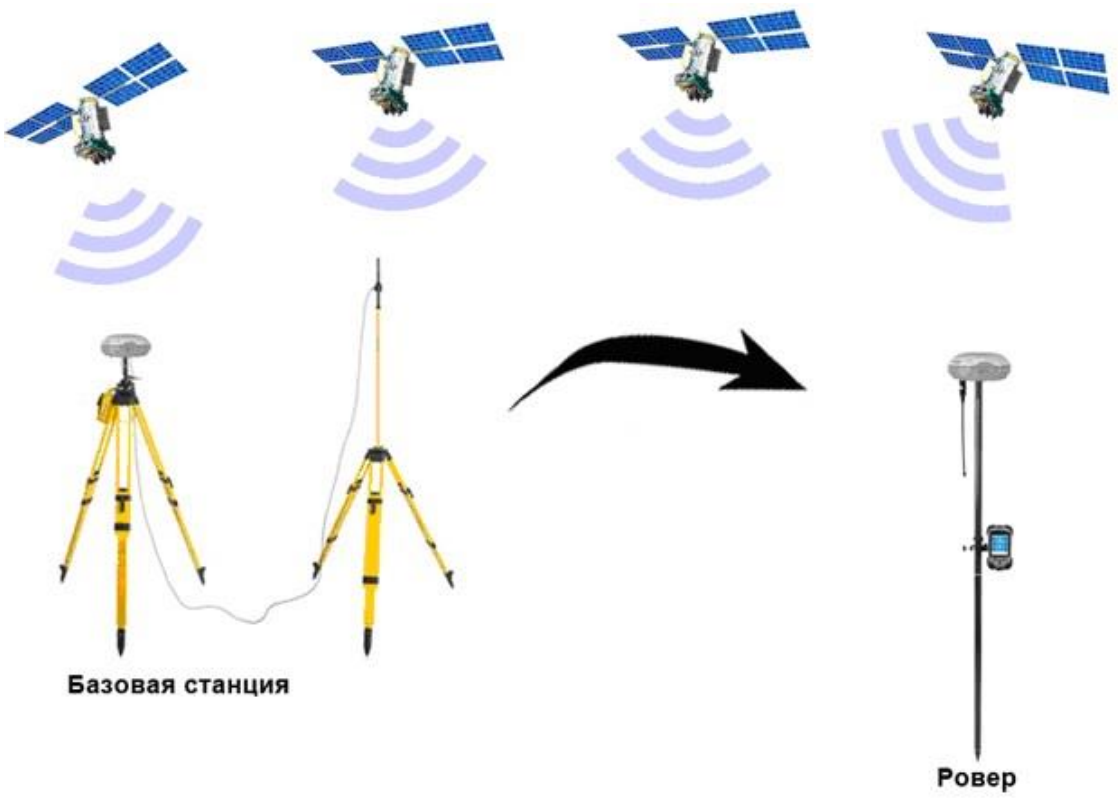


Рисунок 26 – Принцип работы технологии РТК

При использовании режима RTK, аппаратура потребителя должна состоять как минимум из двух навигационных приемников. Одним из этих приемников является базовая станция, выступающая в качестве корректирующей станции. А вторым приемником является установленный на подвижном объекте (в нашем случае на ДПМС) ровер. Базовая станция, координаты которой точно известны, вычисляет дифференциальные поправки – разности между истинными расстояниями до спутников и измеренными с помощью навигационных определений псевдодальностями, и передает эти поправки по беспроводному каналу связи на ровер подвижного объекта. Ровер учитывает принятые поправки при определении своего местоположения. Так как измерение псевдодальностей на базовой станции производится фазовым методом, то точность таких навигационных измерений может достигать нескольких сантиметров.

Ровер необходимо устанавливать на борту ДПМС непосредственно над ответной частью системы автоматической швартовки. При этом, если

ответная часть будет крепиться в районе носа, то система RTK будет обеспечивать сантиметровую точность определения координат носовой части ДПМС, что также будет иметь важное значение не только при швартовке, но и при буксировке.

