ISSN 2949-3684

ВЕСТНИК

МОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Выпуск 103 / 2026

ISSN 2949-3684

Вестник Морского государственного университета. Вып. 103 / 2026 / Морской государственный университет им. адм. Г. И. Невельского. — Владивосток: Мор. гос. ун-т, 2026. — 59 с. ; цв. ил., табл. — Библиогр. в конце ст. — ISSN 2949-3684.

Вестник Морского государственного университета содержит публикации, посвященные актуальным нормативно-организационным, техническим и технологическим проблемам судовождения и безопасности мореплавания, судоремонта, судовых силовых установок и их элементов, логистических транспортных систем и гидрографии, автоматизации и управления технологическими процессами, обработки информации, системного анализа и управления процессами перевозок на морском транспорте. Материалы содержат теоретические выводы и практические рекомендации, которые могут быть использованы для развития научных направлений и для принятия инженерных, административных и коммерческих решений.

Дата выхода в свет - 27 июля 2026 г. Выходит четыре раза в год.

Зарегистрировано Федеральной службой по надзору в сфере связи и массовых коммуникаций. Свидетельство о регистрации Эл № ФС77-82589 от 30.12.2021.

Учредитель и издатель – Федеральное государственное бюджетное образовательное учреждение высшего образования «Морской государственный университет имени адмирала Г.И. Невельского».

Адрес учредителя, издателя и редакции: 690003, Россия, г. Владивосток, ул. Верхнепортовая, 50а.
Электронная почта редакции: vestnik@msun.ru; телефон редакции: +7 (423) 251-76-36.

Цена свободная.

СОДЕРЖАНИЕ

ЭКСПЛУАТАЦИЯ ВОДНОГО ТРАНСПОРТА, ВОДНЫЕ ПУТИ СООБЩЕНИЯ И ГИДРОГРАФИЯ

СУДОВЫЕ ЭНЕРГЕТИЧЕСКИЕ УСТАНОВКИ И ИХ ЭЛЕМЕНТЫ

ЛОГИСТИЧЕСКИЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

ЭКСПЛУАТАЦИЯ ВОДНОГО ТРАНСПОРТА, СУДОВОЖДЕНИЕ, ВОДНЫЕ ПУТИ СООБЩЕНИЯ И ГИДРОГРАФИЯ

УДК 629.5: 629.12.06.003.1

Оценка киберрисков судовых навигационных и коммуникационных систем

Гиркшас Артем Викторасович, курсант, e-mail: tjomih2005@gmail.com

Морской государственный университет имени адмирала Г.И. Невельского, г. Владивосток

В статье рассматриваются киберриски, возникающие при эксплуатации судовых навигационных и коммуникационных систем. Цель исследования состоит в выделении наиболее опасных сценариев воздействия на ECDIS, AIS, GNSS, VSAT и рабочие места экипажа, а также в определении первоочередных мер защиты. Научная новизна заключается в комплексном сопоставлении человеческого фактора, технических уязвимостей и последствий для безопасности мореплавания. Предложена качественная модель оценки риска, пригодная для включения в судовую систему управления безопасностью.

Ключевые слова: морская кибербезопасность, ECDIS, AIS, GNSS, VSAT, фишинг, управление киберрисками.

Assessment of cyber risks of shipborne navigation and communication systems

Girkshas Artyom V., e-mail: tjomih2005@gmail.com

Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

The article examines cyber risks arising during the operation of shipborne navigation and communication systems. The research aims to identify the most dangerous attack scenarios affecting ECDIS, AIS, GNSS, VSAT and crew workstations, and to determine priority protection measures. The scientific novelty lies in the combined comparison of human factors, technical vulnerabilities and consequences for navigational safety. A qualitative risk assessment model suitable for inclusion in a ship safety management system is proposed.

Keywords: maritime cybersecurity, ECDIS, AIS, GNSS, VSAT, phishing, cyber risk management.

Цифровизация судоходства изменила само содержание безопасной навигации. На современном судне электронная картографическая навигационная информационная система, приемники глобальных навигационных спутниковых систем, автоматическая идентификационная система, спутниковая связь, терминалы электронной почты и сервисные рабочие станции образуют связанную информационную среду. В нормальном режиме такая

среда повышает точность судовождения, ускоряет обмен данными с берегом и снижает нагрузку на экипаж. Однако при кибервоздействии те же связи становятся каналами распространения ошибки от одного устройства к другому.

Международная морская организация рассматривает киберриск как риск нарушения судоходных операций, безопасности или защищенности вследствие компрометации компьютерных систем, данных или программного обеспечения [1]. Резолюция MSC.428(98) дополнительно закрепила необходимость учитывать кибериски в системе управления безопасностью судоходной компании [2]. Следовательно, вопрос защиты судовых цифровых систем уже нельзя относить только к сфере информационных технологий. Он прямо связан с безопасностью плавания, предотвращением аварий, сохранностью груза и экологической защитой.

Наиболее проблемной особенностью судовой кибербезопасности является сочетание новых сетевых сервисов с оборудованием, изначально не рассчитанным на противодействие современным атакам. Протоколы обмена данными в навигации создавались в условиях, когда главным приоритетом были надежность передачи и совместимость, а не криптографическая защита. Кроме того, срок службы судового оборудования значительно превышает срок жизненного цикла обычных информационных систем. В результате на борту продолжают использоваться устаревшие операционные системы, сервисные порты, последовательные интерфейсы и стандартные пароли.

Цель настоящей статьи - разработать качественную модель оценки киберрисков судовых навигационных и коммуникационных систем и выделить меры, которые могут быть реализованы на уровне экипажа и судовладельца. Для достижения цели поставлены следующие задачи: определить основные объекты воздействия; описать типовые сценарии фишинга, вредоносного программного обеспечения, спуфинга и вмешательства в спутниковую связь; сопоставить последствия атак с мерами контроля; сформулировать направления совершенствования судовой системы управления киберрисками.

Методы

Исследование выполнено методом качественного анализа угроз. В качестве исходной базы использованы рекомендации ИМО по управлению морскими киберрисками, резолюция MSC.428(98), исследования по кибербезопасности ECDIS, материалы по спуфингу навигационных систем, документы по защите VSAT-связи и открытые сведения о крупных киберинцидентах в судоходстве [1-7]. Такой подход позволяет не ограничиваться одной технической системой, а рассматривать судно как совокупность взаимосвязанных информационных и операционных компонентов.

Границы модели включают мостик, рабочие места экипажа, ECDIS, AIS, GNSS-приемники, спутниковый терминал VSAT, электронную почту, переносные носители и сервисные каналы технического обслуживания. Из анализа исключены портовые операционные системы и береговые цепочки поставок, поскольку они рассматриваются в отдельной статье. В качестве критерия риска применено сочетание трех параметров: вероятность реализации сценария, тяжесть последствий для безопасности плавания и зрелость существующих мер контроля.

Для ранжирования угроз использована трехуровневая шкала: низкий, средний и высокий уровень риска. Высокий уровень присваивается сценарию, если он способен

привести к потере достоверности навигационной информации, нарушению связи с берегом, невозможности использовать электронные карты или к принятию ошибочного решения вахтенным помощником. Средний уровень применяется к сценариям, последствия которых в основном ограничены нарушением доступности сервисов или утечкой данных, но при неблагоприятных условиях могут перерасти в угрозу безопасности. Низкий уровень относится к локальным событиям, быстро устраняемым штатными средствами.

Научная новизна исследования состоит не в описании новой уязвимости, а в объединении разнородных угроз в практическую судовую модель. Такая модель может использоваться как основа для внутренних инструкций, подготовки экипажа и проверки готовности судна к ежегодному аудиту системы управления безопасностью.

Решение задачи: модель оценки риска

Первым элементом модели является человеческий фактор. Фишинг и социальная инженерия остаются наиболее доступным способом начального проникновения, поскольку злоумышленнику не требуется преодолевать сложные технические барьеры. Достаточно убедить члена экипажа открыть вложение, перейти по ссылке или передать учетные данные под видом запроса агента, порта, поставщика связи или судоходной компании. На судне такой сценарий особенно опасен из-за ограниченной возможности быстро проверить отправителя и из-за высокой рабочей нагрузки вахтенного персонала.

Фишинг редко является конечной целью атаки. На практике он часто используется как начальный этап для установки вредоносного программного обеспечения. Вредоносная программа может шифровать файлы, похищать учетные данные, изменять настройки маршрутизации, блокировать доступ к электронным картам или использовать судовую сеть как промежуточную площадку для дальнейшего движения. Инцидент NotPetya показал, что вредоносный код, первоначально не ориентированный исключительно на морскую отрасль, способен вызвать масштабные последствия для глобальной логистики. В отчете A. P. Moller - Maersk указано, что атака NotPetya в 2017 году привела к нарушению транспортно-логистических операций и убыткам порядка 250-300 млн долл. США [6].

Второй элемент модели связан с ECDIS. Исследования показывают, что риски ECDIS формируются не только самим навигационным приложением, но и резервной конфигурацией, операционной системой и сторонними программными компонентами [3]. Если терминал ECDIS подключен к общей сети и использует устаревшие сервисы удаленного доступа или файлового обмена, заражение одного узла может распространиться на резервные средства. В такой ситуации формальное наличие дублирования не гарантирует устойчивости, поскольку основной и резервный терминалы могут иметь одинаковую уязвимость.

Показательный пример использования такой уязвимости - это печально известная атака хакера NotPetya на компанию Maersk в 2017 году, которая запомнилась как одна из первых крупных кибератак на судоходство. На самом деле, она была направлена вовсе не на морской сектор и лишь косвенно причинила ущерб крупнейшей в мире судоходной компании в размере 300 миллионов долларов, а также обошлась компании TNT в 400 миллионов долларов. В глобальном масштабе ущерб от этой атаки составил приблизительно 10 миллиардов долларов, в том числе и в России. Дело в том, что при создании ВПО, NotPetya эксплуатировал уязвимость в протоколе SMBv1, который позволял удаленно управлять данными на машинах, которые не получили обновления софта M.E.Doc – учетной программы, которая использовалась в Maersk до 2017 года. Протокол Server Message Block v1

– это устаревший сетевой протокол для межпроцессорного взаимодействия со старыми системами в сетях Windows. Другими словами, терминал, на который установлен ЭКНИС, использующий устаревшую версию ПО от Майкрософт может быть доступен для удаленного контроля при помощи этого протокола. Все, что понадобилось NotPetya – это отправить на основню машину с сетевым портом 455 модифицированные эксплойты EternalBlue и EternalRomance, которые в 2013 году были разработаны Агенством Национальной Безопасности США, но позже появившимися в сети.

Ниже представлен краткий анализ старого набора инструментов/эксплойтов вокруг SMB/MS17-010/EternalBlue;

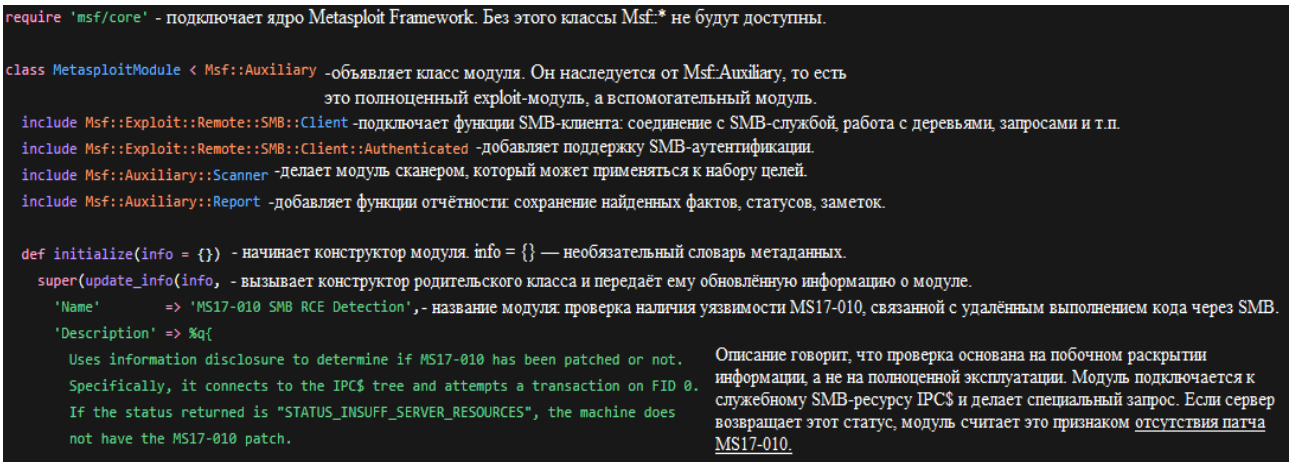


Рисунок 1 – Модуль обнаружения

Главная идея этого Ruby-фрагмента: это **модуль обнаружения**, который описывает, как определить, пропатчена ли SMB-служба против MS17-010.

Рисунок 2 – Сканирование ОС.

Этот фрагмент — **не логика атаки**, а таблица строк, встроенных в бинарник. По ней видно, что программа содержит названия модулей, параметров и версий Windows, а также подписи/комментарии, которые помогают реверсеру понять, какие аргументы передаются в функцию.

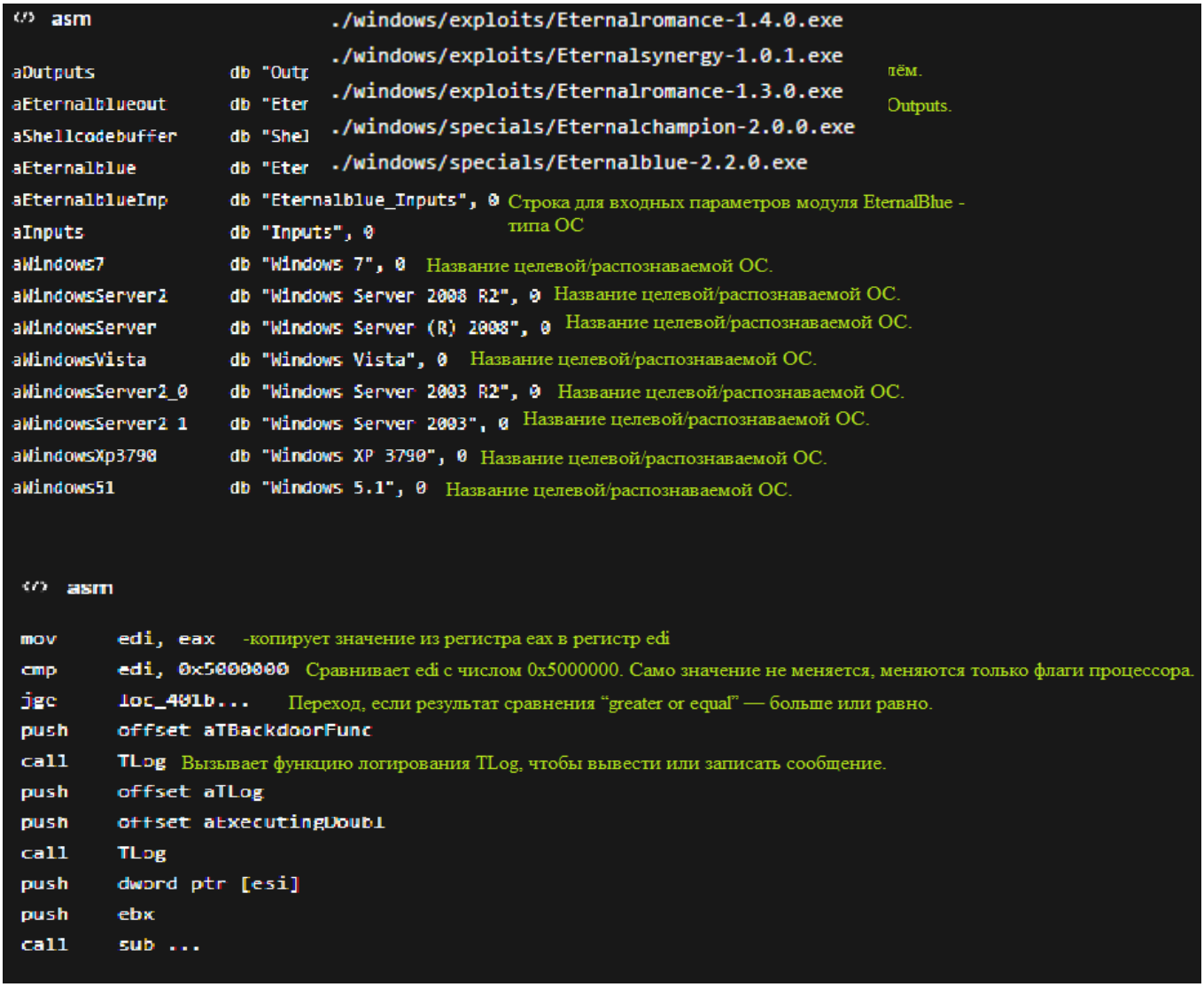


Рисунок 3 – Исполняемые файлы

Это список найденных исполняемых файлов в подкаталогах windows/exploits и windows/specials.

Третий элемент модели - подмена данных GNSS и AIS. Спуфинг представляет собой передачу ложного сигнала или ложного сообщения, которое принимается системой как достоверное. Для GNSS это означает искажение координат, скорости или времени. Для AIS это может выражаться в создании ложных целей, изменении параметров движения судна или сокрытии реального положения. Уязвимость усугубляется тем, что базовые гражданские режимы передачи навигационной информации имеют ограниченную аутентификацию и не обеспечивают полноценную криптографическую проверку источника [4].

Четвертый элемент модели - спутниковая связь VSAT. Она обеспечивает обмен с берегом, доступ к сервисам компании, передачу служебных документов и иногда связь с системами мониторинга. VSAT одновременно является необходимым каналом управления судовой эксплуатацией и потенциальной точкой входа в сеть. Рекомендации по защите VSAT-

сетей указывают на необходимость сегментации, шифрования, контроля удаленного доступа, отключения неиспользуемых сервисов и управления учетными записями [7]. Для судна особенно важно разделять сеть экипажа, административную сеть и сегменты, связанные с навигацией или управлением механизмами.

Пятый элемент модели - переносные носители и обновления. На практике судовые системы часто обновляются во время сервисного обслуживания или с использованием внешних носителей. Если проверка целостности обновлений не выполняется, легитимный процесс технической поддержки может превратиться в канал заражения. Поэтому в судовую процедуру необходимо включать проверку источника, контроль хэш-сумм или цифровой подписи, регистрацию действий сервисного инженера и возможность отката к предыдущей версии.

