ПЕДАГОГИКА
(шифр научной специальности: 5.8.7)

Научная статья
УДК 37
doi: 10.18522/2070-1403-2025-114-1-188-195

СОВЕРШЕНСТВОВАНИЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА СФЕРЫ ВОДНОГО ТРАНСПОРТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АКТУАЛЬНОСТЬ, ТРЕБОВАНИЯ, ПОДХОДЫ

© Семён Михайлович Кузьменко[1], Мария Максимовна Садайло[2]
[1]Научно-исследовательский институт «Специализированные вычислительные устройства защиты и автоматика», г. Ростов-на-Дону; Донской государственный технический университет, г. Ростов-на-Дону, Россия; [2]Институт водного транспорта имени Г.Я. Седова – филиал Государственного морского университета имени адмирала Ф.Ф. Ушакова, г. Ростов-на-Дону; Южный федеральный университет, г. Ростов-на-Дону, Россия
[1]simon_kuzmen@rambler.ru [2]sadailo@iwtsedov.ru

Аннотация. Рассматривается актуальная проблема недостаточности объема и глубины преподавания дисциплин по информационной безопасности (ИБ) в образовательных программах подготовки специалистов среднего звена (судоводителей, судомехаников, электромехаников, логистов) для водного транспорта. Проведен анализ современных киберугроз в морской отрасли, исследованы ФГОС СПО по соответствующим специальностям, требования ключевых российских и международных нормативных документов (Резолюции ИМО MSC.428(98), MSC-FAL.1/Circ.3, руководства ISO/IEC 27001, требования классификационных обществ). На основе выявленного диссонанса между требованиями реальной эксплуатации и содержанием образовательных программ предложены рекомендации по интеграции модулей ИБ в учебные планы.

Ключевые слова: информационная безопасность на водном транспорте, кибербезопасность судов, подготовка кадров среднего звена, среднее профессиональное образование (СПО), ФГОС СПО, Международная морская организация (ИМО), киберустойчивость.

Для цитирования: Кузьменко С.М., Садайло М.М. Совершенствование подготовки специалистов среднего звена сферы водного транспорта в области информационной безопасности: актуальность, требования, подходы // Гуманитарные и социальные науки. 2026. Т. 114. № 1. С. 188-195. doi: 10.18522/2070-1403-2025-114-1-188-195

PEDAGOGY
(specialty: 5.8.7)

Original article

Improving the training of mid-level specialists in the field of water transport in the field of information security: relevance, requirements, approaches

© Semyon M. Kuzmenko[1], Maria M. Sadailo[2]
[1]Research Institute "Specialized Computing Devices for Protection and Automation", Rostov-on-Don; Don State Technical University, Rostov-on-Don, Russian Federation; [2]Sedov Water Transport Institute – a branch Admiral F.F. Ushakov State Maritime University, Rostov-on-Don; Southern Federal University, Rostov-on-Don, Russian Federation
[1]simon_kuzmen@rambler.ru [2]sadailo@iwtsedov.ru

Abstract. This article examines the current problem of the insufficient volume and depth of information security (IS) teaching in educational programs for the training of mid-level specialists (navigators, ship mechanics, electrical engineers, logisticians) for water transport. Against the backdrop of the rapid digitalization of shipping and the introduction of integrated automated control and navigation systems, the risks of cyberattacks on critical maritime infrastructure have increased significantly. The authors analyzed modern cyber threats in the maritime industry, examined the Federal State Educational Standards of Secondary Vocational Education for relevant specialties, and the requirements of key Russian and international regulatory documents (IMO Resolutions MSC.428(98), MSC-

FAL.1/Circ.3, ISO/IEC 27001 guidelines, and classification society requirements). Based on the identified dissonance between the requirements of real-world operations and the content of educational programs, recommendations are proposed for integrating IS modules into curricula.

Key words: information security in water transport, cybersecurity of ships, training of mid-level personnel, secondary vocational education (SVE), Federal State Educational Standard of SVE, International Maritime Organization (IMO), cyber resilience.