Для передачи поправок используется формат RTSM SC-104 версия 3.0, включающий возможность передачи RTK-поправок. При этом скорость передачи должна составлять 2400 бит/с с задержкой не более 0.5 с.

Так как расстояние между базовой станцией и роверами ДПМС в акватории порта невелико, то они будут производить навигационные измерения по одинаковому созвездию спутников и величина геометрического фактора HDOP, непосредственно влияющего на величину ошибки позиционирования, у них будет практически одинакова. Поэтому появляется возможность передавать поправки не на величину измеренных псевдодальностей, а непосредственно поправки на координаты места судна. Для этого может использоваться сообщение RMC протокола NMEA-0183, которое содержит минимально рекомендованный набор навигационных данных. Это сообщение имеет следующую структуру:

$GPRMC,hhmmss.ss,A,llll.ll,a,yyyyy.yy,a,b.b,c.c,xxxxxx,d.d,a,e*hh<CR><LF>

Где:

- $ - начало сообщения;
- «,» - разделитель полей;
- RMC – NMEA заголовок;
- hhmmss.ss – время UTC определения координат;
- A – Статус (A – активный, V - игнорировать);
- llll.ll,a – широта (С/Ю) (например, 3716.149,N)
- yyyyy.yy,a – долгота (В/З) (например, 02242.111,E ;
- b.b – скорость относительно земли, в узлах;
- c.c – направление движения, в градусах;
- xxxxxx – дата: ддммгг;
- d.d,a – магнитное склонение, в градусах (В/З).;

- e – индикатор режима. (A – автономный, D – дифференциальный, E – экстраполяция координат, M – режим ручного ввода, S – режим симулятор, N – недостоверные данные);
- «*» - разделитель контрольной суммы;
- hh – поле контрольной суммы;
- <CR><LF> - завершающие символы.

При столь высоких требованиях к радиоканалу возникает проблема выбора надежного канала передачи. В настоящее время используются три основных способа передач RTK-поправок:

- использование УКВ-модемов, работающих на частоте 450 МГц;
- использование голосовых радиоканалов операторов сотовой связи в режиме CSD;
- использование мобильного интернета.

Использование УКВ-радиоканалов для передачи поправок в нашем случае невозможно, так как данная полоса будет занята широкополосными радиоканалами передачи телеметрии.

Недостаток технологии CSD заключается в необходимости для каждого ДПМС иметь на базовой станции отдельный дорогостоящий GSM-модем и в высокой стоимости тарифов из-за низкой востребованности данной технологии.

Поэтому наиболее оптимальным представляется метод передачи информации посредством интернета, в том числе мобильного. Данный способ связи стал основным на сегодняшний день при работе в режиме RTK как за рубежом, так и в России. Важное условие организации такой работы – наличие статического IP адреса.

При этом наиболее оптимальным решением является использование технологии APIS. В этом случае сервер со статическим адресом и специальной программой, установленной на нем, предоставляет оператор связи. База передает посредством наземного интернет-соединения поправки на данный сервер, а неограниченное количество роверов, зная IP адрес

сервера и серийный номер базы, может подключаться к ней и получать поправки для работы в режиме RTK через мобильный интернет.

Данная технология, при закупке оборудования у оператора, предоставляющего услугу по APIS, абсолютно бесплатна.

Таким образом, технология APIS обладает следующими преимуществами перед остальными:

- от одной базы может работать неограниченное количество роверов;
- минимальные затраты на оплату трафика, которым может пользоваться неограниченное количество роверов;
- отсутствие необходимости получения и оплаты статического IP адреса.
- отсутствие необходимости организовывать собственный сервера с дублированием канала для работы по технологии APIS.