Таблица 1 – Сопоставление угроз судовых навигационных и коммуникационных систем

Угроза	**Уязвимый объект**	**Возможное последствие**	**Приоритетные меры контроля**
Фишинг и социальная инженерия	Электронная почта, терминалы экипажа, служебные аккаунты	Компрометация учетных данных, запуск вредоносного вложения, начальное проникновение в сеть	Обучение экипажа, проверка отправителей, двухфакторная аутентификация, запрет передачи паролей
Вредоносное программное обеспечение	Рабочие станции, файловые ресурсы, сервисные ноутбуки	Шифрование данных, простой электронного документооборота, потеря доступности карт или отчетности	Резервное копирование, антивирусная защита, контроль USB, обновления ОС и приложений
Спуфинг GNSS и AIS	GNSS-приемники, AIS, ECDIS-оверлеи	Ошибочное положение судна, ложные цели, неверная оценка опасности столкновения	Сопоставление с РЛС и визуальным наблюдением, контроль аномалий, подготовка вахтенных помощников
Компрометация ECDIS	Основной и резервный терминалы, ОС, сторонние компоненты	Отказ электронных карт, искажение маршрута, потеря доверия к плану перехода	Изоляция ECDIS, своевременные обновления, отключение лишних сервисов, проверка резервирования
Атака на VSAT	Спутниковый терминал, маршрутизатор, удаленный доступ	Нарушение связи с берегом, перехват трафика, переход из IT-сегмента в критические системы	Сегментация, сильные пароли, шифрование, закрытие открытых портов, журналирование

Результаты

Сопоставление угроз показывает, что наиболее опасными являются не отдельные технические дефекты, а каскадные сценарии. Например, фишинговое письмо может привести к установке вредоносного программного обеспечения, затем к краже учетных данных

администратора, после чего атакующий получает доступ к настройкам сетевого оборудования или сервисной станции. Аналогично, подмена координат GNSS становится критической не сама по себе, а тогда, когда вахтенный помощник без проверки переносит ложные координаты в оценку навигационной обстановки.

Основной результат модели состоит в выделении трех групп мер. Первая группа - организационные меры: назначение ответственных лиц, ведение перечня компьютерных систем, включение киберинцидентов в судовые тревоги, периодическая тренировка экипажа. Вторая группа - технические меры: сегментация сетей, обновления, резервное копирование, контроль съемных носителей, антивирусная защита, отключение неиспользуемых сервисов. Третья группа - навигационные меры: проверка электронной информации независимыми средствами, работа с радиолокационным изображением без избыточной зависимости от AIS, контроль расхождений между GNSS, гирокомпасом, лагом, визуальными ориентирами и радиолокацией.

Практическая ценность предложенной модели заключается в ее пригодности для судовой эксплуатации. Она не требует сложных расчетов и может быть оформлена как чек-лист проверки перед рейсом, при заходе в район с повышенной навигационной сложностью или перед проведением обновлений. При этом модель согласуется с функциональными элементами управления киберрисками: идентификацией, защитой, обнаружением, реагированием и восстановлением [1].

Дополнительным результатом является вывод о необходимости сохранять профессиональные навыки традиционной навигации. Чем выше уровень автоматизации, тем больше риск некритичного доверия электронным данным. Поэтому подготовка экипажа должна включать не только инструктаж по паролям и фишингу, но и практическое распознавание аномалий: внезапного смещения координат, появления большого числа однотипных AIS-целей, исчезновения реалистичных параметров судов, противоречия между AIS и радиолокационной картиной.

Таблица 2 – Приоритетные меры защиты судовых систем

Мера	Назначение	Ожидаемый эффект
Инвентаризация судовых компьютерных систем	Определить, какие устройства, версии ПО и сетевые связи присутствуют на борту	Снижение неопределенности при оценке риска и при расследовании инцидента
Сегментация сетей	Разделить экипажную, административную, навигационную и сервисную зоны	Ограничение распространения атаки после начального проникновения
Проверка обновлений и резервное копирование	Подтвердить подлинность патчей и сохранить возможность восстановления	Сокращение времени простоя и уменьшение последствий заражения
Тренировки по фишингу и спуфингу	Научить экипаж распознавать социальную инженерию и навигационные аномалии	Повышение вероятности раннего обнаружения атаки
Многосенсорная навигационная проверка	Сравнивать данные ECDIS, GNSS, AIS, РЛС и визуального наблюдения	Снижение риска принятия решения по поддельным данным

Выводы и обсуждение

Проведенный анализ подтверждает, что судовые навигационные и коммуникационные системы должны рассматриваться как единая киберфизическая среда. Уязвимость электронной почты, ECDIS, AIS, GNSS или VSAT сама по себе может показаться локальной, но в реальной эксплуатации последствия распространяются на безопасность плавания и управление рейсом. Наиболее значимыми рисками являются фишинг как начальный вектор атаки, вредоносное программное обеспечение как средство нарушения доступности, спуфинг как источник недостоверной навигационной информации и компрометация спутниковой связи как канал удаленного воздействия.

Для судовладельца первоочередными действиями являются включение киберрисков в систему управления безопасностью, создание актуального перечня компьютерных систем, сегментация сетей и контроль обновлений. Для экипажа ключевыми являются проверка источников сообщений, отказ от использования неизвестных носителей, регулярные тренировки и постоянное сопоставление электронных данных с независимыми средствами наблюдения. Такие меры не устраняют риск полностью, но переводят его из неуправляемого состояния в контролируемое.

Дальнейшие исследования целесообразно направить на разработку судовых тренажерных сценариев, в которых фишинг, отказ VSAT, подмена GNSS и появление ложных AIS-целей объединяются в одну учебную ситуацию. Это позволит оценивать не только техническую готовность судна, но и способность экипажа принимать безопасные решения при частичной потере доверия к электронным системам.

Список литературы

1. Guidelines on Maritime Cyber Risk Management : MSC-FAL.1/Circ.3/Rev.3. – London : International Maritime Organization, 2025. – 9 p. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf (дата обращения: 15.05.2026).
2. Maritime Cyber Risk Management in Safety Management Systems : Resolution MSC.428(98). – London : International Maritime Organization, 2017. – 1 p. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428%2898%29.pdf (дата обращения: 15.05.2026).
3. Svilicic, B. Raising Awareness on Cyber Security of ECDIS / B. Svilicic, D. Brčić, S. Žuškin, D. Kalebić // TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. – 2019. – Vol. 13, № 1. – P. 231–236. – DOI: 10.12716/1001.13.01.24.
4. Androjna, A. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness / A. Androjna, M. Perkovič // Transactions on Maritime Science. – 2021. – Vol. 10, № 2. – P. 361–373. – DOI: 10.7225/toms.v10.n02.w08.
5. Protecting VSAT Communications : Cybersecurity Advisory. – Fort Meade : National Security Agency, 2022. – 13 p. – URL: https://media.defense.gov/2022/May/10/2002993519/-1/-1/0/

CSA_PROTECTING_VSAT_COMMUNICATIONS_05102022.PDF (дата обращения: 15.05.2026).

6. A.P. Moller - Maersk. Risk Management. Annual Report 2017. – Copenhagen : A. P. Moller - Maersk, 2018. – 5 p. – URL: https://investor.maersk.com/static-files/d533735a-5df7-423c-8611-d4a2c3bf31b0 (дата обращения: 15.05.2026).
7. Cyber Security for Ports and Port Systems. Code of Practice. – London : Department for Transport, 2020. – 75 p. – URL: https://assets.publishing.service.gov.uk/media/5e284eefe5274a6c3ee68fcd/cyber-security-for-ports-and-port-systems-code-of-practice.pdf (дата обращения: 15.05.2026).
8. EternalBlue Exploit: What It Is And How It Works — SentinelOne redaction team, 2025. https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

Поступила в редакцию 10 июня 2026 г.

УДК 656

Технология разгрузки судов, стоящих на рейде, дирижаблями

Луговец Александр Анатольевич [1], д-р эконом. наук, канд. техн. наук, доцент, e-mail: alal@list.ru
Николаева Полина Александровна [1], e-mail: polsidorova@mail.ru

[1] Морской государственный университет имени адмирала Г.И. Невельского, г. Владивосток

В статье рассмотрена проблема рейдовой выгрузки грузов с судов в условиях Крайнего Севера, где традиционная технология с использованием барж является не эффективной, в связи с ограничениями из-за сурового климата, мелководья и недостаточного развития портовой инфраструктуры. Предложена новая концепция выгрузки грузов с судов, стоящих на рейде, с применением дирижаблей. Описаны преимущества данного метода, включая высокую грузоподъемность, экологичность, снижение времени разгрузки и минимальные требования к береговой инфраструктуре. Приведена детальная технологическая схема выполнения работ, включающая подготовительные операции, позиционирование, подъем груза, транспортировку и выгрузку на необорудованный берег. Сделан вывод о перспективности применения дирижаблей для повышения эффективности и безопасности арктических грузоперевозок.

Ключевые слова: дирижабль, рейдовая разгрузка, необорудованный берег, Крайний Север, морской транспорт, грузоперевозки, Арктика.

Technology for unloading ships in the harbor using airships

Lugovets Alexander A.,[1] e-mail: alal@list.ru,
Nikolaeva Polina A.,[1] e-mail: polsidorova@mail.ru

[1] Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

The article discusses the problem of unloading cargo from ships in the Far North, where the traditional technology of using barges is not effective due to the harsh climate, shallow waters, and insufficient development of port infrastructure. A new concept of unloading cargo from ships in the roadstead using airships is proposed. The advantages of this method, including high cargo capacity, environmental friendliness, reduced unloading time, and minimal requirements for coastal infrastructure, are described. A detailed technological scheme of work performance is given, including preparatory operations, positioning, cargo lifting, transportation, and unloading on an unequipped shore. The conclusion is made about the prospects of using airships to increase the efficiency and safety of Arctic cargo transportation.

Keywords: airship, raid unloading, unequipped shore, Far North, sea transport, cargo transportation, Arctic.

В соответствии с Постановлением правительства РФ от 16 ноября 2021 года № 1946 "Об утверждении перечня районов Крайнего Севера и местностей, приравненных к районам Крайнего Севера, в целях предоставления государственных гарантий и компенсаций для лиц, работающих и проживающих в этих районах и местностях, признании утратившими силу некоторых актов Правительства Российской Федерации и признании не действующими на территории Российской Федерации некоторых актов Совета Министров СССР» [1], районами Крайнего Севера являются Все острова Северного Ледовитого океана и его морей, а также острова Берингова и Охотского морей, а также большое количество населенных пунктов, входящих в 14 субъектов Российской Федерации, к которым можно отнести Магаданскую и Мурманскую области, Чукотский автономный округ, Республика Саха (Якутия) и многие другие, представленные на рисунке 1.

Рисунок 1 - Районы Крайнего Севера и приравненные к ним местности

Природные и климатические особенности данных территорий приводят к существенным ограничениям для развития транспортной инфраструктуры, в связи с чем морской транспорт является основным, обеспечивающим завоз грузов на территорию Арктики. В настоящее Арктической зоне Российской Федерации расположено более 70 крупных и мелких портов и перевалочных пунктов [2]. Многие из них, такие как Тикси, Певек, Эгвекинот, Амдерма и другие используют рейдовую разгрузку судов. Это связано с ледовой обстановкой, особенностями береговой линии, мелководьем, не позволяющим крупным судам подходить к берегу, а также недостаточно развитой портовой инфраструктурой, из-за чего в порту нет достаточной причальной линии для приема всего судна.

Технология и оборудование для выгрузки грузов с судов, стоящих на рейде, на необорудованный берег представляют собой совокупность решений, обеспечивающих выполнение

сложных логистических задач, требующих высокой точности, надежности и адаптивности оборудования для работы в разнообразных условиях, включая мелководье, волнения и нестабильный береговой рельеф [3]. Согласно «Карт типовых и опытных технологических процессов перегрузочных работ, выполняемых в рейдовых портах и портовых пунктах на льду берегового припая и у необорудованного берега» [4], рейдовый перегрузочный процесс состоит из следующих последовательных этапов: судно — плашкоут — буксир — причал — кран — склад, а тип груза влияет на выбор грузозахватных приспособлений, число пакетов с грузом на плашкоуте и количество ярусов укладки. Данная технология для выгрузки контейнера на необорудованный берег представлена на рисунке 2.

Рисунок 2. – Выгрузка контейнера на необорудованный берег с использованием баржи

Несмотря на достаточную универсальность и то, что такой способ выгрузки сейчас является единственным, он имеет достаточное количество недостатков. Эффективность работ сильно зависит от целого ряда причин, в том числе, от гидрометеорологических факторов. Так, при волнении моря свыше 2 – 3 баллов выгрузка останавливается, так как швартовка баржи или плашкоута у борта судна и его буксировка становится небезопасной. Низкая производительность обусловлена также сложностью самого процесса, состоящего из большого количества этапов, что становится особенно критичным в сочетании с низкой грузоподъемностью вспомогательного флота, из-за чего выгрузка партии груза в несколько тысяч тонн может растянуться до 10 суток и более. При этом, традиционная технология разгрузки судна опасна, работы со плашкоутами и баржами производятся в условиях качки, что увеличивает риск травмирования рабочих, порчи оборудования, потери и снижения качества груза. В связи с этим, предложена концепция выгрузки грузов с судов, стоящих на рейде, дирижаблями [5].

Данная технология работ обладает рядом преимуществ:

- повышение эффективности работ, связанное с большей грузоподъемностью транспортного средства, меньшей зависимостью от волнений моря и снижением количества перевалок груза;
- снижение требований к инфраструктуре, так как дирижаблю не требуется причалов, кранов, подъездных путей и складских площадок в непосредственной близости от берега. Отсутствие ограничений в планировании маршрута перелета позволяет устроить склад в любом, наиболее подходящем месте, а для хранения самих летательных аппаратов не требуется специализированных сооружений и сложного оборудования;

- повышение безопасности грузовых операций и упрощение процесса управления выгрузкой грузов за счет выполнения работ меньшим количеством рабочих и сокращения количества операций.

Конечно, недостатки у такого способа воспроизводства работ тоже имеются. К ним можно отнести:

- необходимость специального обучения персонала как для управления дирижаблем, так и для производства работ по разгрузке судна на рейде;
- отсутствие нормативной документации.

Так как преимущества применения современных летательных аппаратов легче воздуха являются более весомыми в сравнении с использованием барж, была разработана технология разгрузки судов, стоящих на рейде, дирижаблями. В общем виде, она представляет собой:

1. Общие положения

Выгрузка с судна на необорудованный берег осуществляется силами экипажа с дополнительным штатом подготовленных моряков. Работа на судне организуется по двухсменному графику под руководством опытных бригадиров из числа членов экипажа и под контролем вахтенных помощников капитана. Общее руководство всеми операциями по выгрузке судна осуществляется капитаном судна и по согласованию с ним.

2. Подготовительная операция

Вахтенный помощник капитана судна, совместно с метеослужбой проверяет скорость и направление ветра, видимость, облачность и осадки в районе рейда и на береговой площадке: скорость ветра не должна превышать 20 м/с, видимость свыше 3 километров. В это время, судовая команда с использованием судовых грузовых устройств формирует пакет с грузом на грузовой раме в просвете люка трюма или на грузовой палубе, в зависимости от размеров грузовой рамы, с учетом рода груза, его массы и размеров. Далее, матрос на судне, совместно с бортоператором дирижабля подготавливают зацеп за грузовую раму, проверяют мягкие подвесы на соответствие грузоподъемности и типу груза. Командир дирижабля определяет точку зависания дирижабля над судном с учетом высоты надстроек, антенн, с безопасным вертикальным зазором.

3. Подлет и позиционирование

Дирижабль под руководством командира вылетает с берегового аэродрома к судну на крейсерской скорости. Летательный аппарат подлетает к судну и снижается на высоту точки зависания, переходит в режим зависания (над просветом люка или грузовой палубой) с компенсацией сноса ветром. Бортоператор дирижабля опускает грузовые тросы тельферов к грузовой раме.

4. Подъем груза на внешний подвес

Судовая бригада докеров-механизаторов под контролем вахтенного помощника и бортоператора зацепляет мягкие подвесы за замки тросов тельферов. Бортоператор медленно поднимает грузовую раму на высоту 5-10 метров над палубой для проверки устойчивости и отсутствия раскачивания груза свыше 0,5 метров, после чего, с помощью системы управления подвесом окончательно поднимает груз до уровня килевой фермы и фиксирует замками. Командир дирижабля проверяет центровку дирижабля по бортовым индикаторам, чтобы центр масс находился в пределах допустимого диапазона.

5. Транспортировка и выгрузка на берег

Дирижабль под руководством командира отходит от судна на расстояние безопасного удаления от надстроек и набирает высоту и на крейсерской скорости и высоте по рельефу перелетает к береговой площадке выгрузки. Летательный аппарат зависает над береговой складской площадкой или точкой выгрузки с отклонением до одного метра. Бортоператор от-

крывает замки тельферов и опускает грузовую раму на приемную платформу или складскую площадку со скоростью не более 0,5 м/с. Береговая команда освобождает грузовую раму, расстроповывает груз и разгружает грузовую раму, после чего бортоператор поднимает тросы тельферов, закрывает замки.

6. Заключительная операция (возврат на судно или на базу)

Дирижабль под руководством командира корабля, при необходимости выполнения следующего рейса, возвращается к судну, где повторяются этапы по формированию и доставке пакетов груза на берег. После окончания цикла выгрузки, летательный аппарат возвращается на береговой аэродром базирования, а техническая служба совершает послеполетный осмотр дирижабля, проверяет подвесную систему, при необходимости осуществляет дозаправку.

При необходимости совершения нескольких рейсов подряд формирование следующего подъема груза на судне и расформирование на берегу может быть совмещено с полетом дирижабля.

Использование технологии выгрузки грузов с судов, стоящих на рейде, с помощью дирижаблей, позволяет решить большое количество проблем, характерных для традиционной технологии: глубина и рельеф дна, отсутствие оборудованных причальных стенок и устаревшая инфраструктура портов и портпунктов, а также сложные ледовые и метеорологические условия. Предложенная технологическая схема позволяет осуществлять выгрузку грузов непосредственно с судна на необорудованный берег, сокращая количество операций с грузом, что сокращает время разгрузочных работ, а также снижает затраты на выполнение логистических операций. Таким образом, использование летательных аппаратов легче воздуха является альтернативой традиционной рейдовой разгрузке судна плашкоутами и может быть рекомендована к поэтапному внедрению в практику северного завоза, особенно для доставки тяжеловесных и крупногабаритных грузов в труднодоступные районы Крайнего Севера.

Список литературы

1. Постановление правительства РФ от 16 ноября 2021 года № 1946 "Об утверждении перечня районов Крайнего Севера и местностей, приравненных к районам Крайнего Севера, в целях предоставления государственных гарантий и компенсаций для лиц, работающих и проживающих в этих районах и местностях, признании утратившими силу некоторых актов Правительства Российской Федерации и признании не действующими на территории Российской Федерации некоторых актов Совета Министров СССР»
2. Вехи большого пути : [сайт] // Arctic Russia : [электронный ресурс]. – URL: https://arctic-russia.ru/article/vekhi-bolshogo-puti/
3. Лукьянов, Г.Е. Выгрузка на необорудованный берег / Г. Е. Лукьянов, А. А. Максимов // Молодой ученый. – 2024. – № 52(551). – С. 49-53.
4. РД 31.41.03-79. Карты типовых и опытных технологических процессов перегрузочных работ, выполняемых в рейдовых портах и портовых пунктах, на льду берегового припая и у необорудованного берега.
5. Николаева, П. А. Возможность интеграции морского транспорта с дирижаблями при выгрузке груза на необорудованный берег / П. А. Николаева // Научные проблемы водного транспорта. – 2026. – № 87. – С. 132-143. – DOI 10.37890/jwt.vi87.701. – EDN NGHTIV.