For citation: Kuzmenko S.M., Sadailo M.M. Improving the training of mid-level specialists in the field of water transport in the field of information security: relevance, requirements, approaches. *The Humanities and Social Sciences.* 2026. Vol. 114. No 1. P.188-195. doi: 10.18522/2070-1403-2025-114-1-188-195

Введение

Водный транспорт, являясь критически важной артерией мировой экономики, переживает период глубокой цифровой трансформации. Внедрение интегрированных мостиковых систем (IBS), электронных картографических навигационно-информационных систем (ЭКНИС), систем автоматической идентификации (АИС), комплексной автоматизации машинных отделений и развитие «умных» портов кардинально повысили эффективность судоходства. Однако параллельно с этим создалась обширная поверхность для кибератак [13]. Инциденты с такими гигантами, как Maersk и CMA CGM, а также растущее число атак на навигационные и коммерческие системы судов демонстрируют, что киберугрозы перешли из теоретической плоскости в оперативную реальность, несущую прямые риски безопасности мореплавания, охране окружающей среды и экономической стабильности [16].

При этом основным слабым звеном в цепочке киберзащиты зачастую становится человеческий фактор, а именно недостаточная подготовленность экипажей и технического персонала. Проблема заключается в системном отставании образовательных программ среднего профессионального образования (СПО) для водного транспорта от технологических вызовов и нормативных требований в области информационной безопасности (ИБ). Подготовка специалистов среднего звена – будущих судоводителей, механиков, электромехаников – фокусируется на традиционных компетенциях, оставляя вопросы кибергигиены и осознанного взаимодействия с цифровыми системами на периферии учебного процесса.

Целью статьи является разработка научно-обоснованных и практико-ориентированных предложений по интеграции содержательных модулей по ИБ в учебные планы подготовки специалистов среднего звена для водного транспорта. Для достижения цели поставлены следующие задачи:

1. Проанализировать современный ландшафт киберугроз в морской отрасли.
2. Изучить и сопоставить требования международных нормативных документов (ИМО, ISO) и российских ФГОС СПО соответствующих специальностей.
3. Оценить текущее состояние преподавания основ ИБ в учреждениях СПО морского и речного профиля.
4. Предложить структурную и содержательную модель интеграции ИБ-компонентов с учетом специфики СПО.
5. Обосновать практические механизмы внедрения и развития данной модели.

Обсуждение

Современные вызовы и риски информационной безопасности на водном транспорте

Эволюция киберугроз в морской отрасли демонстрирует тревожную динамику: от целевых атак на IT-инфраструктуру береговых офисов (как в случае с вирусом-шифровальщиком NotPetya) до прямого воздействия на системы, отвечающие за безопасность судна [15]. Сегодня можно выделить несколько ключевых векторов атак:

Навигационные системы: GPS-спуфинг, вмешательство в работу ЭКНИС (ECDIS), искажение или компрометация данных АИС, что может привести к навигационным ошибкам, посадке на мель или столкновению.

Судовые автоматизированные системы: Внедрение вредоносного ПО в системы управления главным двигателем (PMS), интегрированные мостиковые системы (IBS) или

грузовые системы, что чревато потерей управляемости, повреждением оборудования или экологической катастрофой.

Коммерческие и портовые системы: Атаки на Port Community Systems (PCS), системы оформления судовых документов, что приводит к блокировке грузовых операций, финансовым потерям и логистическому коллапсу.

Судовые сети: Проникновение в локальную сеть судна через незащищенные точки доступа (спутниковые терминалы, Wi-Fi экипажа), с последующим перемещением по сегментам сети и атакой на критическое оборудование.

Последствия успешных кибератак носят комплексный характер: от прямых финансовых потерь и хищения конфиденциальных данных до экологического ущерба, угрозы жизни экипажа и потери репутации компании. Мы видим, что цифровые и операционные технологии на современном судне неразделимы. Следовательно, у всех специалистов, взаимодействующих с этими системами, должна быть сформирована базовая кибергигиена и четкое понимание принципов минимизации киберрисков. Это требование является основополагающим для обновления образовательных программ.

Нормативно-правовая база как основа для обновления образовательных программ

Международные требования за последние годы стали строгими и конкретными. Резолюция ИМО MSC.428(98) обязывает включить управление киберрисками в Системы управления безопасностью (СУБ) судовых компаний не позднее первого ежегодного проверочного аудита после 1 января 2021 г. [12]. Руководящий документ MSC-FAL.1/Circ.3 [14] детализирует рекомендации по оценке уязвимостей и защите судовых систем. Эти документы прямо указывают на необходимость обучения и повышения осведомленности персонала. Стандарты ISO/IEC 27001 и требования классификационных обществ (PMPC, DNV и др.) также акцентируют внимание на человеческом факторе.