3.2 Алгоритм определения навигационных элементов движения дистанционно пилотируемого морского судна

ДПМС с ВРК обладает исключительными маневренными характеристиками: может разворачиваться на месте на 360^0, двигаться боком и под любым углом к ДП. Поэтому для него возникает необходимость контролировать скорость движения не только центра тяжести, но и носа и кормы. Для определения этих параметров, как уже отмечалось выше, целесообразно использовать спутниковый компас с антенной системой на свободной базе, каковым является компас СН-5703 ОКБ Навис. При этом будут использоваться две антенные системы по три антенны в каждой, установленные на носу и корме ДПМС. Для определения составляющих скоростей объекта необходимо решить задачу определения пространственной ориентации объекта. При работе по сигналам НКА ГНСС необходимо определение углов ориентации местной системы координат, связанной с объектом (на практике часто в качестве осей местной системы

рассматриваются строительные оси объекта) относительно осей топоцентрической системы координат (ТПЦК), начало которой совпадает с началом координат местной системы. ТПЦК связана с объектом и ее центр совпадает с положением последнего. Оси ТПЦК направлены соответственно из центра объекта следующим образом: ось Y вдоль по местному меридиану, ось X дополняет систему до правой системы координат и направлена на восток по горизонтали, ось Z направлена вертикально вверх (Рисунок 27).

Связь между местной системой координат и ТПЦК описывается с помощью углов Эйлера, которыми в нашем случае являются крен, дифферент и курс.

Задача определения угловой ориентации объекта по сигналам НКА осуществляется в два этапа. На первом этапе определяются угловая ориентация местной системы координат относительно геоцентрической системы координат (ГЦСК) OXYZ, затем полученные углы ориентации в ГЦСК пересчитываются в ТПЦК $PX^1Y^1Z^1$, тем самым определяются искомые углы крена, дифферента и курса.

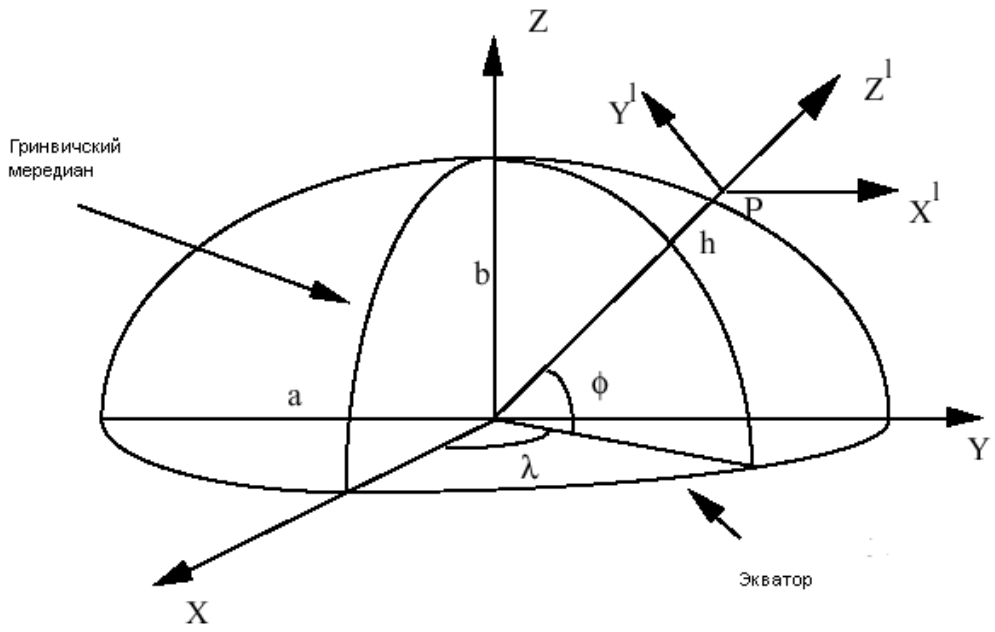


Рисунок 27 – Связь между ГЦСК и ТПЦС

В настоящее время все современные образцы навигационной аппаратуры потребителей (НАП) используют интерферометрический