Поступила в редакцию 13 июля 2026 г.

УДК 656.61.08

Концепция «резилентная безопасность» в морском судоходстве

Мотрич Владимир Николаевич, доцент, e-mail: MotrichVN@msun.ru

Морской государственный университет имени адмирала Г.И. Невельского, г. Владивосток

Показана эволюция взглядов на причины аварий на море и моделей, объясняющих их механизм, в историческом развитии. Приведено описание теории домино Гейнриха, теории «швейцарского сыра» и эпидемиологических теорий аварий. Рассмотрены достоинства и недостатки линейных, сложных линейных и нелинейных моделей аварий, а также перспективы использования концепции «резилентная безопасность» и модели функционального резонанса в целях предотвращения аварий на море. Описаны принципы инженерии резилентной безопасности. Затронуты вопросы о роли и значении прогнозирования и мониторинга развития ситуации, гибкого реагирования и адаптивных возможностей. Содержатся предложения о дальнейшем совершенствовании системного управления безопасностью и использовании программ управления ресурсами мостика с точки зрения приложения концепции «резилентная безопасность» при подготовке судоводителей.

Ключевые слова: безопасность, аварии, несчастные случаи, моделирование, причины аварий.

“Resilient safety” concept in maritime shipping

Motrich Vladimir N., e-mail: MotrichVN@msun.ru

Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

This article explores the evolution of views on maritime safety and their models over time. It also describes Heinrich's domino theory, the "Swiss cheese" theory, and epidemiological theories of emergency care. It examines the characteristics and limitations of linear, complex linear, and nonlinear models of emergency situations, as well as perspectives on the use of the concept of "resilient safety" and the functional resonance model for preventing accidents at sea. The principles of sustainable safety engineering are described. The article addresses the development and implementation of forecasting and situational awareness, flexible response, and adaptive capabilities. It also includes proposals for improving systemic safety management and the use of bridge decision management programs, with implications for the application of the "resilient safety" concept in navigator training.

Keywords: safety, accidents, incidents, modeling, causes of accidents.

Морская индустрия характеризуется высоким риском, и аварии на море часто имеют катастрофические последствия, как для сообщества людей, так и для окружающей среды. Состояние нулевой аварийности в общих чертах и есть безопасность. Хотя имеется много определений безопасности, которые используются в юриспруденции, судостроении и социологии, именно безаварийное плавание – это то, чего желают судовладельцы, операторы судов и моряки.

Цель настоящей статьи отнюдь не продолжить бесконечный спор о конкретных формулировках, а рассмотреть одну из концепций XXI века, по-новому объясняющую причины аварий, и попытаться оценить ее влияние на безопасность мореплавания и будущую подготовку моряков.

Также необходимо пояснить термин «управление безопасностью», под которым понимается решения и практические действия, которые могут направлять, контролировать и вмешиваться в основные операции с целью обеспечения или поддержания безопасности эксплуатации судна.

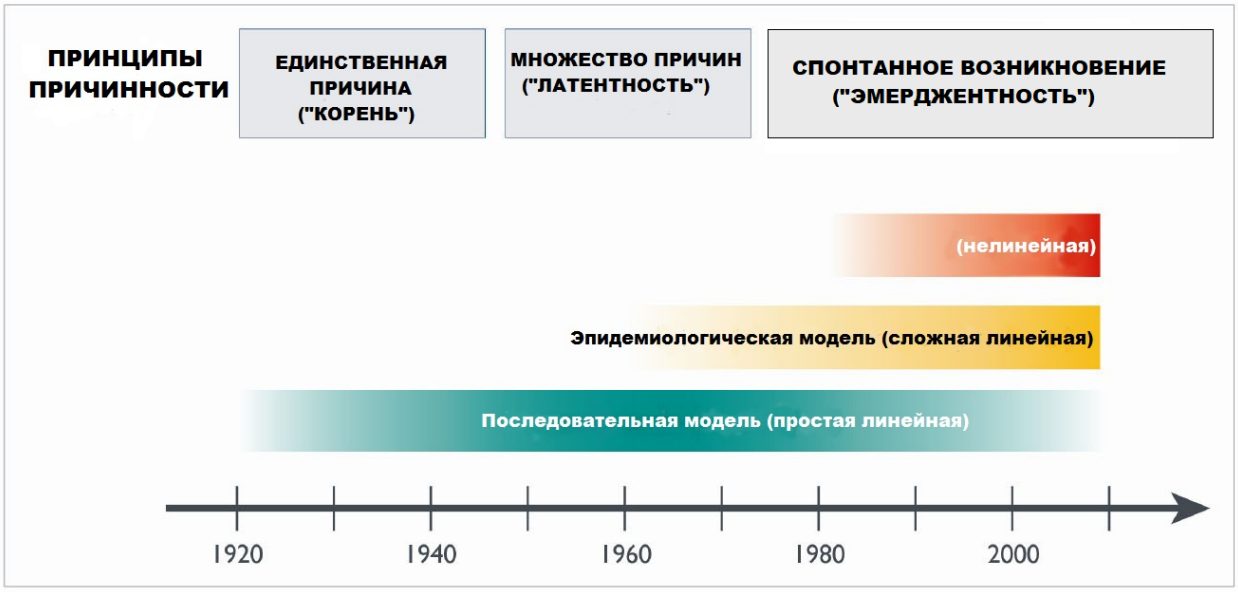


Рисунок 1. Эволюция моделирования аварий

Для управления безопасностью в любой сфере необходимо понимать, как и почему происходят аварии и инциденты, и что делает организацию безопасной. Аварии происходят без предупреждения, участники аварии не могут играть роль нейтрального наблюдателя, события при аварии развиваются за очень короткий промежуток времени и часто имеют ореол таинственности. Именно поэтому существует множество теорий и моделей причин аварий. Эволюция развития взглядов на возникновение аварий и моделей, объясняющих их механизм, показана на рис. 1.

Можно начать с рассмотрения одной из первых «теорий аварийности», суть которой в том, что аварии и несчастные случаи являются следствием «судьбы» или «божьей воли». В обоих случаях нежелательные события предопределены и происходят независимо от того, пытаемся мы их избежать или нет. При таком понимании аварийных случаев действия по обеспечению безопасности практически бессмысленны.

Исторически сложилось так, что в морском мире финансовая выгода ставилась выше безопасности экипажа и окружающей среды. Сэмюель Плимсоль, депутат британского пар-

ламента, автор Закона о грузовой марке, в 1873 году писал, что большое количество судов регулярно отправлялось в море в таком плачевном и плохо обеспеченном состоянии, что они могли достичь пункта назначения только в хорошую погоду, а многие были настолько перегружены, что практически не могли добраться до места назначения, если море было хоть немного неспокойным» [1].

К сожалению, потребовалась гибель «Титаника» и 1517 человек, чтобы морской мир наконец-то обратил внимание на проблемы безопасности, которые долгое время преследовали отрасль. После катастрофы «Титаника» и принятия конвенции СОЛАС пройден долгий путь реагирования на аварии, а не попыток их предотвратить. Некоторые из ключевых морских конвенций являются прямым результатом таких катастроф, как разливы нефти с танкеров «Torrey Canyon» в 1967 году и «Amoco Cadiz» в 1977 году, а также опрокидывание судна «Herald of Free Enterprise» в 1993 году, — это одни из самых заметных событий, которые привели к серьезным изменениям в морском мире.

С давних пор применяется предписывающий подход, основанный на убеждении, что снижение числа случаев катастроф и аварий морских судов, гибели и травматизма членов экипажа может быть достигнуто путем установления на международном и национальном уровне обязательных для применения правил и норм, регулирующих различные аспекты эксплуатации судов, деятельности судоходных и других морских предприятий.

В период от начала XIX века и до конца XX столетия причины аварий в основном приписывались механическим неисправностям и структурным повреждениям, которые считались предотвратимыми при соблюдении технических стандартов и руководств, разработанных профессиональными инженерами, архитекторами и проектировщиками, нормативные документы главным образом регламентировали технические аспекты безопасности мореплавания.

В результате технических усовершенствований действительно удалось снизить частоту и тяжесть последствий морских происшествий. Однако сокращение отказов в технологиях выявило основополагающее влияние человеческой ошибки на причины аварий. Эти факторы тщательно изучались, хотя по-прежнему использовался подход, предполагающий, что нежелательные события развиваются линейно и последовательно.

Так называемая «теория предрасположенности к несчастным случаям» постулировала, что некоторые люди более склонны к несчастным случаям, чем другие, потому что они более небрежны, неуклюжи, склонны к риску или по другим причинам. Эта теория заложила основу для того, чтобы в первую очередь обвинять отдельных лиц в авариях. Сегодня эта теория используется редко, хотя предубеждения остались.

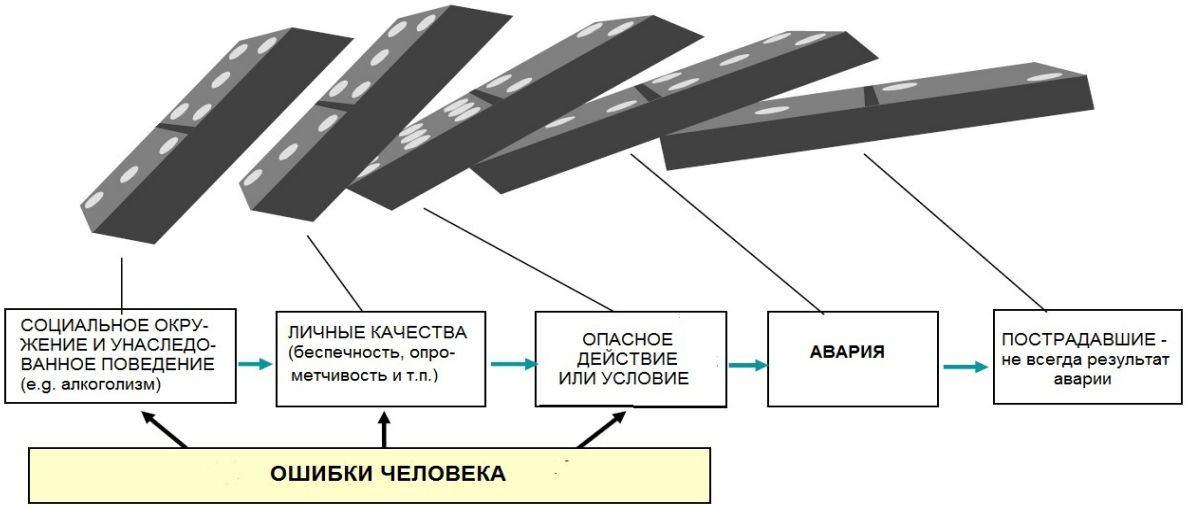


Рисунок 2. Принцип «домино»

Системное изучение механизма аварий началось с работ Герберта Гейнриха, сотрудника страховой компании “Traveller” в Беннингтоне, штат Вермонт. В своей книге «Предотвращение производственных аварий», вышедшей в свет в 1931 году и выдержавшей пять изданий, он предложил для объяснения причин аварий «теорию домино», которая относится к простыми линейными или последовательными моделями (рис. 2). Простые линейные модели предполагают, что аварии являются кульминацией серии событий или обстоятельств, которые взаимодействуют последовательно друг с другом линейным образом, и что этих аварий можно избежать, предприняв действия и устранив одну из причин в линейной последовательности. Простые линейные модели подвергались критике за то, что не отражают сложность реального мира. Идея линейной причинности происходит из естественных наук, где такие корреляции обнаруживаются: например, когда вы бросаете камень, он всегда падает. В социальных науках, которые изучают людей, таких причинно-следственных связей не существует [2].

В годы мировых войн активизировались исследования в области теорий отбора персонала, обучения и мотивации и положили начало в 1960-х и 1970-х годах эпохе человеческого фактора. Принятие Конвенции о стандартах подготовки, сертификации и несения вахты (Конвенция ПДНВ) в 1978 году привело к смещению акцента к роли отдельных моряков в аварийных ситуациях. Конвенция установила минимальные профессиональные стандарты для моряков, но ожидаемого резкого снижения аварийности не произошло.

Рисунок 3. Катастрофа парома «Herald of Free Enterprise»

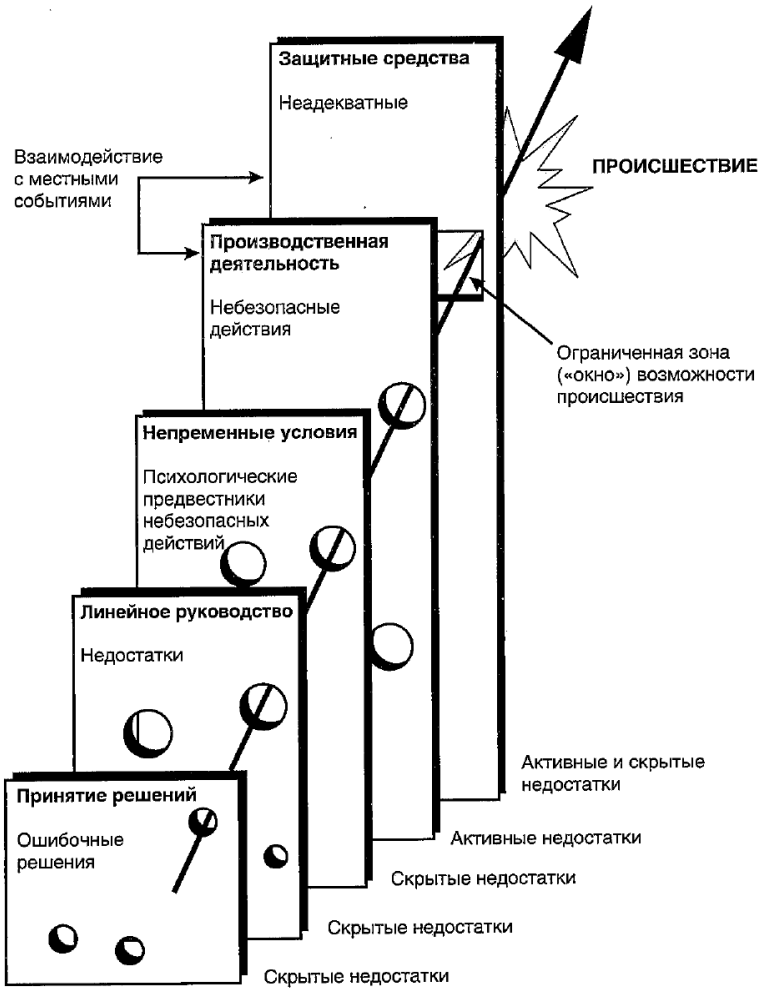
Хотя, как технический подход в рамках Международной конвенции СОЛАС, так и акцент на поведенческих и человеческих факторах в рамках Конвенции ПДНВ привели к значительному улучшению безопасности, многие морские аварии показали, что человеческие ошибки могут быть вызваны организационными факторами и низкими стандартами управления. Гибель парома «Herald of Free Enterprise» в 1987 году (рис. 3), в результате которого погибли 193 человека, рассматривается как один из главных факторов, способствовавших переходу морской отрасли к следующему этапу обеспечения безопасности благодаря принятию Международного кодекса управления безопасностью (МКУБ) в 1993 году и смещению акцента на организационные причины и культуру безопасности.

Получили развитие сложные линейные и эпидемиологические модели, которые до сих пор преобладают в расследовании аварий. Было осознано, что люди редко являются единственной причиной аварий или ошибок, и что эффективность человеческой деятельности основана на сложных взаимодействиях социально-технической системы, составляющей организацию [2].

Сложные линейные модели предполагают, что несчастные случаи являются результатом сочетания небезопасных действий и скрытых опасных условий внутри системы, следующих по линейному пути. В этих моделях предполагается, что предотвращение несчастных случаев должно быть сосредоточено на укреплении барьеров и защитных механизмов [2].

Эпидемиологические модели являются разновидностью сложных линейных моделей, которые рассматривают события, приводящие к несчастным случаям аналогично распространению болезни. Небезопасные действия, совершаемые операторами, рассматриваются как симптомы скрытых организационных проблем, которые могут дремать в организации годами, прежде чем проявятся, так же, как болезнь. Одним из ключевых исследователей в этом подходе является Джеймс Ризон и его теория организационных аварий рекомендована ИКАО и Резолюцией ИМО А.884(21) «Руководство по расследованию человеческих факторов в авариях и инцидентах на море». Основной недостаток модели Ризона, получившей название «Модели швейцарского сыра» (рис. 4) в статическом взгляде организации; реальная социо-

техническая система более динамичная и «дыры» постоянно перемещаются, переходя из одного качественного состояния в другое [2].



Источник: James Reason. 1990. Human Error. Cambridge University Press.

Рисунок 4. «Теория швейцарского сыра» Джеймса Ризона

В этот период также была выдвинута концепция культуры безопасности, которая утверждала, что риски и несчастные случаи часто вызваны плохой культурой безопасности, когда организации и операторы не имеют культуры, поддерживающей безопасную деятельность. Так, в докладе научного комитета ООН UNSCEAR в 1988 году основной причиной Чернобыльской катастрофы названо отсутствие культуры безопасности. Сама же культура безопасности была определена как «совокупность характеристик и установок организаций и отдельных лиц, которая устанавливает, что вопросы безопасности получают должное внимание в силу их значимости» в качестве первостепенной задачи.

Дальнейшее развитие эта концепция получила в изданиях МАГАТЭ, материалах конференций по вопросам ядерной безопасности в Атланте, Рио-де-Жанейро и др. Такое внимание к этой проблеме в ядерной энергетике вызвано тем, что низкая «культура безопасности» лежит в основе всех инцидентов, происшедших на АЭС. При этом отмечалось, что персонал — ключевое звено в формировании высокой «культуры безопасности». Участие каждого работника является необходимым условием достижения высоких стандартов безопасности, при этом руководители всех уровней должны быть лидерами в этом процессе [2].

Концепция культуры безопасности существует в большинстве отраслей с высоким уровнем риска и утвердилась в некоторых из них задолго до того, как стала общепринятой практикой в судоходстве. Поэтому неудивительно, что рекомендации атомной отрасли широко применяются при разработке политики и процедур СУБ.

В 1997 году в Резолюции, одобренной 20-й Ассамблеей ИМО, указывалось видение, принципы и цели Организации в отношении человеческого элемента в судоходстве. В числе целей было содействие, через принципы человеческого элемента, продвижению морской культуры безопасности. Детализация этого нового подхода к безопасности на море получила выражение в резолюции ИМО А.900, принятой 21-й Ассамблеей ИМО (1999 г.), в которой устанавливались цели деятельности Организации в XXI столетии. В числе заданий комитетов и подкомитетов ИМО было обеспечение эффективного применения культуры безопасности и бережного отношения к природной среде во всех видах деятельности Организации.

Ключ к созданию культуры безопасности заключается в:

- признании того, что несчастные случаи можно предотвратить, следуя правильным процедурам и установленной передовой практике;
- постоянном осмыслении вопросов безопасности; и
- стремлении к постоянному совершенствованию.