(фазовый) принцип измерения угловых координат. Интерферометрический принцип определения направления на источник сигнала основывается на том, что разность фаз сигналов $\Delta\rho$, принимаемых антеннами, разнесенными на расстояние $\left|\vec{b}_{AB}\right|$, пропорциональна косинусу угла α между базой интерферометра и направлением на НКА (Рисунок 28).

$$\Delta\rho = \frac{2\pi}{\lambda} \cdot \left|\vec{b}_{AB}\right| \cdot \cos\alpha, \qquad (1.7)$$

Поскольку интервал однозначного определения фазы равен (-π,π), измерения разности фаз в интерферометре являются однозначными только при длине базовой линии (расстоянии между антеннами $\left|\vec{b}_{AB}\right| \le \lambda / 2$).

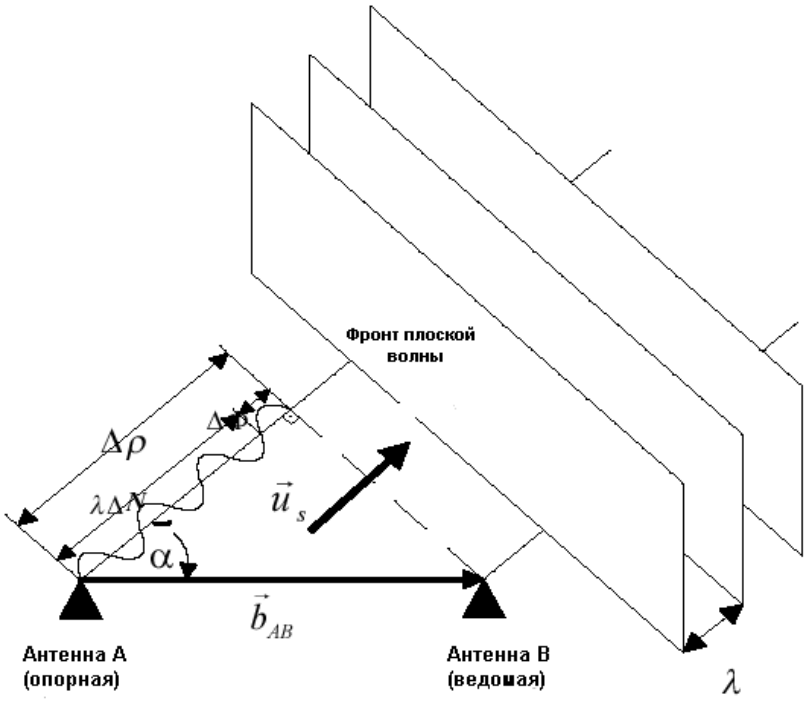


Рисунок 28 – Радиоинтерферометрический принцип решения задачи угловой ориентации объекта по сигналам ГНСС

В общем случае косинус угла между базой интерферометра и направлением на НКА и измеряемая интерферометром разность фаз сигнала в разнесенных антеннах связаны соотношением:

$$\cos\alpha = \frac{\lambda}{\left|b_{AB}\right|} \cdot \left(\Delta N + \frac{\Delta\rho}{2\pi} \right), \qquad (1.8)$$

где ΔN - неизвестное целое число циклов фазы несущей частот НКА;

$\Delta\rho$ - измеренный фазовый сдвиг, лежащий в пределах $0 \le \Delta\rho \le 2\pi$.

Поэтому для решения задачи необходимым этапом является процедура разрешения (устранения) неоднозначностей фазовых измерений для каждого из используемых НКА.

Поскольку в результате решения задачи относительных определений, проекции базовых линий интерферометра определены в прямоугольной геоцентрической системе координат, то для решения задачи пространственной ориентации, необходимо проекции базовых линии перевести в ТПЦК. Переход от геоцентрической системы координат в ТПЦК осуществляется с помощью матрицы перехода:

$$\begin{bmatrix} Y \\ X \\ Z \end{bmatrix} = \begin{bmatrix} -\sin\phi\cdot\cos\lambda & \cos\phi\cdot\sin\lambda & \cos\lambda \\ \sin\lambda & \cos\lambda & 0 \\ \cos\phi\cdot\cos\lambda & \sin\phi\cdot\cos\lambda & \sin\lambda \end{bmatrix} \cdot \begin{bmatrix} X_Г \\ Y_Г \\ Z_Г \end{bmatrix}, \qquad (1.9)$$

где $X_Т = \begin{bmatrix} Y & X & Z \end{bmatrix}^T$ – вектор в ТПЦК;

$\begin{bmatrix} X_Г & Y_Г & Z_Г \end{bmatrix}^T$ – вектор, заданный в ГЦСК;

λ, φ –значения широты и долготы соответствующие началу отсчета ТПЦК и системы координат связанной с объектом.

Курс объекта может быть определен из выражений (1.7–1.9), как угол между направлением одной из базовых линий антенной системы, направленной вдоль ДП, и осью ТПЦК, совпадающей с плоскостью истинного меридиана. Составляющие скорости объекта определяются по изменению координат выбранной точки (носа, кормы, центра тяжести) вдоль соответствующей оси за единицу времени. Проекции скорости по двум осям местной системы координат, лежащим в плоскости горизонта (при отсутствии крена, дифферента и качки), будут определяться выражениями:

$$V_x = \frac{\Delta x}{\Delta t}; V_y = \frac{\Delta y}{\Delta t}. \quad (1.10)$$

Расположении осей базовых линий антенной системы вдоль осей местной системы координат позволит определять продольные и поперечные составляющие векторов скорости носа и кормы ДПМС в системе координат, связанной с судном (Рисунок 29).

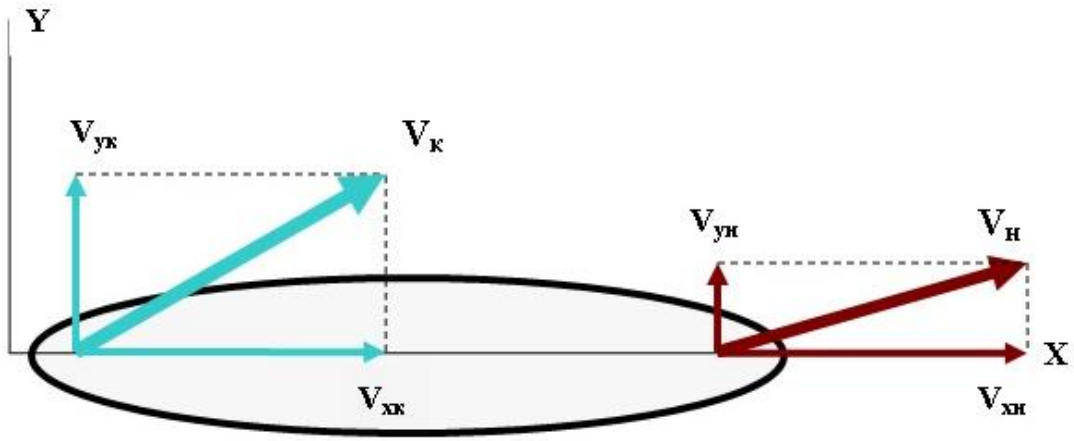


Рисунок 29 – Вектора скоростей носа и кормы ДПМС в местной системе

В данной системе координат ось *x* связана с ДП судна, а ось *y* проходит в плоскости поперечного сечения. Как видно из рисунка, ДПМС одновременно совершает линейное движение со сносом и вращением. Спутниковый компас с двумя антенными системами будет выдавать значения продольной и поперечной составляющих скорости для носа ($V_{хн}$, $V_{ун}$) и кормы ($V_{хк}$, $V_{ук}$) в местной системе координат. При этом $V_{хн} = V_{хк}$.