Хотя ИМО стремится сделать морской мир безопаснее, мы не можем игнорировать множество недавних аварий, которые в той или иной степени ускользнули от действующего нормативного режима. Некоторые из них связаны с конструкцией, но большинство связаны с человеческой ошибкой.

Рисунок 5. Катастрофа лайнера «Costa Concordia»

В 2012 году круизный лайнер «Costa Concordia» попытался пройти слишком близко к берегу, сел на мель и в итоге затонул, в результате чего 32 человека погибли или пропали без вести (рис. 5). Верховный кассационный суд оставил в силе 16-летний тюремный срок для капитана, признанного виновным в многочисленных убийствах, причинении кораблекрушения и оставлении судна, когда пассажиры и экипаж еще находились на борту. Результаты расследования этой аварии указывают на человеческую ошибку в виде небезопасной навигации

и последующих неэффективных процедур эвакуации экипажем, то, что лежит в основе Международной конвенции ПДНВ и Кодекса МКУБ [3].

Поиск новых эффективных способов предотвращения ошибок людей в процессе эксплуатации судна или хотя бы своевременного установления таких ошибок и их исправления, вселил уверенность в том, что проблема обеспечения безопасности мореплавания будет решена на качественно новом уровне.

Концепция «резилентной безопасности» возникла в XXI веке как ответ на ограниченность традиционных подходов к обеспечению безопасности. Она во многом опирается на исследования высоконадежных организаций, таких как атомные электростанции и т.п.

Известно, что некоторые системы кажутся более устойчивыми, чем другие. Эта нашло отражение в идее о том, что системы обладают свойством, называемым «резилентностью» (от англ. resilience - гибкость), которая приобрела чрезвычайно большую популярность в последние десятилетия.

Под резилентностью понимается повышенная способность поглощать возмущения, в отличие от робастности (от англ. robust — «крепкий», «надёжный», «устойчивый») —способности системы поддерживать свой уровень показателей при любых обстоятельствах [4].

Инжинерия резилентности — это подход к проектированию и эксплуатации сложных социотехнических систем, направленный на обеспечение их работоспособности в различных условиях. В отличие от традиционного подхода к безопасности, который часто опирается на ретроспективный анализ происшествий для выявления и устранения ошибок (реактивный подход), инженерия резилентности ставит во главу угла прогнозирование и способность системы к постоянной адаптации (проактивный подход).

Применительно к этому подходу, резилентность — это внутренняя способность системы корректировать свое функционирование до, во время или после таких событий, как изменения, сбои или благоприятные возможности, тем самым поддерживая необходимую работоспособность как в ожидаемых, так и в непредвиденных условиях.

В основе концепции резилентной безопасности лежит теория функционального резонансного анализа (Functional Resonance Analysis Method, FRAM), разработанная профессором Датской академии технических наук Эриком Холлнагелем, которая моделирует функционирование сложных социотехнических систем, фокусируясь на вариативности показателей, а не на линейной причинно-следственной связи.

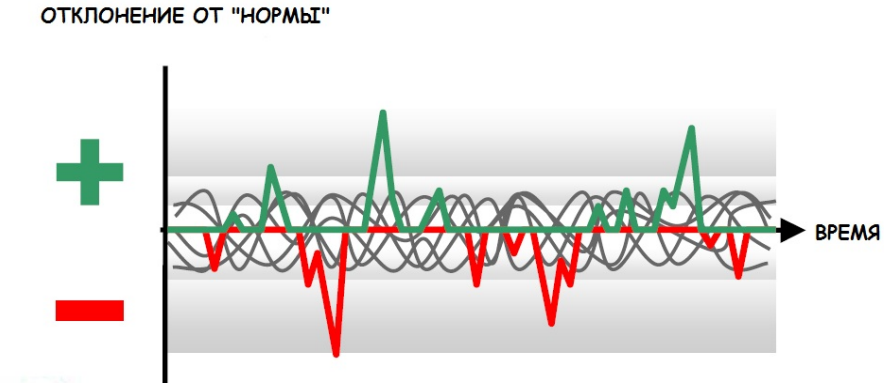


Рисунок 6. Изменчивость производительности человека

По мнению Холлнагеля, «силы (то есть люди, технологии, латентные условия, барьеры) нелинейно комбинируют, ведя тем самым к инциденту или аварии».

При выполнении задания вследствие изменчивости производительности результаты на выходе имеют отклонения от нормы, как в положительную сторону, так и в отрицательную

(рис. 6). Последние в традиционных моделях рассматриваются как отказы или ошибки. Но если авария представляется как результат нормальной изменчивости производительности, а не отказа или неправильной работы, в отличие от аналогии цепочки, динамику развития событий и совпадений более точно описывает аналогия резонанса.

Термин «резонанс» означает неожиданно сильный отклик системы, а «стохастический» отражает тот факт, что причина эффекта — хаотическое воздействие, шум (рис. 7).

Изменчивость – это всеобщее свойство биологических систем и различают:

- врожденную изменчивость (психологические и физиологические процессы);
- креативную изменчивость (преодоление ограничений или неопределенности);
- организационно-стимулированная (удовлетворение требований, привлечение ресурсов);
- социально-стимулированная (неформальные рабочие стандарты);
- контекстуально-стимулированная (адаптация к условиям работы).

Такая изменчивость позволяет системе более эффективно достичь целей, принося в жертву детали, которые при нормальных условиях излишние. Человек имеет склонность развивать такие рабочие методы, которые требуют наименьших затрат сил и экономят время [4].

Рисунок 7. Схема резонанса: А – обычный резонанс; Б – стохастический резонанс

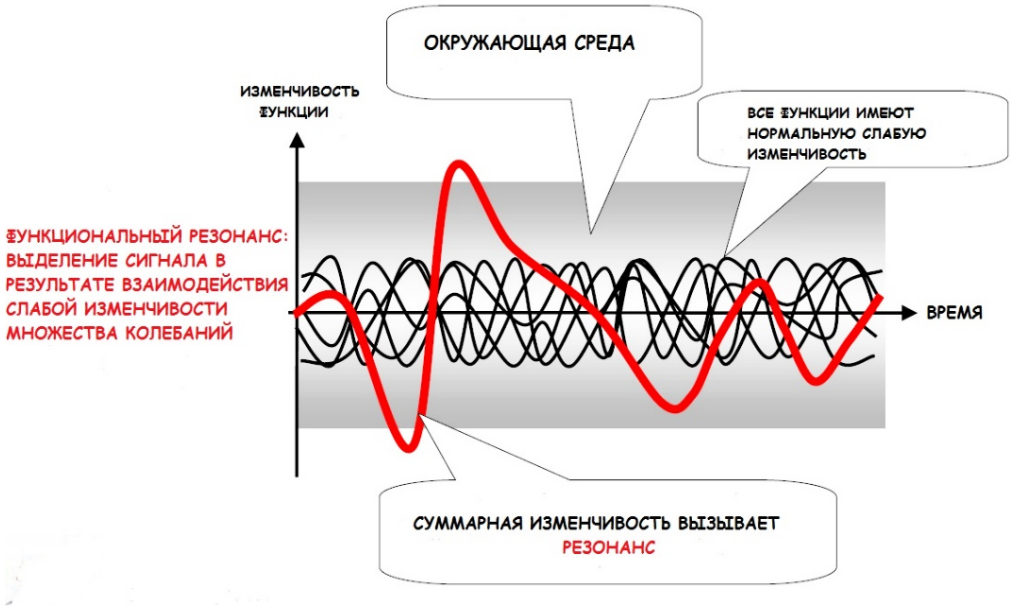


Рисунок 8. Функциональный резонанс

Возможны следующие сочетания:

- Функциональный резонанс (неожидаемый нелинейный результат нормальной изменчивости) (рис. 8).
- Действия, основанные на ожиданиях (обычные действия);

- Неожидаемые последствия (точное предвидение невозможно);
- Комбинация небезопасных действий и латентных условий.

Четыре главных источника изменчивости:

- Люди;
- Технология;
- Латентные условия;
- Барьеры.

В том случае, когда величина изменчивости внутри настолько велика, что система не может ее поглотить – возможен нежелательный исход в виде функционального резонанса, приводящего к тому, что система оказывается неспособной справиться с ним в нормальном операционном режиме [4].

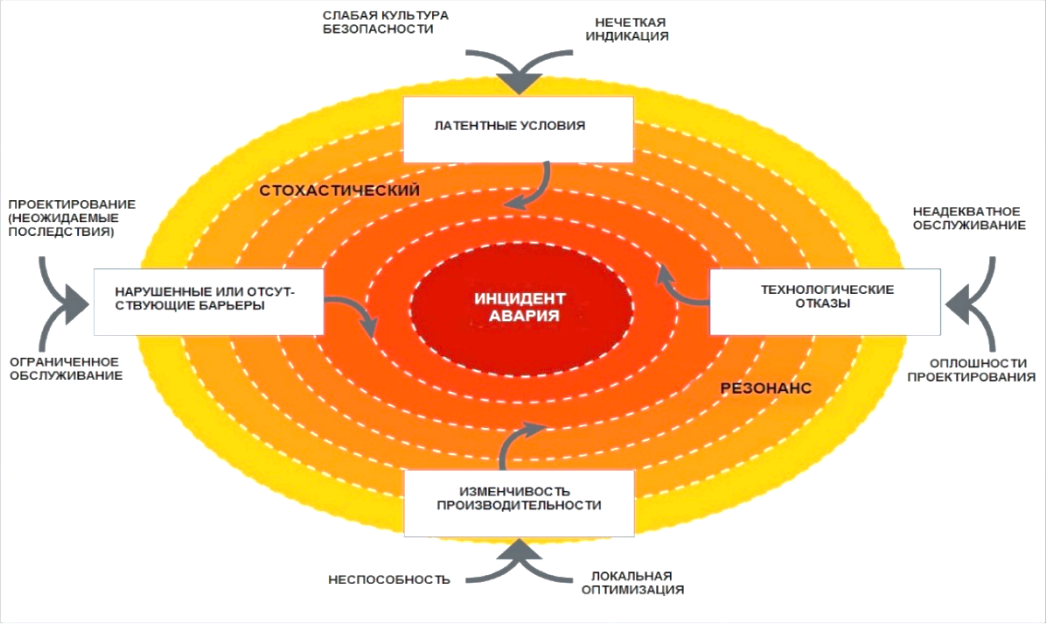


Рисунок 9. Функциональный резонанс как модель аварии (Холлнагель, 2004)

FRAM представляет системную деятельность в виде взаимосвязанных функций, каждая из которых характеризуется входными и выходными данными, предварительными условиями, ресурсами, контролем и временными рамками, что позволяет анализировать нелинейное взаимодействие вариаций этих элементов для получения результатов (рис. 9). В отличие от традиционных моделей оценки рисков, в которых основное внимание уделяется неудачам, в FRAM успехи и неблагоприятные события рассматриваются как результат одних и тех же процессов функционального резонанса, при которых вариации усиливаются или ослабляются за счет взаимосвязей, что позволяет заблаговременно выявлять потенциал устойчивости и уязвимые места. Этот метод был применен для моделирования выполненной работы в динамичных средах, что позволило сделать вывод о том, что устойчивость возникает благодаря способности системы поглощать и адаптироваться к изменениям [4].

К середине 2010-х инженерия резилентной безопасности получила распространение в таких секторах, как авиация, ядерная энергетика, получившая развитие с учетом уроков аварии Фукусимской АЭС, а также высокотехнологическая медицина. В наступившей эпохе резилентной безопасности была отброшена идея линейного причинно-следственного механизма, и эти новые модели фокусируются на процессах с петлями обратной связи информации и управления. Аварии стали рассматриваться как результат несовершенных процессов, вклю-

чающих взаимодействие между людьми, социальными и организационными структурами, инженерной деятельностью, а также физическими и программными компонентами системы.

Традиционные методы, известные как «Безопасность-I», направлены на снижение вариативности за счет стандартизации и поиска виновных, при этом упускается из виду то, как системы регулярно адаптируются для достижения успеха. Инженерия резилентной безопасности, соответствующая концепции «Безопасность-II», рассматривает свойство организации по достижению устойчивости, управляя компромиссами в производительности в режиме реального времени.

По сути, инженерия резилентной безопасности определяет четыре фундаментальные способности, которые позволяют системам успешно функционировать в сложных условиях:

Прогнозирование: предвидение потенциальных изменений, сбоев или возможностей на основе предусмотрительности и мониторинга меняющихся факторов риска [4].

Мониторинг: выявление отклонений или слабых сигналов в режиме реального времени для своевременного обнаружения препятствий и предполагает выявление отклонений и потенциальных проблем путем постоянного наблюдения за сигналами системы.

Это две взаимосвязанные функции, которые позволяют системам сохранять работоспособность в условиях нестабильности и перемен.

Мониторинг направлен на наблюдение за текущим состоянием системы и ее развитием в краткосрочной перспективе с целью выявления аномалий или предпосылок к сбоям, а прогнозирование — на моделирование потенциальных сценариев будущего для подготовки к возникающим рискам или возможностям. Интеграция искусственного интеллекта улучшает мониторинг за счет обработки огромных потоков данных в режиме реального времени, прогнозирования аномалий и поддержки динамической корректировки на критически важных этапах. Эти методы основаны на упреждающем подходе к развитию потенциала, что позволяет заблаговременно реагировать на возникающие угрозы [4].

Реагирование: гибкая корректировка действий обеспечивается за счет надежности элементов, резервирования систем или быстрого восстановления.

Адаптация и оперативность реагирования в инженерии резилентной безопасности — это способность социотехнических систем в режиме реального времени подстраиваться под меняющиеся требования, как ожидаемые, так и возникающие внезапно, а также восстанавливаться после сбоев для поддержания основных функций.

Резервирование ресурсов, избыточных мощностей или свободных ресурсов при планировании процессов, дополнительно повышает гибкость, предоставляя возможности для смягчения последствий потрясений и поиска нестандартных решений.

Человеческий фактор играет здесь вспомогательную роль, поскольку адаптивное поведение операторов способствует оперативному реагированию системы без заранее подготовленных сценариев. Новые методы моделирования позволяют организациям создавать сложные сценарии, тестировать потенциальные уязвимости и учитывать их при проектировании [4].

Обучение: анализ результатов, в том числе успешных и неудачных, для совершенствования будущих адаптаций и устранения разрывов между «идеальным представлением о работе» (замысел проекта) и «реальной работой» (фактическая практика).

Ярким примером создания новых адаптивных возможностей является внедрение в авиационной отрасли системы управления ресурсами экипажа (Crew Resource Management, CRM) после крупных авиакатастроф, которые делают упор на командную коммуникацию и принятие решений в стрессовых ситуациях, и изменили культуру в кабине пилотов, превратив ее из иерархической в культуру сотрудничества. Внедрение принципов инженерии рези-

лентной безопасности в систему CRM снизило количество ошибок и ускорило восстановление после сбоев.

По такому же пути пошел и морской транспорт.

Человеческие ошибки по-прежнему доминируют, составляя значительную долю факторов, способствующим аварии, создавая впечатление, что человеческий фактор является слабым звеном в морской системе. Радикальным методом повышения безопасности на море является полное исключение человеческого фактора. Но даже автономная навигация и беспилотные системы не смогут заменить человека, который принимает окончательное решение.

Поскольку человеческие ошибки невозможно полностью исключить, для их минимизации разработана программа управления ресурсами мостика. В соответствии с требованиями Международной конвенции ПДНВ с поправками подготовка судоводителей по этой программе обязательна для судоводителей. В 2023 году Морской международной организацией одобрен пересмотренный модельный курс 1.22 «Управление ресурсами мостика»

Программа использует целевой подход и содержит как реактивные, так и проактивные элементы. Проактивные элементы связаны с оценкой рисков, а реактивные — с материалами расследований аварий (рис. 10).

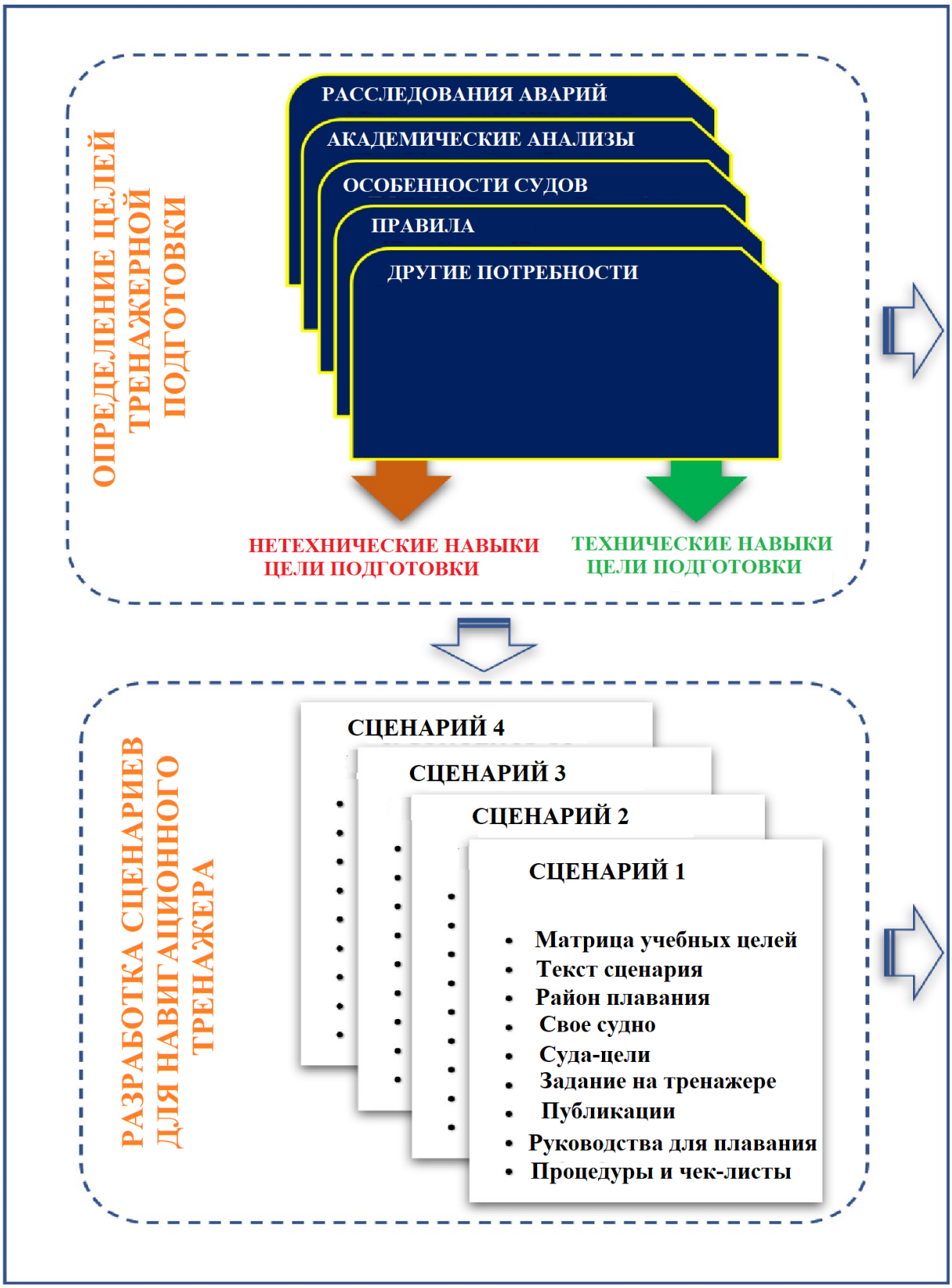


Рисунок 10. Программа «Управление ресурсами мостика»

Управление ресурсами мостика фокусируется на навыках судоводителей, таких как построение команды, взаимодействие в ней, общение, лидерство, принятие решений и управление ресурсами, и включает это в более широкую картину организационного и нормативного

управления. Управление ресурсами занимается управлением оперативными задачами, а также стрессом, отношениями и рисками. Эта концепция признает, что существует множество элементов эффективности и безопасности труда, таких как индивидуальные, организационные и нормативные факторы, и их необходимо предвидеть при осуществлении планирования. Управление ресурсами начинается перед рейсом с плана перехода и продолжается до конца рейса подведением итогов перехода.

Для прохождения этого курса используется полномасштабный навигационный тренажер, имитирующий оборудование мостика и маневренные характеристики тех судов, на которых предполагается работа специалистов, проходящих подготовку, с системой визуализации, воспроизводящей навигационную обстановку и особенности судопотока в предполагаемом районе плавания. Мостик должен быть оборудован имитатором УКВ-радиотелефона, подключенным к инструкторской станции, для связи с лоцманскими станциями, системами управления движением судов (VTS), портовыми службами и другими судами во время занятий. Инструктор будет выступать в роли других станций при ответе на звонки или их инициировании. Аналогично, внутренний телефон в машинном отделении должен быть подключен к инструкторской станции. Должна быть обеспечена возможность подачи звуковых и световых сигналов, требуемых Международными правилами предотвращения столкновений судов в море МППСС-72.

Курс поощряет творческий подход и предоставляет инструктору полную свободу в выборе сценариев тренажерный занятий в соответствии с целями подготовки. В качестве материалов для разработки сценариев используются доклады по расследованию аварийных случаев, публикации авторитетных организаций морской отрасли, морские навигационные карты и пособия, процедуры и чек-листы. Сценарии должны учитывать влияние ветра и течения, влияние мелководья, влияние берега/канала, взаимодействие мостика и лоцмана, постановка на якорь/швартовка и чрезвычайные ситуации, такие как неисправность руля, отказ двигателя, отказ навигационных средств и т.п.

На заключительном этапе проводится разбор и сбор отзывов от обучающихся для дальнейшего развития и улучшения содержания курса. Цели обучения и упражнения на тренажере должны разрабатываться инструкторами. Сценарии, которые необходимо выполнить, должны быть составлены с учетом соответствия оборудования и функций тренажера, а также предварительных требований целевой группы обучающихся. Объем, сложность и реалистичность задач варьируются в зависимости от оборудования и функций тренажера, а также целевой группы.

Итоговое оценивание предназначено для измерения достижений обучающихся в соответствии с определенными целями и показателями эффективности. Оно может принимать форму экзамена или задания и проводится в конце курса. Цель итогового оценивания — оценить обучающихся и определить, достигли ли они требуемого уровня компетентности. При оценке достижения компетентности в таблице A-II/1 Кодекса ПДНВ инструкторы должны руководствоваться критериями оценки компетентности в столбце 4 таблицы и результатами обучения, указанными в подробном описании [5].

Аналогичным принципам следует курс «Управление ресурсами машинного отделения», цель которого лучшее понимание инженерных систем и оборудования судна, отработка процедур для повышения безопасности и снижения вероятности ошибочных действий при эксплуатации судовой силовой установки [7, 8, 9].

Дальнейшее развитие технология обучения моряков получила в программе «Управление морскими ресурсами» (Maritime Resource Management - MRM), которая стремится к развитию позитивного отношения, хорошей личной коммуникации, лидерских качеств и соблюдению операционных процедур в рамках управления рисками на рабочем месте. Поскольку курс

MRM фокусируется на вопросах человеческого фактора, а не на конкретных технических задачах, он идеально подходит для всех дисциплин и уровней, как палубных, машинных, так и береговых.

Условия работы экипажа быстро меняются, и тренажерная подготовка призвана способствовать адаптации человеческих возможностей. Только за последние десятилетия мы стали свидетелями следующих изменений:

- усложнение технических систем и широкое использование автоматизации и дистанционного управления;
- сокращение численности экипажей, многонациональность экипажей, меняющиеся стандарты обучения;
- изменение условий эксплуатации и коммерческой деятельности; и
- более требовательная и сложная нормативно-правовая среда.

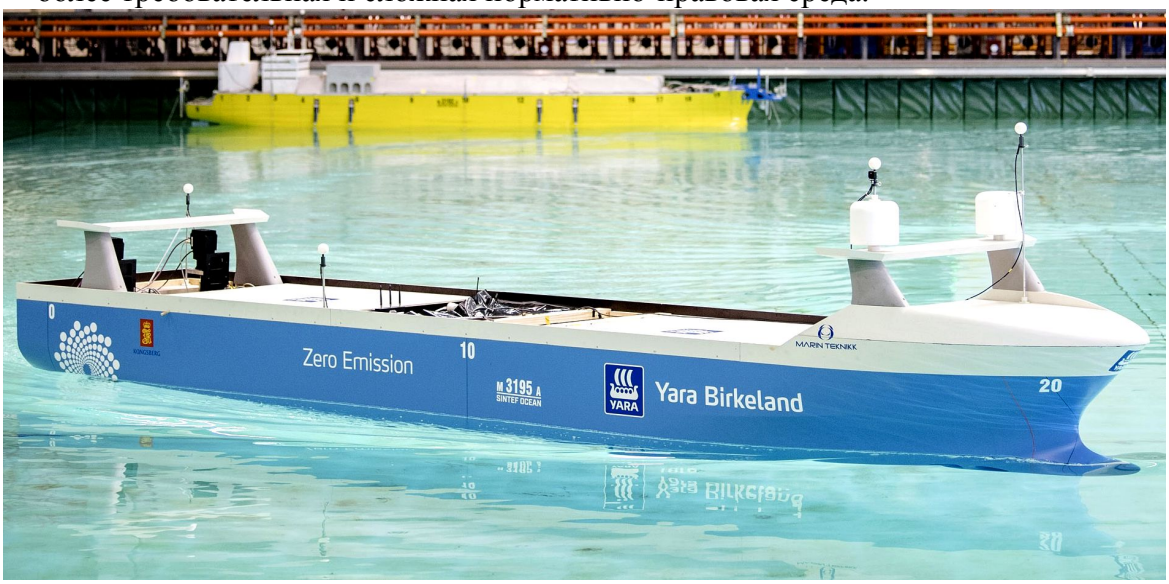


Рисунок 11. Первый в мире автономный контейнеровоз «Yara Birkeland»

Новые вызовы связаны с бурным развитием автономно действующих судов без экипажа (рис. 11). Резилентность в контексте морских автономных надводных судов (MASS) — это способность системы сохранять работоспособность и обеспечивать безопасность при воздействии внешних угроз, сбоев, кибератак или неблагоприятных условий морской среды. Для MASS это критически важно, так как они используют передовые технологии — искусственный интеллект, сенсоры, системы связи и управления, которые повышают эффективность, но одновременно создают новые риски [6].

Список литературы

1. “Our seamen. An Appeal” by Samuel Plimsol [Электронный ресурс] – Режим доступа:// https://archive.org/details/ourseamenanappe00plimgoog.
2. Managing Maritime Safety. Edited by Oltedal H. Routeledge Taylor & Fransis Group. London, New York, 2018 p.189.
3. Мотрич В.Н. Горькие уроки морских аварий – Санкт-Петербург: ООО «Морсар», 2015 – 336 с.
4. Hollnagel E., Woods D., Leveson N. Resilience engineering: concepts and percepts. Ashgate, Aldershot, England; Burlington, VT, p. 397.

5. Bridge Resource Management Guidance. UK Chamber of Shipping. Witherby Publishing Groupe, London, 2020. P.65.
6. Haugen S., Kristiansen S., Maritime Transportation Safety Management and Risk Analisis. Second Edition, Routeledge Taylor & Fransis Group. London, New York, 2023 p.673.
7. Глазюк Д.К., Соболенко А.Н. Мероприятия по обеспечению безаварийной работы и реальная практика аварий дизелей на судах промыслового флота. «Рыбное хозяйство» № 4, - М:, 2012 г. с. 104 - 107.
8. Соболенко А.Н. Характерные аварийные отказы судовых дизелей в эксплуатации по причине человеческого фактора. Морские интеллектуальные технологии. № 3(33) Т.1. 2016. С. 173-179.
9. Гомзяков М.В., Соболенко А.Н. Анализ причин некоторых аварийных случаев судовых энергетических установок в Дальневосточном регионе в 2020 году. Морские интеллектуальные технологии. 2021.№ 4-3 (54). С. 72-78.

Поступила в редакцию 25 июня 2026 г.

УДК 629.5: 629.12.06.003.1

Киберустойчивость портовой инфраструктуры и морских цепочек поставок

Рогозин Михаил Валериевич, курсант, e-mail: fertheraserg@gmail.com

МГУ им. адм. Г. И. Невельского, Владивосток

В статье исследуется проблема киберустойчивости портовой инфраструктуры и морских цепочек поставок. Цель работы состоит в определении уязвимых зон портовых операционных систем, автоматизированных терминалов, бортовых OT-систем и сервисов поставщиков оборудования. Новизна исследования заключается в представлении порта и судна как единой цифровой цепочки, где сбой одного участника способен вызвать каскадное нарушение перевозочного процесса. Предложена модель распределения мер защиты между организационным, техническим и межорганизационным уровнями.

Ключевые слова: портовая инфраструктура, цепочка поставок, OT-системы, PCS, киберустойчивость, IACS UR E26, IACS UR E27.

Cyber resilience of port infrastructure and maritime supply chains

Rogozin Mikhail V., e-mail: fertheraserg@gmail.com

Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

The article studies the cyber resilience of port infrastructure and maritime supply chains. The pur pose is to identify vulnerable areas of port community systems, automated terminals, shipboard OT systems and equipment supplier services. The novelty of the research is the presentation of the port and the ship as a single digital chain, where a failure of one participant can cause cascading disruption of transport operations. A model for distributing protective measures among organizational, technical and interorganizational levels is proposed.

Keywords: port infrastructure, supply chain, OT systems, PCS, cyber resilience, IACS UR E26, IACS UR E27.

Порт и судно все чаще функционируют как части единой цифровой цепочки. Портовые операционные системы, электронный документооборот, автоматизированные терминалы, системы планирования грузовых операций, сервисы таможенного оформления и оборудование поставщиков связаны между собой непрерывным обменом данными. Такая взаимосвязанность позволяет ускорять обработку грузов, сокращать время стоянки, повышать прозрачность логистики и уменьшать количество бумажных процедур. Одновременно она создает новую зависимость морских перевозок от доступности и достоверности цифровых сервисов.

Если в судовой навигации киберинцидент чаще проявляется как угроза конкретному рейсу, то в порту его последствия могут распространяться на множество судов, терминалов, перевозчиков, экспедиторов и государственных органов. Нарушение работы Port Community System, терминальной операционной системы или сервиса поставщика оборудования способно вызвать задержки оформления, невозможность принять или выдать контейнер, ошибку в грузовом плане, блокировку складских операций и рост очереди судов. Поэтому кибербезопасность портовой инфраструктуры является не только технической, но и организационно-экономической задачей.

Международная ассоциация портов и гаваней отмечает, что усиление цифровизации портовых сообществ требует расширения диалога по кибербезопасности между государственными и частными участниками [3]. Всемирный банк рассматривает Port Community System как платформу обмена данными между судовладельцами, перевозчиками, терминальными операторами, экспедиторами, таможенными и портовыми органами, предназначенную для повышения эффективности, безопасности и надежности торговых операций [4]. Следовательно, компрометация такой платформы влияет не на один компьютер, а на согласованность работы всей логистической среды.

Цель статьи - определить основные факторы киберустойчивости портовой инфраструктуры и морских цепочек поставок. Для достижения цели решаются задачи: выделить уязвимые элементы портовой цифровой среды; описать влияние бортовых OT-систем на общую устойчивость перевозочного процесса; рассмотреть риски поставщиков оборудования и программного обеспечения; предложить модель распределения защитных мер между участниками морской цепочки поставок.

Методы

Работа основана на системном анализе портовой и цепочечной кибербезопасности. В качестве источников использованы рекомендации ИМО, документы IAPH по кибербезопасности портовых сообществ, материалы Всемирного банка по PCS, требования IACS UR E26 и UR E27, исследования по кибербезопасности портовых систем и открытые сведения о влиянии атаки NotPetya на транспортно-логистическую деятельность [1-8].

Объект исследования - цифровая инфраструктура морской цепочки поставок. В ее состав включены портовые операционные системы, автоматизированные терминалы, системы взаимодействия с таможенными и портовыми органами, сервисы планирования грузовых операций, бортовые OT-системы судна и сервисы производителей оборудования. Предмет исследования - уязвимости, возникающие на стыке организационных границ: судно - порт, терминал - перевозчик, производитель - судовладелец, государственный орган - частный оператор.

Методика включает три этапа. На первом этапе проводится декомпозиция инфраструктуры на функциональные уровни: организационный, информационный, операционно-технологический и межорганизационный. На втором этапе для каждого уровня определяются типовые сценарии нарушения конфиденциальности, целостности и доступности. На третьем этапе предлагаются меры защиты и определяется, какой участник цепочки должен нести ответственность за их выполнение.

Ключевым допущением исследования является то, что портовая киберустойчивость не может быть обеспечена силами одного IT-подразделения. Поскольку цифровая цепочка

включает множество самостоятельных организаций, для устойчивости необходимы единые правила обмена информацией об инцидентах, согласованные требования к подключению внешних систем и распределение ответственности за восстановление.

Решение задачи: модель киберустойчивости цепочки

Портовая цифровая среда отличается от судовой тем, что в ней одновременно взаимодействуют участники с разной степенью зрелости кибербезопасности. Крупный терминальный оператор может использовать современные средства мониторинга, но подключенный экспедитор или небольшой подрядчик может иметь слабую защиту учетных записей и устаревшие рабочие станции. Злоумышленник выбирает не самый важный, а самый доступный узел. После этого он пытается использовать доверенные связи для перехода к более значимым системам.

Первый уровень модели - организационный. Он включает политику кибербезопасности порта, распределение ролей, обучение персонала, порядок сообщения об инцидентах и процедуры восстановления. Основная ошибка на этом уровне состоит в том, что кибербезопасность иногда воспринимается как вопрос отдельного технического специалиста. В действительности нарушение PCS или терминальной системы влияет на коммерческие обязательства, расписание судозаходов, взаимодействие с государственными органами и репутацию порта.

Второй уровень - информационный. Он охватывает документы, заявки, электронные разрешения, данные о грузах, контейнерах, судозаходах, опасных грузах и платежах. Нарушение целостности таких данных может иметь не менее серьезные последствия, чем отказ оборудования. Например, ошибочная информация о грузе или контейнере способна привести к неправильному размещению, задержке оформления или нарушению требований безопасности. Поэтому для PCS важны не только резервные копии, но и контроль полномочий, журналирование изменений, подтверждение критических операций и возможность проследить источник данных.

Третий уровень - операционно-технологический. Он включает автоматизированные краны, терминальное оборудование, системы управления доступом, видеонаблюдение, энергоснабжение, грузовые и балластные системы судов, а также интерфейсы обмена с бортовыми OT-системами. На этом уровне особенно опасно смешение IT и OT без контролируемых шлюзов. Если офисная сеть, сервисный ноутбук или удаленный доступ поставщика имеют прямой путь к технологическим контроллерам, то обычный фишинговый инцидент может привести к физическому простою терминала или ошибке в грузовой операции.

Четвертый уровень - межорганизационный. Он связан с поставщиками оборудования, программного обеспечения, облачных сервисов и технической поддержки. Атака на поставщика может быть выгоднее атаки на конкретный порт, потому что один поставщик обслуживает множество клиентов. Для морской отрасли это особенно актуально из-за длительного срока эксплуатации оборудования и зависимости от специализированных производителей. Требования IACS UR E26 и UR E27 направлены на повышение киберустойчивости судов и бортовых систем, в том числе за счет более системного подхода к проектированию и поставке оборудования [2].

Таблица 1 – Уровни киберустойчивости портовой цифровой цепочки

Уровень модели	Уязвимые элементы	Типовой сценарий	Ответственные участники
Организационный	Политики, персонал, процедуры реагирования	Позднее обнаружение инцидента и несогласованные действия служб	Администрация порта, оператор терминала, служба безопасности
Информационный	PCS, электронные заявки, данные о грузах и судозаходах	Подмена сведений, блокировка оформления, нарушение прослеживаемости операций	Оператор PCS, таможенные и портовые органы, перевозчики
Операционно-технологический	Краны, системы доступа, энергоснабжение, бортовые OT-интерфейсы	Переход из офисной сети к технологическому оборудованию и остановка операций	Терминальный оператор, судовладелец, сервисные организации
Межорганизационный	Поставщики ПО, производители оборудования, облачные сервисы	Компрометация обновлений или удаленной поддержки с воздействием на многих клиентов	Поставщик, классификационное общество, судовладелец, порт

Результаты

В результате анализа установлено, что ключевым свойством портовой киберустойчивости является способность сохранять минимально допустимый уровень операций даже при частичной компрометации цифровых сервисов. Для этого недостаточно иметь резервную копию базы данных. Необходимо заранее определить, какие процессы можно перевести на ручной режим, какие операции должны быть остановлены до проверки данных, кто принимает решение о возобновлении работы и как участники цепочки получают достоверную информацию.

Первым практическим результатом является необходимость единого реестра критических цифровых зависимостей. В него должны входить PCS, терминальная операционная система, каналы связи с таможней, сервисы планирования погрузки, системы контроля доступа, серверы обновлений, учетные записи поставщиков и удаленные подключения. Без такого реестра невозможно определить, какой сервис является критическим, а какой может быть временно отключен без угрозы для безопасности и непрерывности перевозок.

Вторым результатом является приоритет сегментации и контролируемого обмена между IT и OT. Офисные системы должны быть отделены от технологического оборудования, а удаленный доступ поставщиков должен предоставляться по временным правилам, с многофакторной аутентификацией, журналированием и последующим отключением. Для портов и терминалов это особенно важно, поскольку на одной площадке взаимодействуют собственные сотрудники, подрядчики, экипажи судов, агенты и представители государственных органов.

Третьим результатом является необходимость совместного реагирования. Если порт скрывает инцидент из-за опасений репутационных потерь, судовладельцы и перевозчики не смогут своевременно изменить планы. Если судно не сообщает о подозрительном файле грузового плана, терминал может получить зараженный документ. Поэтому обмен информацией

об инцидентах должен быть встроен в договорные и эксплуатационные процедуры, а не зависеть только от добровольной инициативы отдельных сотрудников.