Тогда суммарный вектор скорости носа или кормы будет определяться в блоке обработки по формуле:

$$V_{н(к)} = \sqrt{V_{хн}^2 + V_{ун(к)}^2}, \quad (1.11)$$

Однако при движении по маршруту также необходимо знать составляющие скорости, путевой угол и угол сноса центра тяжести судна в географической системе координат. Переход к ТПЦК иллюстрируется рисунком 30.

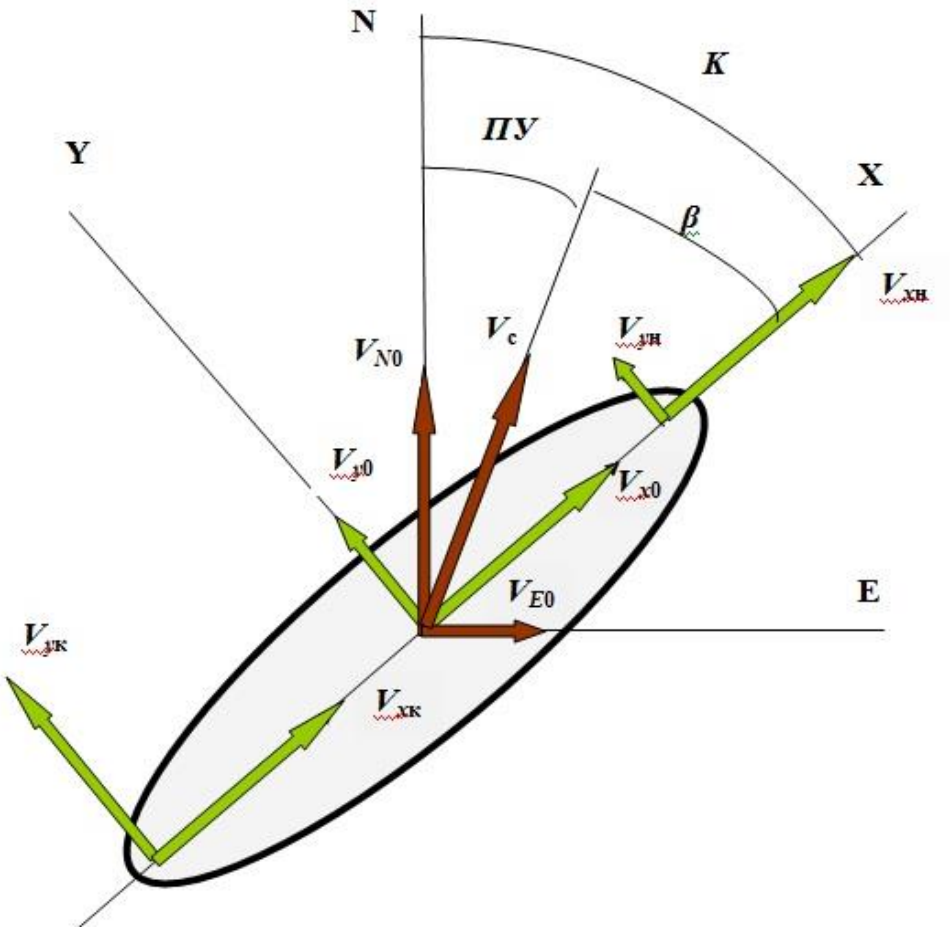


Рисунок 30 – Скорость ДПМС в географической системе координат

Если центр тяжести судна лежит на оси симметрии горизонтального сечения, то поперечная составляющая скорости будет равна:

$$V_{y0} = (V_{yн} + V_{yк}) / 2, \tag{1.12}$$

При этом также будет выполняться условие: $V_{xн} = V_{x0}$.