Таблица 2 – Практические меры повышения киберустойчивости

Мера защиты	Содержание меры	Практический результат
Единая политика кибербезопасности портового сообщества	Согласованные требования к подключению участников, обмену данными и уведомлению об инцидентах	Снижение хаоса при атаке и единое понимание обязанностей
Сегментация IT и OT	Физическое или логическое разделение офисных систем и технологического оборудования	Ограничение перехода атаки к кранам, доступу, энергоснабжению и грузовым операциям
Контроль поставщиков и обновлений	Проверка цифровых подписей, учет удаленного доступа, требования к безопасной разработке	Снижение риска атаки через доверенный сервисный канал
Планы ручного режима	Описание операций, которые могут выполняться при недоступности PCS или терминальной системы	Поддержание минимальной непрерывности и безопасное восстановление
Совместные учения	Сценарии с участием порта, терминала, судна, агента и государственных органов	Проверка готовности всей цепочки, а не отдельной организации

Выводы и обсуждение

Портовая инфраструктура и морские цепочки поставок образуют сложную цифровую систему, в которой технологические, коммерческие и административные процессы взаимно зависят друг от друга. Поэтому киберинцидент в порту нельзя оценивать только по количеству зараженных компьютеров. Его реальная тяжесть определяется влиянием на судозаходы, обработку грузов, достоверность данных, безопасность терминальных операций и способность участников цепочки восстановить работу.

Предложенная модель показывает, что киберустойчивость должна строиться на четырех уровнях: организационном, информационном, операционно-технологическом и межорганизационном. На каждом уровне должны быть определены собственные угрозы, меры контроля и ответственные участники. Особое значение имеет межорганизационный уровень, поскольку современные атаки часто используют доверенные связи с подрядчиками, производителями оборудования и поставщиками программного обеспечения.

Для практического применения рекомендуется создать реестр критических цифровых зависимостей, внедрить единые правила подключения внешних участников, отделить технологические сегменты от офисных сетей, контролировать удаленный доступ поставщиков, регулярно проводить совместные учения и закрепить порядок обмена информацией об инцидентах. Дальнейшие исследования целесообразно направить на количественную оценку эко-

номических потерь от остановки PCS и на моделирование каскадных задержек судов при отказе одного или нескольких цифровых сервисов порта.

Список литературы

1. Guidelines on Maritime Cyber Risk Management : MSC-FAL.1/Circ.3/Rev.3. – London : International Maritime Organization, 2025. – 9 p. – URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf (дата обращения: 15.05.2026).
2. IACS UR E26 and E27 Press Release. – London : International Association of Classification Societies, 2023. – URL: https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release (дата обращения: 15.05.2026).
3. Port Community Cyber Security. – Antwerp : International Association of Ports and Harbors, 2020. – 16 p. – URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf (дата обращения: 15.05.2026).
4. Port Community Systems: Driving Trade in the 21st Century. – Washington : World Bank Group, 2024. – 60 p. – URL: https://documents1.worldbank.org/curated/en/099092624152038561/pdf/P176587-54dd3e7b-e083-43cc-9df3-10b441697c0d.pdf (дата обращения: 15.05.2026).
5. Meyer-Larsen, N. Enhancing the Cybersecurity of Port Community Systems / N. Meyer-Larsen, R. Müller // Dynamics in Logistics: Proceedings of the 6th International Conference LDIC 2018. – Cham : Springer, 2018. – P. 318–323. – DOI: 10.1007/978-3-319-74225-0_43.
6. Eichenhofer, J. O. An In-Depth Security Assessment of Maritime Container Terminal Software Systems / J. O. Eichenhofer, E. Heymann, B. P. Miller, A. Kang. – 2020. – URL: https://arxiv.org/abs/2006.12056 (дата обращения: 15.05.2026).
7. Cyber Security for Ports and Port Systems. Code of Practice. – London : Department for Transport, 2020. – 75 p. – URL: https://assets.publishing.service.gov.uk/media/5e284eefe5274a6c3ee68fcd/cyber-security-for-ports-and-port-systems-code-of-practice.pdf (дата обращения: 15.05.2026).
8. A. P. Moller - Maersk. Risk Management. Annual Report 2017. – Copenhagen : A. P. Moller - Maersk, 2018. – 5 p. – URL: https://investor.maersk.com/static-files/d533735a-5df7-423c-8611-d4a2c3bf31b0 (дата обращения: 15.05.2026).

Поступила в редакцию 5 июня 2026 г.

СУДОВЫЕ ЭНЕРГЕТИЧЕСКИЕ УСТАНОВКИ И ИХ ЭЛЕМЕНТЫ

УДК 621.892.096: 629.3

Саморегенерирующиеся фильтры повышенной эффективности для отчистки горюче-смазочных материалов на судах: анализ конструкции и моторная эффективность

Фролов Евгений Владимирович, аспирант [1],
Мойсейченко Данил Денисович, аспирант [1],
Кича Геннадий Петрович, доктор технических наук, доцент [1], e-mail: kicha@msun.ru

[1] Морской государственный университет имени адмирала Г.И. Невельского, г. Владивосток

Обоснована актуальность исследований, нацеленных на проектирование судовых устройств для фильтрования горюче-смазочных материалов, отличающихся высокими параметрами по тонкости отсева и пропускной способности. Выявлены недостатки существующих аналогов, выражающиеся в неудовлетворительной очистки, слабой регенерационной способности и малом ресурсе автономной работы фильтров, что ограничивает возможность использование таких аппаратов в современных автоматизированных судовых энергосистемах.
Акцентировано внимание на проблеме износа судовых дизелей, вызванных переходом на высоковязкое малосернистое топливо, содержащее абразивные включения, образующиеся в ходе каталитического крекинга нефтепродуктов. Для минимизации негативных последствий указана необходимость обеспечения надежной и эффективной подготовки топлива и смазочных материалов на протяжении длительного периода (3–5 тыс. ч) без участия обслуживающего персонала.
Предложены и аргументированы основные пути усовершенствования конструкций саморегенерирующихся фильтров, где ключевая роль отводится применению специализированных тканых фильтровальных материалов с оптимальной поровой структурой, гарантирующей высокий уровень отделения примесей и легкую регенерацию. Представлена конструкция фильтрующего элемента свечного типа, позволяющая увеличить прочность изделия, повысить долю свободного пространства и эффективность задействования всей площади фильтрации как в рабочем цикле, так и при промывке.
Детально рассмотрены новаторские подходы к компоновке и работе фильтровальных блоков в режиме регенерации, предполагающие последовательное воздействия на отсеивающую перегородку потока жидкости, воздушной эмульсии и сжатого воздуха, что гарантирует высококачественное удаление загрязнений. Отмечена возможность адаптации процесса регенерации фильтра в зависимости от природы загрязнений и характеристик используемого фильтровального материала.
Проведенные испытания продемонстрировали существенное повышение надежности защиты дизельного двигателя от преждевременного изнашивания благодаря комбинации в системе смазки полноценного полнопоточного фильтрования и дополнительного центробежного сепарирования. Эксплуатация нового устройства позволила замедлить процесс старения смазочного масла и продлить период его бесперебойной работы даже в тяжелых условиях эксплуатации двигателей повышенной фарсировки, функционирующих на низкокаче-

ственных сортах топлива. Длительность непрерывной работы предлагаемого саморегенерирующегося фильтра достигает заявленного показателя в 3–5 тыс. ч без проведения профилактических мероприятий.
Экспериментальные исследования подтвердили, что новая система превосходит традиционные схемы очистки масла, обеспечивая сокращение степени износа силовых агрегатов на 40–60 %, экономное расходование горюче–смазочных материалов и значительное повышение моторесурса судовой энергетической установки.

Ключевые слова: судовые дизели, саморегенерирующийся фильтр, очистка моторного масла, фильтрующие элементы, тканые фильтровальные сетки, регенерация фильтра маслоочистительный комплекс, автономность работы фильтра, абразивный износ, комбинированная очистка, центробежный сепаратор, высоковязкое топливо.

Self-Regenerating High-Efficiency Filters for Purification of Fuels and Lubricants on Ships: Design Analysis and Engine Efficiency

Frolov Evgeny V.,[1]
Moiseychenko Danil D.,[1]
Kicha Gennady P. [1], e-mail: kicha@msun.ru

[1] Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

The relevance of research aimed at designing marine filtration units for fuels and lubricants with high performance in terms of filtration fineness and throughput capacity is substantiated. The shortcomings of existing analogues are identified, including unsatisfactory purification efficiency, poor regeneration capability, and a short autonomous operating life of the filters, which limits the applicability of such devices in modern automated marine power systems.
Attention is drawn to the problem of wear in marine diesel engines caused by the transition to high-viscosity low-sulphur fuels containing abrasive particles generated during catalytic cracking of petroleum products. To minimise the negative consequences, the necessity is indicated for ensuring reliable and efficient conditioning of fuel and lubricants over a long period (3,000–5,000 hours) without operator intervention.
The main directions for improving the design of self-regenerating filters are proposed and justified, with a key role assigned to the use of specialised woven filter materials with an optimal pore structure that guarantees a high level of contaminant removal and easy regeneration. A candle-type filter element design is presented, which increases product strength, enhances the proportion of free space, and improves the utilisation of the entire filtration area both in the working cycle and during backwashing.
Innovative approaches to the layout and operation of filter banks in the regeneration mode are examined in detail, involving the sequential action on the filter medium of a liquid flow, an air emulsion, and compressed air, which ensures high-quality contaminant removal. The possibility of adapting the regeneration process depending on the nature of contaminants and the characteristics of the filter medium is noted.
Conducted tests have demonstrated a significant improvement in the reliability of diesel engine pro tection against premature wear, thanks to a combination of full-flow filtration and additional cen-

trifugal separation in the lubrication system. Operation of the new device made it possible to slow down the ageing of the lubricating oil and extend its trouble-free service life even under severe operating conditions of highly boosted engines running on low-grade fuels. The continuous operation time of the proposed self-regenerating filter reaches the specified 3,000–5,000 hours without preventive maintenance.
Experimental studies have confirmed that the new system outperforms traditional oil purification schemes, reducing wear of power units by 40–60 %, ensuring economical consumption of fuels and lubricants, and significantly increasing the service life of the marine power plant.

Keywords: marine diesel engines, self-regenerating filter, engine oil purification, filter elements, woven filter meshes, filter regeneration, oil cleaning complex, autonomous filter operation, abrasive wear, combined purification, centrifugal separator, high-viscosity fuel.

Введение. Проблематика энергосбережения и увеличения межремонтного срока службы судовых энергетических установок обретает всё большую значимость на фоне растущего спроса на высококачественное топливо и моторные масла. Тем не менее, текущие условия эксплуатации подразумевают широкое применение низкосортных видов топлива, получаемых методом каталитического крекинга нефти, которые содержат частицы алюминия и кремния размером 5–20 мкм, оказывающие крайне разрушительное воздействие на двигатель. Указанные вещества обладают ярко выраженными абразивными характеристиками, провоцируя ускоренный износ ключевых звеньев двигателя, таких как цилиндра-поршневая группа, подшипниковые узлы и детали топливной аппаратуры.

Для уменьшения негативного влияния перечисленных факторов необходимо внедрение результативных средств очистки горюче-смазочных материалов, способных обеспечить надежную работу механизмов в составе судовых энергоустановок. Анализ показывает, что наиболее перспективным вариантом являются фильтры с самовосстанавливающимися характеристиками, позволяющие достигать высоких показателей долговечности и работоспособности фильтрующихся элементов без частых профилактических вмешательств. Такие фильтры способны непрерывно функционировать в течение продолжительного времени, значительно продлевая ресурс основных агрегатов и повышая общую надежность энергоснабжения судна.

Разработчики новых типов самовосстанавливающихся фильтров (СРФ) опираются на накопленный опыт и итоги предыдущих исследований, направляя усилия на достижение максимальной технологической и экономической результативности создаваемых изделий. Это достигается путем оптимизации структурных параметров фильтровальных материалов, совершенствования конструктивных решений и внедрения прогрессивных технологий обработки загрязненных рабочих сред. Применение таких фильтров позволяет существенно снизить затраты на техническое обслуживание и ремонт, одновременно повышая экологическую безопасность и чистоту эксплуатации морского транспорта.

Принципы проектирования объекта исследований и его конструктивные особенности

В разработанных аналитических схемах для саморегенерирующихся фильтров было обоснована целесообразность использования тканых полотен с перекрестным переплетением нитей. Данный тип фильтрованного материала обеспечивает повышенную эффективность извлечения твёрдых нерастворимых частиц из горюче-смазочных жидкостей и отличается высокой степенью восстановления исходных эксплуатационных характеристик после очист-

ки. На базе совокупности теоретических выводов и экспериментальных данных были определены главные направления совершенствования рабочего процесса СРФ. Эти направления в дальнейшем были материализованы в новых технических решениях при создании модернизированных автоматизированных аппаратов для подготовки топлива и смазочных материалов.

При разработке СРФ нового поколения приоритетной задачей являлось оснащение судовой автоматизированной фильтровальной системы компонентами, способными гарантировать её безотказную работу при высокой пропускной способности. Применительно к контуру смазки судового дизеля такая установка включает (рис. 1): грязеотстойник, контрольный (индикаторный) фильтр, а также объединённый очистной модуль из СРФ и тарельчатого центробежного сепаратора. Данная компоновка подтвердила свою эффективность даже в аварийно-напряжённых условиях эксплуатации [3], когда дизель работал с высокой степенью фарсировки по среднему эффективному давлении на тяжёлых вязких топливах.

Новый вектор развития конструкций СРФ потребовал значительного повышения скорости потока промывочной жидкости [3]. Указанный эффект достигается формированием мощного импульса промывки за счёт создания высокого давления продувки и увеличения площади проходного сечения клапана сброса «грязного» потока. Использование многофазной промывочной среды с последующей дополнительной продувкой сжатым воздухом интенсифицирует удаление накаливающихся осадков. Внедрение адаптивного алгоритма, в котором частота и продолжительность цикла регенерации автоматически подстраиваются под адгезионные свойства загрязнений, обеспечивает высокую степень автономности функционирования СРФ [4].

С инженерной точки зрения наиболее оптимальной формой был признан фильтрующий элемент, выполненный в виде свечи. Такая геометрия обеспечивает наилучшие прочностные параметры и качественный смыв накопленных загрязнителей. Пружинный несущий каркас придаёт фильтрующей основе необходимую механическую жесткость и сохраняет хорошую пропускную способность. Переменный шаг намотки проволоки формирует предпосылки для максимального задействования всей площади фильтрующей поверхности как при очистке среды, так и при проведении регенерации. Проведённые теоретические исследования позволили воспроизвести в расчётных моделях процессы фильтрования и восстановления, обеспечив высокую тонкость отделения и полноту извлечения нерастворимых частиц из горюче-смазочных сред при одновременной качественной очистке самих фильтрующих элементов от накопившегося шлама.

Основным достоинством тканой сетки с полотняным переплетением является возможность регулирования его задерживающей способности и легкости восстановления путём изменения геометрических параметров переплетения сетчатой структуры. Подбирая рациональные соотношения между шагом основы, диаметром продольных и поперечных проволок (нитей), можно добиться того, что преобладающая масса загрязнителей будет осаждаться именно на внешней стороне сетчатого полотна, что существенно облегчает их последующее удаление промывкой. Кроме того, подобная структурная организация позволяет реализовать двухступенчатую фильтрацию, при которой в процессе разделения примесей задействованы как наружные, так и внутренние области фильтрующей перегородки [4].

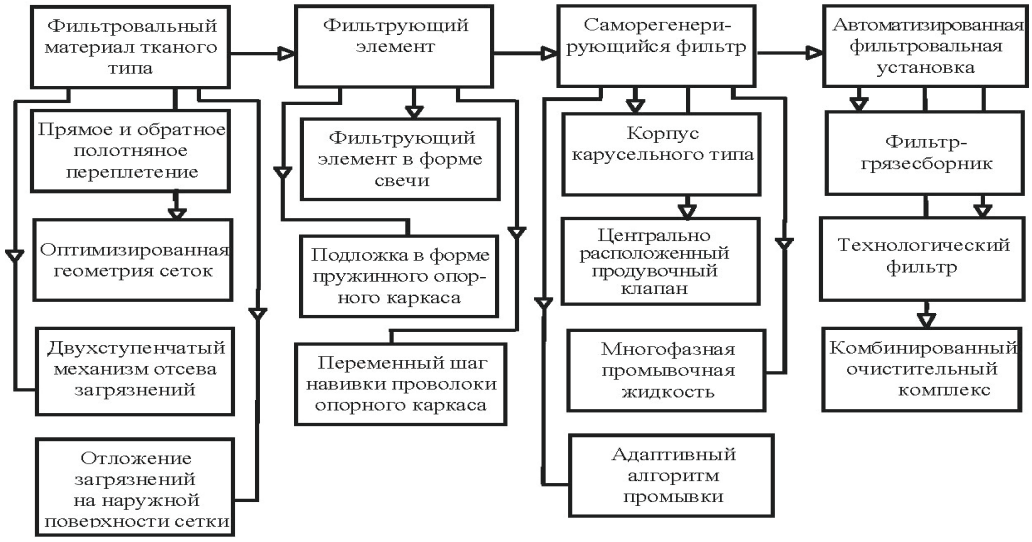


Рис. 1. Новые научно-технические решения по совершенствованию СРФ

Устройство саморегенерирующегося фильтра и принцип его действия

Очистной аппарат проектировался для работы в автоматизированных судовых энергосистемах. Он предназначен для подготовки моторных масел с высокими моюще-диспергирующими показателями, а также низкокачественных топлив, загрязнения которых имеют повышенную адгезию к фильтрующей перегородке. Пропускная способность масляного очистителя варьируется от 120 до 360 м³/ч в зависимости от числа установленных фильтровальных камер (от 2 до 6). Номинальная тонкость задержания частиц при очистке масла составляет 30–50, для топливной – 10–20 мкм. Топливный вариант фильтра имеет не более трёх камер и пропускную способность до 30 м³/ч.

Конструктивное исполнение фильтра типа СРФД включает следующие основные сборочные единицы (рис. 2): опорное основание (поз. 1), корпус (поз. 2), фильтровальные секции (поз. 3) с размещёнными внутри них элементами (поз. 4). В корпусном узле выполнены сообщающиеся магистрали, обозначенные литерами А и Б, которые служат для подвода загрязнённой и отвода очищенной жидкости к секциям. Здесь же находится общий коллектор для направления чистого масла или топлива потребителю. На фундаментной плите фильтра имеются аналогичный патрубок для входа очищаемой среды и патрубок для удаления отработанных загрязнений.

В центральной части корпуса установлены переключатель потоков (поз. 5) и распределительный золотник (поз. 6). Последний вмонтирован в камеру продувочного воздуха (поз. 7), закреплённую на корпусе фильтра. На этой камере смонтирован переходной патрубок для крепления электромеханического привода (поз. 8) поворотного механизма переключателя. Камера продувки воздухом оснащена впускным клапаном с электрическим управлением (поз. 11) и обратным клапаном (поз. 10). Переключатель потоков 5 разделяет внутри корпуса полости с грязной и чистой жидкостью, а также распределяет её по фильтровальным секциям. Кроме того, он генерирует обратный поток, необходимый для выноса отложений из секций и с поверхности фильтрующих элементов.

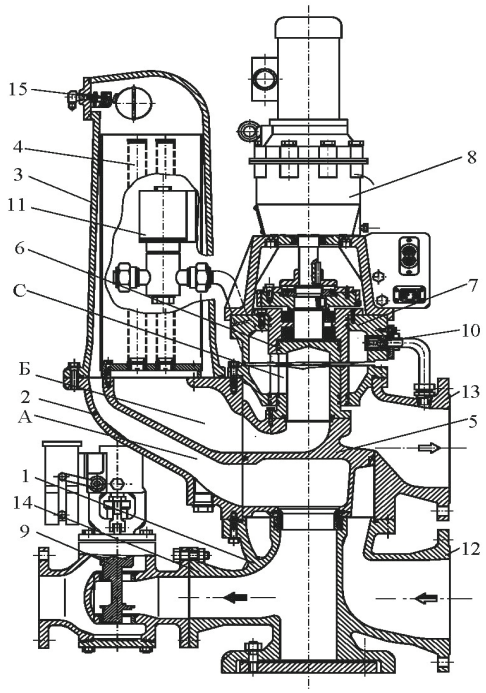


Рис. 2. Саморегенерирующийся фильтр СРФД-120

Фильтровальные секции 3 зафиксированы на корпусной детали вертикально по окружности на равном удалении от продольной оси фильтра. В зависимости от типоразмера очистителя одна секция может содержать от 10 до 20 фильтрующих элементов. В верхней части каждой секции имеется поплавковое устройство с обратным клапаном, служащее для удаления накапливающейся воздушной фазы.

Принцип работы фильтра

Неочищенное топливо или масло поступает в нижнюю кольцевую полость А, отверстия которой расположены по периметру центральной цилиндрической полости корпуса. Через эти отверстия жидкость направляется к фильтрующим элементам, размещённым внутри секций, где и происходит её очистка. Жидкость, прошедшая этап фильтрации, из внутреннего объёма элементов перемещается в полость чистого продукта Б и далее через выпускной патрубок 13 подаётся конечному потребителю.

Режим фильтрации активен для всех секций, доступ которых из приёмной зоны 12 через полость А открыт, а полость Б соединена с внутренней полостью выпускного патрубка 13. Фильтрация осуществляется при смещении выступа (хобота) переключателя 5 в позицию, при которой полости А и Б сообщаются с полостью впускного 12 и выпускного 13 патрубков (на рис. 2 эта позиция не показана). Данный режим может сохраняться во всех секциях при нейтральном положении переключателя, когда все входные отверстия полости А и все выходные отверстия полости Б находятся в открытом состоянии. Возможна также ситуация (представленная на рис. 2), когда упомянутые полости перекрыты, и в одной из секций идёт регенерация либо она находится в режиме ожидания.

Как только перепад давления на фильтровальном аппарате достигает значения 0,08–0,1 МПа, запускается процесс регенерации одной либо сразу всех секций. В первом случае вме-

сто восстанавливаемой секции в работу вводится резервная. Однако основной алгоритм работы СРФД-120 предполагает поочерёдное восстановление фильтрующих элементов во всех секциях с последующим возвратом распределительного механизма в нейтральное положение. В таком режиме все секции участвуют в фильтрации. Как только перепад давления достигает предельной величины, автоматика с помощью электропривода 8 переводит переключатель в положение, показанное на рис. 2. При этом секция отключается от процесса фильтрации и подготавливается к регенерации. К этому моменту в продувочной камере 7 под избыточным давлением 0,3–0,5 МПа находится масляно-воздушная (либо топливно-воздушная) эмульсия, которая готовится по специальному циклу: через клапан 11 подаётся сжатый воздух, а через штуцер 10 – нефтепродукт.

Сам процесс регенерации протекает следующим образом: под действием воздушного давления из продувочной камеры 7 нефтепродукт из полости Б начинает двигаться в обратном направлении через фильтроэлементы. Этот этап начинается с открытия клапана 9. Смытые с элементов загрязнения через патрубок 14 и клапан 9 направляются в отстойник-грязевик. После полного вытеснения жидкости из фильтровальной секции через элементы последовательно пропускаются масло (или топливо), а затем – эмульсия. При схлопывании пузырьков эмульсии происходит разрушение и отслоение прочных отложений. Финальная продувка фильтроэлементов сжатым воздухом через клапан с электрическим управлением гарантирует полное удаление остаточных загрязнений.

По завершении цикла клапаны 9 и 11 закрываются. Включается поворотный механизм, который переводит распределительное устройство к следующей секции, после чего цикл регенерации повторяется. Секция, прошедшая восстановление, вновь заполняется очищаемой жидкостью, и в ней возобновляется фильтрация. После того как все секции по очереди пройдут цикл регенерации, переключатель возвращается в нейтральное положение. В таком состоянии он не взаимодействует ни с одной из секций, и все они функционируют в штатном режиме фильтрации.

При адаптивном режиме промывки регенерация продолжается до тех пор, пока перепад давления на фильтре не снизится до заданного нижнего порога. В таком случае процесс идёт вплоть до полного восстановления гидравлических и разделительных характеристик фильтрующего устройства.

Результаты испытаний саморегенерирующегося фильтра

Предварительная подготовка дизеля к испытаниям включала: удаление нагаров с поршневых поверхностей, предварительное взвешивание компрессионных и маслосъёмных колец, шатунных вкладышей, а также нанесение искусственных реперов (лунок) на цилиндровые гильзы.

Интенсивность изнашивания поршневых колец и подшипниковых вкладышей оценивалась по снижению их массы за время испытательного этапа методом взвешивания на аналитических весах типа ВЛА-200. На цилиндровых гильзах с использованием прибора УПОИ-6 создавались лунки в пяти поясах по шести направляющим. Этот же измерительный прибор применялся для контроля изменения длины лунок до начала и после завершения этапа. Пересчёт длины лунок в величину диаметрального износа выполнялся по специализированным таблицам [4]. На каждом этапе замеры проводились дважды — до начала и после окончания испытаний. Для регистрации износа шеек коленчатого вала использовался аналогичный ме-

тод искусственных баз с применением прибора УПОИВ-2. Оценка степени нагарообразования на поршнях после каждого этапа производилась согласно методике 344Т [2, 4, 6] с определением площади, толщины и твёрдостных характеристик отложений.

Отбор проб циркуляционного масла для лабораторных анализов производился каждые 100 часов работы как при штатной, так и при опытной системе очистки. Концентрацию общих и зольных примесей, нерастворимых в бензине, контролировали методом центрифугирования по ГОСТ 20684-75. Щелочное и кислотное числа определяли по ГОСТ 11362-96. Содержание смолистых компонентов идентифицировали методом ИК-спектроскопии [4]. Глубину окислительных процессов в масле находили хроматографическим способом как отношение интегральной интенсивности поглощения карбонильных связей (–C=0) к интегральной интенсивности поглощения связи –C=C– ароматических колец.

Перед вводом в эксплуатацию проведена калибровка контрольно-измерительных приборов системы очистки. Выполнена проверка герметичности всех соединений и работоспособности фильтрующих элементов. Установлены начальные значения кислотного числа и содержания смол в свежем масле для последующего мониторинга. На основе паспортных характеристик фильтра рассчитан прогнозируемый ресурс до первой регенерации. Разработаны инструкции для обслуживающего персонала и утверждён график планового контроля состояния фильтра.

Таблица 1

Характеристики штатного и опытного комбинированного маслоочистительного комплекса

Показатель	Штатный комплект	Опытный комплект
Тип полнопоточного маслоочистителя	СРФ БМЗ	СРФД-120
Пропускная способность полнопоточного фильта, м^3/ч Промывочный индекс фильтра, отн. ед.	120 0,6	120 3
Тонкость отсева, мкм	90	30
Тип байпасно подключаемого центробежного сепаратора	СЦ-1,5	СОСЦ-3
Номинальная пропускная способность тарельчатого сепаратора, м^3/ч	1,5	3
Индекс производительности сепаратора, м^2	3306	5254
Фактор разделения, отн. ед.	3200	4300

Таблица 2

Эффективность очистки комбинированных маслоочистительных комплексов в дизеле 8ДН35/62

Показатель	Штатная очистка	СРФД-120+ СОСЦ-3

Состояние моторного масла:		
Концентрация нерастворимых примесей, %:		
общих	2,5 ± 0,3	1,3 ± 0,1
зольных	0,46 ± 0,07	0,28 ± 0,04
Содержание смолистых веществ, %	6,9 ± 0,8	5,2 ± 1,1
Глубина окисления, %	10,2 ± 1,3	9,7 ± 1,1
Кислотность, мг КОН/г	4,1 ± 0,5	2,7 ± 0,4
Щелочность, мг КОН/г	3,7 ± 0,5	6,2 ± 0,7
Старение и очистка масла, г/ч:		
Интенсивность очистки от нерастворимых продуктов:		
общих	1240 ± 50	5870 ± 250
зольных	248 ± 11	1630 ± 90
Скорость срабатывания присадок	3100 ± 160	1140 ± 50
Периодичность обслуживания СРФ, тыс. ч *Из-*	1,7 ± 0,3	5,3 ± 0,6
нашивание деталей двигателя:		
поршневых колец, г/1000 ч	18,2 ± 2,1	12,6 ± 1,1
цилиндровых втулок, мкм/1000 ч	15,2 ± 1,9	10,2 ± 0,9
вкладышей подшипников (мотылевых), г/1000	9,3 ± 0,7	5,5 ± 0,6
ч шеек (мотылевых) коленчатого вала, мкм/	8,1 ± 0,7	5,2 ± 0,5
1000 ч *Оценка нагаро-лакообразования, балл:*		
канавки компрессионных и маслосъемных ко-	2,2 ± 0,3	1,5 ± 0,2
лец юбка поршня суммарная оценка	20,2 ± 2,3	14,9 ± 1,6

Проведённый анализ результатов моторных испытаний (табл. 2) убедительно демонстрирует превосходство новой автоматизированной системы очистки масла по сравнению со штатным вариантом. Если анализировать влияние на процессы старения масляной среды, то сочетание СРФД-120 и СОСЦ-3 даёт значительно более интенсивное удаление нерастворимых загрязнений. Низкий уровень износа подшипников и шеек коленчатого вала обеспечивается прежде всего эффективностью фильтра СРФД-120, номинальная тонкость очистки которого составляет 30 мкм против 90 мкм у штатного полнопоточного очистителя. В свою очередь, снижение скорости изнашивания поршневых колец и цилиндровых гильз достигнуто за счёт применения сепаратора СОСЦ-3, индекс производительности которого почти в 1,6 раза выше, чем у штатного сепаратора СЦ-1,5.

Обобщая состояние масла на первом этапе (со штатными средствами) и на втором (с автоматизированной системой), можно уверенно констатировать значительно более низкую интенсивность старения масла при использовании агрегатов СРФД-120 и СОСЦ-3. Данный вывод подтверждается меньшей глубиной окисления углеводородов и замедленной выработкой присадок. На втором этапе содержание карбоксильных продуктов и смол в масле оказалось ниже (9,7 против 10,2 % и 5,2 против 6,9 % соответственно). О снижении скорости срабатывания присадок свидетельствует уровень щелочности в итоговых пробах масла: на втором этапе она уменьшилась с 9 до 6,2 мг КОН/г, тогда как на первом этапе падение было более глубоким – до 3,7 мг КОН/г.

Улучшенные показатели качества масла в опытной системе объясняются снижением интенсивности срабатывания присадок в 2,7 раза (см. табл. 2). Положительные изменения состояния масла при использовании новых средств очистки вызваны более активным удалени-

ем зольных продуктов деструкции присадок, которые выступают как ингибиторы окисления углеводородов.

Положительные изменения в состоянии масла существенно повлияли на процессы нагаро- и лакообразования на поршнях. Менее интенсивное старение масла на втором этапе привело к уменьшению количества и твёрдости отложений на деталях цилиндро-поршневой группы. При балльной оценке уровень нагаро- и лакообразования показал снижение интенсивности отложений на всех поршневых поверхностях в среднем на одну треть (см. табл. 2). Кроме того, загрязнение поддона картера шламовыми отложениями на втором этапе оказалось в 1,8 раза ниже.

По результатам измерения остаточного перепада давлений на фильтрующих элементах после завершения каждого этапа с помощью расчётной методики [9] был определён прогнозируемый ресурс необслуживаемой работы СРФ. Автономность маслоочистителя СРФД-120 по данному показателю оказалась в 3,2 раза выше, чем у фильтра СРФ БМЗ. Последующая длительная эксплуатация дизеля 8ДН32/62 с опытной комбинированной системой тонкой очистки масла подтвердила высокую надёжность и продолжительный ресурс автономной работы нового фильтра, в том числе в более жёстких условиях — при использовании масел с пониженными моюще-диспергирующими свойствами по сравнению с маслом М-10$Г_2$(цс). Особенно ярко преимущества СРФД-120 проявляются в судовых тронковых дизелях, работающих на низкосортных высоковязких топливах типа топочный мазут [2, 5].

По итогам моторных испытаний комбинированной полностью автоматизированной системы тонкой очистки масла на базе фильтра СРФД-120 и сепаратора СОСЦ-3 можно сделать однозначный вывод: данная система способна обеспечить надёжную защиту судового тронкового дизеля от абразивного износа при сжигании высоковязких топлив по ГОСТ 32510-2013, получаемых в результате глубокой переработки нефти. Интенсивное удаление посредством сепарирования нерастворимых, и особенно зольных, мелкодисперсных примесей из унифицированных рабочих масел типов М-10(14,16)$Г_2$(цс), М-14(16)$Д_2$(цл20) и М-14(16)$Д_2$(цл30) (ГОСТ 12337-2020) замедляет процессы их старения. Это создаёт предпосылки для длительного использования масел без полной замены, компенсируя лишь естественный угар. Предлагаемый на базе фильтра СРФД-120 и сепаратора СОСЦ-3 комбинированный комплекс тонкой очистки обеспечивает высокий уровень автоматизации смазочных систем современных судовых дизелей.

Заключение

1. Создан и прошёл натурные испытания опытный образец саморегенерирующегося фильтра СРФД–120, способный непрерывно работать без технического обслуживания не менее 3000 часов. При номинальной тонкости задержания механических примесей элементов 30–50 мкм и пропускной способности 120 м³/ч устройство надёжно защищает подшипники и шейки коленчатого вала судовых дизелей от абразивного изнашивания. На основе данной конструкции возможно создание типоразмерного ряда полнопоточных маслоочистителей производительностью до 360 м³/ч. При замене в СРФД–120 фильтрующей сетки на тканый материал полотняного переплетения с номинальной

тонкостью отсева 10–20 мкм устройство может быть преобразовано в топливный фильтр с пропускной способностью 30 м³/ч.

2. Повышенная эффективность разработанного очистителя СРФД–120 как в режиме фильтрования, так и при регенерации достигается за счёт следующих конструктивно-технологических факторов:

– применением тканых сеток с перекрестным полотняным переплетением оптимизированной геометрии, обеспечивающим сбалансированные показатели очистки и лёгкость восстановления;

– жёсткой конструкцией фильтрующего узла свечного типа, отличающегося высоким коэффициентом живого сечения опорного каркаса и полноценным использованием всей фильтрующей поверхности в обоих режимах;

– повышением промывочного индекса фильтра, достигаемого интенсивной обратной продувкой фильтрующих элементов многофазным потоком (очищаемой жидкости вместе с воздушно–капельной эмульсией), а также использованием адаптивного алгоритма регенерации, автоматически учитывающего адгезионные свойства накапливающихся загрязнений.

3. Моторные испытания комбинированной полностью автоматизированной системы глубокой очистки масла, построенной на принципах полнопоточного фильтрования и байпасного центробежного сепарирования, подтвердили практическую возможность ресурсосберегающего использования моторного масла в судовых тронковых дизелях высокой фарсировки. Даже при работе на высоковязком низкокачественном топливе обеспечивается надёжная защита деталей двигателя от абразивного износа, а моторное масло с высокими термоокислительными и моюще-диспергирующими свойствами переводится в режим длительной эксплуатации без замены. Предложенная система очистки значительно превосходит большинство серийных аналогов: интенсивность старения моторного масла снижается в 1,4–1,7 раза, а скорость изнашивания основных деталей двигателя уменьшается на 30–60 %.

Список литературы

1. Микутенок Ю.А., Шкаренко В.А., Резников В.Д. Смазочные системы дизелей. Л.: Машиностроение, 1986. 125 с.
2. Кича Г.П. Эксплуатационная эффективность новых маслоочистительных комплексов в форсированных дизелях // Двигателестроение. 1987. № 6. С. 25–29.
3. Кича Г.П., Надежкин А.В., Бойко С.П. Результаты эксплуатационных испытаний саморегенерирующегося фильтра в судовых дизелях в составе комбинированного маслоочистительного комплекса // Вестн. Гос. ун-та морского и речного флота имени адмирала С.О. Макарова. 2019. № 4(56). С. 718–726.
4. Кича Г.П., Надежкин А.В., Перминов Б. Н. Ресурсосберегающее маслоиспользование в судовых дизелях. Владивосток: Мор. гос. ун-т, 2011. 372 с.
5. Кича Г.П., Надежкин А.В., Глушков С.В. Комплексное системное решение проблемы ресурсосберегающего маслоиспользования в судовых дизелях // Морские интеллектуальные технологии. 2016. Т. 1, № 3(33). С. 118–126.

6. Кича Г.П., Пак Н.К. Новые инженерные решения в конструкциях саморегенерирующихся фильтров для очистки топлив и смазочных материалов на судах // Морские интеллектуальные технологии. 2013. № 1. С. 203–207.

9. Бойко С.П., Кича, Г.П. Экспериментальное моделирование эффективности процесса регенерации самоочищающихся фильтров, функционирующих в системах смазки судовых дизелей // Морские интеллектуальные технологии. 2015. № 3(29). Т. 1. С. 95–101.

10. Кича Г.П., Надежкин А.В., Пак Н.К. Саморегенерирующийся фильтр новой конструкции для очистки топлив и смазочных масел на судах // Научные проблемы транспорта Сибири и Дальнего Востока. 2013. № 1. С. 203–207.

11. Бойко С.П., Кича, Г.П., Надежкин А.В. Расчет параметров регенерации самоочищающихся фильтров смазочных систем судовых дизелей // Морские интеллектуальные технологии. 2020. Т. 2, № 1(47). С. 123–130.

12. Кича Г.П., Надежкин А.В., Перминов Б.Н. Имитационное моделирование смазки трибосопряжений и изнашивания основных деталей ДВС // Транспортное дело России. 2004. № 2. С. 51–53.

13. Кича Г. П., Семенюк Л.А., Тарасов М.И. [и др.] Эксплуатационная эффективность полнопоточной тонкой очистки моторного масла в судовых вспомогательных дизелях // Научно-технический сборник Российского морского регистра судоходства. 2020. № 58/59. – С. 71–80.