Тогда скорость ДПМС будет определяться выражением (1.11), только вместо составляющих скоростей носа и кормы в местной системе координат подставляем составляющие скорости центра тяжести судна. Угол сноса ДПМС (β) находим из уравнения:

$$\beta = arctg\left(\frac{V_{y0}}{V_{x0}}\right), \tag{1.13}$$

Отсюда находим путевой угол (ПУ) по формуле:

$$ПУ = К + \beta. \tag{1.14}$$

При этом положительный угол сноса отсчитывается от ДП в сторону правого борта. А курс вычисляется в спутниковом компасе относительно базовой оси системы антенн, направленной вдоль ДП с учетом матрицы преобразований (1.9), дающей направление истинного меридиана.

Тогда, зная путевой угол, можно определить составляющие скорости центра тяжести судна в географической системе координат, необходимые для обеспечения проводки судна с помощью ЭКНИС. Как видно из рисунка 1.19, северная и восточная составляющие скорости судна будут определяться выражениями:

$$V_N = V_c \cos ПУ; \quad V_E = V_c \sin ПУ . \qquad (1.15)$$

Вывод:

В данной главе были представлены: алгоритм получения и расчета дополнительной навигационной информации для швартовки безэкипажных судов в режиме реального времени, алгоритм определения навигационных элементов движения дистанционно пилотируемого морского судна с использованием сигналов ГЛОНАСС.

Заключение

Современный уровень развития технической и научной базы позволяет начать работы по конструированию систем безэкипажного судовождения.

Исходя из необходимости увеличения эффективности работ по процессам проводки и швартовки судов в портовой зоне, целесообразно сконцентрировать научный интерес на данном направлении.

Успешная реализация проекта по созданию системы управления движением безэкипажных судов в условиях порта для выше обозначенных целей приведет к значительному росту эффективности и увеличению уровня безаварийности.

Целью данной работы являлось исследование алгоритма получения дополнительной навигационной информации для швартовки безэкипажных судов в режиме реального времени.

В ходе данной дипломной работы были выполнены следующие задачи:

- Рассмотрены классификации безэкипажных судов
- Произведен обзор спутниковых навигационных приборов
- Рассмотрена структурная схема СДУ ДПМС
- Исследован алгоритм получения и расчёта дополнительной навигационной информации для швартовки ДПМС в режиме реального времени

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Першиц Р.Я. Управляемость и управление судном. — Л.: Судостроение, 1983. — 272 с.
2. Снопков В.И. Технология перевозки грузов морем. — СПб.: Научное издательство и комплекс цифровой печати «Профессионал», 2005. — 560 с.
3. Снопков В.И. Управление судном. — СПб.: Научное издательство и комплекс цифровой печати «Профессионал», 2004. — 536 с.
4. Международный сервис морского и внутреннего водного транспорта “Инмарин” https://inmarin.ru/press-centr?id=332600 (дата обращения 14.04.2021)
5. Положения по классификации морских автономных и дистанционно управляемых надводных судов (МАНС) НД № 2-030101-037 Санкт - Петербург 2020
6. Борисова А.Ю., Смаль А.В. Анализ разработок современных бесплатформенных инерциальных навигационных систем // Инженерный вестник. — 2017. — № 5. — С. 50—57.
7. ГОСТ 29205-91 Совместимость технических средств электромагнитная. Радиопомехи индустриальные от электротранспорта. Нормы и методы испытаний. — М.: Изд-во стандартов, 1993. — 8 с.
8. Шахнов С.Ф. Помехозащищенность и устойчивость радиолиний речных дифференциальных подсистем ГНСС ГЛОНАСС/GPS: монография. — СПб.: Изд-во Политехн. ун-та, 2015. — 170 с.
9. Антонович К.М. Использование спутниковых радионавигационных систем в геодезии в 2 т. — Т. 2. — М.: ФГУП «Картгеоцентр», 2006. — 360 с.
10. Меерович В.Д., Долгий И.Д. Стохастическая фильтрация навигационных параметров подвижных объектов с использованием комплексирования спутниковых и трекерных измерений // Известия

высших учебных заведений. Северо-Кавказский регион. Серия: Технические науки. — 2015. — № 1 (182). — С. 19—26.