14. Кича Г. П., Надежкин А. В., Семенюк Л. А. Новые стахостические модели очистки топлив и масел судовыми центробежными аппаратами со сложной гидродинамической обстановкой // Морские интеллектуальные технологии. 2018. № 4(42). Т. 5. С. 77–89.

Поступила в редакцию 22 июля 2026 г.

УДК 656.073+656.6

Выбор технологий для автоматизированного морского терминала на Дальнем Востоке России: анализ опыта Китая

Баранникова Анастасия Олеговна, к.и.н., e-mail: aobarannikova@gmail.com

Морской государственный университет имени адмирала Г.И. Невельского, г. Владивосток

Аннотация: Поддержание конкурентоспособности морского порта в новых реалиях немыслимо без внедрения современных технологий. Китай является мировым лидером в сфере автоматизации контейнерных перевозок и портово-логистических процессов, и его опыт представляется полезным для других стран, в том числе и для России в целом и ее дальневосточного региона в частности. Тем более, что для дальневосточных портов актуален вопрос повышения производительности контейнерных терминалов в условиях нехватки трудовых ресурсов, сложных климатических и экономических условий. При этом при заимствовании любого опыта технологического развития, необходимо учитывать ряд факторов: от местной специфики и ограничений до конечной цели данного развития. В данной статье рассматриваются отдельные технологии, применяющиеся в морских портах Китая, с точки зрения применимости и целесообразности их внедрения в отдельном дальневосточном контейнерном терминале.

Ключевые слова: умный порт, цифровизация, автоматизация, автоматизированный контейнерный терминал, Китай.

Selecting Technologies for an Automated Marine Terminal in the Russian Far East: An Analysis of China's Experience

Barannikova Anastasia O., e-mail: aobarannikova@gmail.com

Maritime State University named after Admiral G.I. Nevelskoy, Vladivostok

Maintaining the competitiveness of a seaport in the new reality is unthinkable without the implementation of modern technologies. China is a global leader in the automation of container shipping and port logistics processes. Its experience is useful for other countries, including Russia in general and its Far East region in particular. This is especially true given the pressing need for Far Eastern ports to improve the productivity of container terminals amid labor shortages and challenging climatic and economic conditions. When adopting any technological development experience, it is necessary to consider a number of factors: from local specifics and constraints to the ultimate goal of the development. This article examines specific technologies used in Chinese seaports, examining their applicability and feasibility for implementation at a specific Far Eastern container terminal..

Keywords: smart port, digitalization, automation, automated container terminal, China.

Развитие контейнерных перевозок в Азиатско-Тихоокеанском регионе приводит к необходимости модернизации портовой инфраструктуры. Одним из важных направлений повышения эффективности морских терминалов является автоматизация портово-логистических процессов.

Признанным мировым лидером в данной области является Китай, который на конец прошлого года построил уже 60 автоматизированных контейнерных терминалов, в том числе и в таких крупных портах, как Шанхай, Тяньцзинь, Циндао и Нинбо. В китайских автоматизированных терминалах представлены такие технологии, как автоматизированные причальные и козловые краны (STS и RTG/ARMG), беспилотные транспортные средства AGV (Automated Guided Vehicle), системы OCR-распознавания контейнеров, внедрены терминальные операционные системы (TOS) и цифровые системы мониторинга и диспетчеризации и т д.

Для России, особенно для портов Дальнего Востока, вопрос автоматизации портовых процессов и мощностей также актуален. Перед регионом стоит задача повышения производительности контейнерных терминалов в условиях нехватки трудовых ресурсов, и сложного климата, не говоря уже о том, что поддержание конкурентоспособности порта в новых реалиях немыслимо без внедрения современных технологий. Однако прямое копирование китайской модели автоматизации представляется нецелесообразным - слишком разные масштабы грузооборота, структура судозаходов и климатические условия. Например, в отличие от крупнейших китайских портов, ориентированных на обработку сверхкрупных контейнеровозов свыше 20 000 TEU, российские дальневосточные порты работают преимущественно с судами вместимостью до 10 000 TEU и имеют кратно меньший грузооборот и площадь (см. Таблица 1).

В связи с этим имеет смысл проанализировать опыт автоматизизации контейнерных терминалов Китая на предмет того, какие технологии наиболее применимы и приемлемы для небольшого морского терминала на Дальнем Востоке России с учетом таких местной специфики и таких проблем, как кадровый дефицит, хрупкость энергосистем и экологии, ограниченный грузооборот и т д.

Таблица 1. Сравнение средних показателей портов ДВ РФ и КНР (составлено по данным [1, 7, 10])

Характеристики	**Дальневосточный порт**	**Нинбо-Чжоушань**
Грузооборот	880 000 TEU в год	40 000 000 TEU в год
Количество судозаходов	2000 судов в год	300 судов ежедневно
Площадь	4 кв км	9 кв км
Класс судов	Panamax, Post-Panamax (max 10 000 TEU)	Super-Post-Panamax, Triple E-class (20 000 TEU)

Роботизированные системы

Автоматизированные краны

В китайских портах применяются два вида кранов - полностью автоматизированные и управляемые дистанционно. Для дальневосточного порта перспективными представляются полуавтоматические краны, с дистанционным управлением, автоматическим позиционированием спредера и оснащенные стабилизирующими системами. Такие решения дешевле полной автоматизации, проще в эксплуатации, устойчивее к погодным условиям.

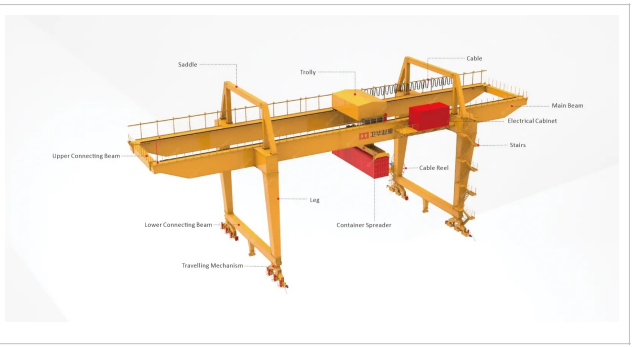
При этом для условий дальневосточного порта можно ограничиться Post-Panamax Class — (7000 −13000 TEU). Super Post-Panamax[1] используется в крупных портах Китая и Европы, но для ДВ избыточен, к тому же слишком высоки затраты, нагрузка на причал и сложность обслуживания. Например, стоимость кранов класса Post-Panamax может составлять 8-12 миллионов долларов США, тогда как краны класса Super Post-Panamax стоят уже 12-15 миллионов, а стоимость сверхкрупных судо-береговых кранов может достигать 20 млн долларов США и выше [4].

В климатических условиях Дальнего востока краны на рельсах представляются более надежными, чем краны на на резиновых колесах. У них выше выше устойчивость (в условиях ветров, обледенения и т д), меньше энергопотребление, а также ниже затраты на обслуживание и первоначальная стоимость.

Таблица 2. Сравнение примерной стоимости кранов на резиновых колесах и рельсах (по данным [5, 9])

RTG	RMG
Средняя стоимость — около 2 млн. долларов США за единицу.	Полуавтоматический RMG — 300–600 тыс. долларов США Полностью автоматизированный — 0.8 - 1.2 млн. долларов США.
Техобслуживание - 50 тыс. долларов США в год	Техническое обслуживание - 10-50 тыс. долларов США в год
Срок службы и долговечность: 15–25 лет	Срок службы и долговечность: 30 лет и более.

[1] 1.Handysize Class — 260—1000 TEU 2. Handymax Class — 1000—1700 TEU 3. Feeder Class — 1700—2500 TEU 4. Sub-Panamax Class — 2500—4000 TEU 5. Panamax Class — (4000—7000 TEU) 6. Post-Panamax Class — (7000 −13000 TEU) Компания APL предложившая новые морские пути без прохождения Панамского канала, положила начало развития новых контейнеровозов типа Post-Panamax.В настоящее время 30 % мирового контейнерного флота составляют суда типа post-panamax. 7. Super-Post-Panamax Class/E-class(свыше 14000 TEU). 8. Triple E-class — 18000TEU



Автоматизированный транспорт

Автоматизированный транспорт (AGV) может значительно повысить эффективность транспортировки, но при этом имеет и ряд недостатков - ограниченный радиус действия, длительное время зарядки, и высокая стоимость, которая складывается из потребности в создании сопутствующей инфраструктуры, обеспечении определенного качества дорожного покрытия и обучения персонала. Переход на полностью беспилотный транспорт требует магнитной / GNSS RTK-навигации, лидаров, V2X, зарядной инфраструктуры, отдельной системы управления. Все это влечет за собой значительные капиталовложения для портов, поэтому до сих пор ведутся дебаты о применении AGV в портах [3]. Полностью автоматизированные AGV-системы окупаются только при огромном грузообороте, плотном потоке судов и круглосуточной загрузке техники. Для небольшого порта более рациональным представляется применение технологии platooning (один ведущий тягач, несколько ведомых, синхронное движение колонной). Это позволит сократить число операторов/водителей, но при этом избежать трат на дорогостоящее оборудование. Отдельные китайские порты переходят от схемы «чистых AGV» к более гибридным схемам на терминалах среднего размера, так как AGV оказались очень дорогими в эксплуатации. Другие внедряют более совершенные технологии. Например, порт Тяньцзинь вместо AGV развернул роботизированные транспортные средства с искусственным интеллектом (ART) и интеллектуальную систему вождения, разработанную совместно с компанией Huawei. Система использует камеры и радары для определения окружающей среды, а затем применяет BeiDou — спутниковую навигационную систему, аналогичную GPS, для точного позиционирования. После этого ARTs загружает данные о местоположении и состоянии дорог в облако через сеть 5G. Однако при этом сеть должна быть спроектирована таким образом, чтобы преодолевать помехи, которые создаются портовыми кранами, контейнерами и зданиями [8].

Помимо автоматизированных кранов и роботизированного транспорта, в китайских портах активно используется робототехника для инспекций контейнеров, экологического мониторинга, охраны периметра и т д. Например, в порту Циндао оснащенные регулируемыми камерами и алгоритмами машинного зрения, роботы распознают маркировку, номера контейнеров и возможные повреждения даже в условиях недостаточного освещения [2].

Для дальневосточного порта также были бы полезны роботы для инспекции и мониторинга, в том числе экологического, которые осуществляют обход/облет причалов,

кранов, подстанций, акватории, складов, топливных объектов, а также контроль температуры, вибраций, утечек, обледенения.

Также роботы могут быть задействованы для видеонаблюдения и охраны (автоматическое патрулирование периметра, тепловизионный контроль, выявление возгораний и т д). В целом, имеет смысл внедрять робототехнические средства, которые могут выполнять опасные, рутинные операции и работать в ночное время и в труднодоступных местах.

Цифровые технологии

Терминальные операционные системы (TOS)

Терминальные операционные системы по праву считаются «мозгом» умного порта. Они осуществляют планирование, отслеживание и управление операциями и ресурсами порта в режиме реального времени, управляют погрузкой, разгрузкой и распределением контейнеров, назначают задания для техники и персонала, а также осуществляют обмен данными с судоходными линиями, таможней, клиентами. Китайские порты активно внедряют отечественные разработки, например, порт Шанхая - интеллектуальную систему управления и контроля ITOS и NEO-TOS, порт Тяньцзинь - систему управления контейнерным терминалом JTOS.

Преимущества внедрения современных TOS-систем - относительно низкие капитальные затраты, повышение прозрачности операций, значительное сокращение времени на операции. Без данной технологии практически немыслим современный терминал.

Концепция умного порта строится вокруг интеграции порта, таможни, судоходных линий, железной дороги, экспедиторов, санитарного и экологического контроля. Подобная система подошла бы и для небольшого российского терминала. Цифровое оформление судозаходов, таможенного оформления, ветеринарного/фитосанитарного контроля, железнодорожной отправки значительно сокращает время простоя и позволяет обходиться меньшим штатом сотрудников. Также к TOS могут быть подключены отдельные специализированные системы, например, система предиктивной диагностики оборудования, которая позволяет прогнозировать поломки, сокращать простои и снижать расходы на ремонт. Также полезна система экологического мониторинга, вроде той, что применяется в китайских портах и осуществляет мониторинг воздуха и воды на предмет вредных выбросов. Для дальневосточных портов такие системы особенно актуальны из-за близости природоохранных территорий и рыбохозяйственной зон.

OCR (системы автоматического распознавания контейнеров)

Если TOS можно считать «мозгом» умного порта, то системы автоматического распознавания контейнеров - его «глазами». OCR обеспечивает эффективный, бесконтактный способ идентификации, отслеживания и контроля контейнеров. При использовании решений OCR на периметре терминала оборудование быстро идентифицируется автоматически со значительно меньшим количеством ошибок по сравнению с ручной регистрацией. Это приводит к повышению производительности за счет снижения количества неправильно идентифицированных контейнеров, попадающих на контейнерную площадку. При этом в

условиях холодных зим Дальнего Востока необходимо использование морозостойких камер, систем обогрева и защищённые корпуса для оборудования, входящего в систему OCR.

Прочая инфраструктура

Энергосеть

По мере того, как на Дальнем Востоке России имеются проблемы с энергоинфраструктурой (некоторые энергосети изношены, зимой отмечаются высокие пики нагрузки и возможны перебои), даже частично автоматизированный терминал должен иметь собственную энергосеть.

Здесь также полезен китайский опыт. Так, например, в порту Циндао активно используют накопители энергии, интеллектуальное управление нагрузкой, водородную и электрическую технику и береговое электроснабжение судами во время стоянки. При чем для преодоления ограничений (длина кабелей, ограниченная мобильность оборудования и сложность операций) был разработан робот для подключения высоковольтного берегового электроснабжения, способный свободно маневрировать в узком пространстве между портальными кранами и судами, быстро и точно выполняя подключение даже при отклонениях в швартовке.

Для небольшого порта достаточно будет создания отдельной микросети (microgrid) с резервными источниками и системы берегового питания судов (shore power).

Серверный центр / микроЦОД

Наконец, для работы TOS, OCR и прочих цифровых компонентов необходим центр обработки данных. Необходимо не только обрабатывать данные в реальном времени и надежно их хранить, но и обеспечить бесперебойную связь и высокую скорость передачи сигнала. С такой функцией справляются централизованные дата-центры. В то же время «классический» ЦОД целесообразен для крупного порта, который генерирует огромные массивы видео, управляет сотнями AGV, обрабатывает миллионы IoT-событий. Например, в порту Шэньчжэнь используется ЦОД общей площадью около 700 м2 на 90 стоек [6]. Помимо строительства собственного дата-центра можно арендовать стойки в удаленном коммерческом ЦОДе, но это может привести к снижению скорости передачи данных и подвергнуть риску безопасность этих данных.

Для небольшого порта имеет смысл ограничиться Edge Data Center или МикроЦОД, который будет обеспечивать работу TOS, OCR, IoT и видеоаналитики. МикроЦОДы автономны, легко доставляются, разворачиваются и масштабируются, оснащены системами охлаждения и более целесообразны с точки зрения затрат и энергосбережения.

Заключение

Несмотря на быстрое и активное внедрение новых портовых технологий рядом стран, в том числе и Китаем, число автоматизированных контейнерных терминалов в мире пока незначительно, по ряду причин. В то время, как автоматизация может повысить эффективность работы порта и, в конечном счете, его прибыльность, внедрение необходимых технологий на начальном этапе требует значительных капитальных затрат и окупается только при условии высокого грузооборота и доходности порта. Например, общий объем инвестиций в строительство четвертой фазы шанхайского терминала Яншань составил почти 2 миллиарда долларов, при этом грузооборот порта Яншань стабильно рос от 10,1 млн TEU в 2010 году до 50 млн TEU к 2025 году. При этом Китай руководствуется правилом, что гораздо легче технически и экономически целесообразней создавать автоматизированный терминал с нуля, чем переоснащать уже функционирующий обычный терминал - в таких терминалах можно ограничиться выборочной автоматизацией процессов.

Если Китай, осуществляя автоматизацию своих портов, руководствуется, главным образом, стремлением сохранять лидирующие позиции в сфере контейнерных перевозок, оптимизировать обработку огромного грузопотока и решить экологические проблемы, вызванные бурным экономическим ростом, то для портов Дальнего Востока России ключевой задачей становится поддержание конкурентоспособности, интеграция в транспортно-логистические цепочки СВА в сложных экономических, климатических и демографических условиях.

Таким образом, с точки зрения исходных условий и экономической целесообразности, для дальневосточных терминалов наиболее приемлемой видится гибридная автоматизация, поэтапное внедрение технологий, приоритет цифровизации над роботизацией и адаптация оборудования к холодному климату. Основная задача заключается не в том, чтобы построить «полностью безлюдный мегапорт» по типу Яншаня, а создать устойчивый, энергонезависимый и цифровой терминал средней мощности с минимальными эксплуатационными затратами. С этой точки зрения китайский опыт интересен в части не тотальной роботизации, а в части отдельных цифровых решений и энергетической автономности.

Список литературы

1. Владивостокский морской торговый порт. URL: https://vmtp.ru/
2. Умные помощники: как роботы преобразили столетний порт Циндао. Жэньминь жибао. 12/01/2026. URL: https://russian.people.com.cn/n3/2026/0112/c31518-20412962.html
3. Chen, Q. (2023). The impact of AGV application on port operating efficiency. Theoretical and Natural Science,18,19-29.
4. Coherent Market Insights. Ship-to-Shore Cranes Market Analysis and Forecast: 2026-2033. URL: https://www.coherentmarketinsights.com/market-insight/ship-to-shore-cranes-market-4369
5. DONGQI GROUP website. URL: https://id.craneyt.com/knowledge/100-ton-gantry-crane
6. Huawei Smart Modular Data Center Solution Helps Shenzhen Port Group Go Digital. Huawei Technologies Co., Ltd. website. URL: https://digitalpower.huawei.com/en/cases/data-center-facility/shenzhen-port-huawei-smart-modular-data-center
7. Xinhua. URL: https://english.news.cn/home.htm
8. Yang Jiejin, The future of ports is in Tianjin, China. Huawei Technologies Co., Ltd. website. URL: https://www.huawei.com/en/media-center/transform/21/16-tianjin-port
9. Yuantai Crane Machinery website. URL: https://www.ythoist.com/gantry-crane/rubber-tired-gantry-crane.html
10. Zhejiang seaport. URL: https://www.zjseaport.com/jtwwen/

Поступила в редакцию 22 июля 2026 г.

ВЕСТНИК
МОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Выпуск 103/ 2026

Дата выхода в свет – 27 июля 2026 г.
Выходит четыре раза в год.

Зарегистрировано Федеральной службой по надзору
в сфере связи и массовых коммуникаций.
Свидетельство о регистрации Эл № ФС77-82589 от 30.12.2021.

Учредитель и издатель – Федеральное государственное бюджетное образовательное учреждение высшего образования «Морской государственный университет имени адмирала Г.И. Невельского».

Адрес учредителя, издателя и редакции: 690003, Россия, г. Владивосток, ул. Верхнепортовая, 50а.
Электронная почта редакции: vestnik@msun.ru; телефон редакции: +7 (423) 251-76-36.