11. Кульнев В., Михайлов С. Анализ направлений и состояния разработок функциональных дополнений к спутниковым радионавигационным системам // Беспроводные технологии. — 2006. — № 4. — С. 61—69.
12. Ведякова А.О. Идентификация в условиях внешнего возмущения с использованием нейронных сетей // International Journal of Open Information Technologies. — 2014. — Т. 2. — № 3. — С. 18—22.
13. Сазонов А.Е., Дерябин В.В. Прогнозирование траектории движения судна при помощи нейронной сети // Вестник Государственного университета морского и речного флота имени адмирала С.О. Макарова. — 2013. — № 3 (22). — С. 6—13.
14. Дерябин В. В. Нейросетевые системы прогноза скорости дрейфа судна // Вестник Государственного университета морского и речного флота имени адмирала С.О. Макарова. — 2015. — № 5 (33). — С. 7–14.
15. Дерябин В.В. Прогноз счислимых координат судна на основе нейронных сетей // Транспортное дело России. — 2015. — № 4. — С. 159—165.
16. Столлингс В. Основы защиты сетей. Приложения и стандарты: пер. с англ. — М.: Издательский дом «Вильямс», 2002. — 432 с.
17. RFC 4120 The Kerberos Network Authentication Service (V5). — URL: https://tools.ietf.org/html/rfc4120 (дата обращения 12.05.2021)
18. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А.А Афанасьев, Л.Т. Веденьев, А.А.Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. — М.: Горячая линия–Телеком, 2009. — 552 с.
19. RFC 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). — URL: https://tools.ietf.org/html/rfc4556#section-3.2.3.1 (дата обращения 17.05.2021)

20. Басс Л., Клементс П., Кацман Р. Архитектура программного обеспечения на практике. — СПб.: Питер, 2002. — 576 с.
21. О'Лири Д. ERP системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение, эксплуатация. — М.: ООО «Вершина», 2004. — 272 с
22. Постановление Правительства РФ от 15 июля 2006 г. №439-23. «Об утверждении Таблицы распределения полос частот между радиослужбами Российской Федерации». — М.: Минсвязи, 2006. — 187 с.
23. Касти Дж. Большие системы. Связность, сложность и катастрофы: пер. с англ. — М.: Мир, 1982. — 216 с.
24. Квейд Э. Анализ сложных систем: пер. с англ. — М.: Сов. радио, 1979. — 519с.
25. Авдуевский В.С. Надежность и эффективность в технике: Справочник в 10-ти томах. — Т. 3 «Эффективность технических систем». — М.: Машиностроение, 1988. — 328 с.
26. Венцель Е.С. Исследование операций: задачи, принципы, методология: монография. — М.: Наука, 1988. — 208 с.
27. Автоматизированные системы мониторинга судоходства / А.Н. Маринич, И.Г. Проценко, В.Ю. Резников и др.; Под общ. ред. Ю.М. Устинова. — СПб.: Судостроение, 2003. — 245 с.
28. Буцанец А.А Задача экспериментального исследования позиционирования корпуса судна для информационных систем.
29. Сикарев И.А. Гаранин А.В. Общие принципы построения систем управления движением дистанционно пилотируемого морского судна в портовой зоне на базе сетевого протокола NMEA-2000.
30. Вовченко Н.В. Роль Электронных информационных систем в развитии средств навигации.
31. Буцанец А.А. Разработка предложений по типовой структуре системы дистанционного управления беспилотным техническим флотом.

32. Сикарев И.А. Киселевич Г.В. Гаранин А.В. Методы аутентификации при построении системы дистанционно управления и мониторинга безэкипажных судов.
33. Сикарев И.А. Киселевич Г.В. Гаранин А.В. Предотвращение угрозы информационной безопасности с помощью применения протокола KERBEROS при организации системы удаленного управления судном.
34. Каретников В.В Бекряшев В.А Чистяков Г.Б Использование функционала ГАИС “ЭРА-ГЛОНАСС” для нужд маломерного флота и беспилотных судов.