Анализ динамики изменений за последние годы ФГОС СПО по специальностям 26.02.03 «Судовождение» [1; 2; 3], 26.02.05 «Эксплуатация судовых энергетических установок» [4; 5; 6], 26.02.06 «Эксплуатация электрооборудования и средств автоматики» [7; 8; 9], 38.02.03 «Операционная деятельность в логистике» [10; 11] показывает, что формулировки, касающиеся безопасности, всё ещё носят общий характер (например, «обеспечивать безопасность…», «соблюдать требования охраны труда»). Прямых упоминаний кибербезопасности, управления цифровыми рисками или защиты судовых информационных систем в перечне профессиональных компетенций и содержании учебных дисциплин не обнаруживается. Существует явный пробел между императивами ИМО и содержанием российских образовательных стандартов для уровня СПО. Тем не менее, ФГОС 2024 впервые явным образом вводит понятие «компетенции цифровой экономики» и разрешает создавать под них отдельные учебные модули.

Таблица 1

Сравнительный анализ требований к IT-компетенциям в ФГОС СПО по специальности 26.02.05 «Эксплуатация судовых энергетических установок»

Вид компетенции / аспект	ФГОС 2014 г. (Приказ Минобрнауки № 443) [4]	ФГОС 2020 г. (в ред. 2022 г.) (Приказ Минпросвещения № 674) [5]	ФГОС 2024 г. (Приказ Минпросвещения № 873) [6]
Общие компетенции (ОК), связанные с IT	ОК 4: Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач. ОК 5: Использовать информационно-коммуникационные технологии	ОК 02: Использовать современные средства поиска, анализа и интерпретацииинформации и информационные технологии для выполнения задач профессиональной деятельности (Раздел III, п. 3.2).	ОК 02: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности (Раздел III, п. 3.2).

Вид компетенции / аспект	ФГОС 2014 г. (Приказ Минобрнауки № 443) [4]	ФГОС 2020 г. (в ред. 2022 г.) (Приказ Минпросвещения № 674) [5]	ФГОС 2024 г. (Приказ Минпросвещения № 873) [6]
	в профессиональной деятельности. ОК 9: Ориентироваться в условиях частой смены технологий в профессиональной деятельности (Раздел V).		
IT-навыки в рамках профессиональных компетенций (ПК)	Прямых упоминаний IT в формулировках ПК нет. Требования к работе с информацией и техникой включены в контекст эксплуатации оборудования.	Прямых упоминаний IT в формулировках ПК нет. Подразумеваются в рамках эксплуатации автоматизированных систем и средств управления.	Прямых упоминаний IT в формулировках ПК нет. Подразумеваются в рамках эксплуатации электрооборудования, средств автоматики и цифровых систем управления.
Цифровые технологии и экономика	Специальных требований или модулей по цифровой экономике нет.	Специальных требований или модулей по цифровой экономике нет.	Образовательной организации предоставлено право вводить в вариативную часть модуль по освоению компетенций цифровой экономики, соответствующих видам деятельности программы (Раздел III, п. 3.4). Вариативная часть направлена, в том числе, на учет требований цифровой экономики (Раздел II, п. 2.3).
Виртуальные технологии и симуляторы	Прямых упоминаний нет.	Допускается применение виртуальных аналогов помещений и оборудования при использовании дистанционных технологий (п. 4.3.2).	Допускается замена оборудования его виртуальными аналогами (Раздел IV, п. 4.4, подп. "г").
Информационная безопасность и кибергигиена	Прямых упоминаний нет.	В рамках дисциплины «Информатика» упоминается использование приемов антивирусной защиты и технических средств защиты информации (Таблица 5, ЕН.02).	В рамках общесистемных требований и компетенций прямо не выделена. Может подразумеваться в контексте использования современных IT (ОК 02) и защиты информации на судне.
Работа с профессиональной IT-документацией и данными	ОК 10: Владеть письменной и устной коммуникацией на государственном и иностранном языке (косвенно).	ОК 09: Пользоваться профессиональной документацией на государственном и иностранном языках (Раздел III, п. 3.2). Требуется доступ к современным профессиональным базам данных и информационным системам (п. 4.3.1).	ОК 09: Пользоваться профессиональной документацией на государственном и иностранном языках (Раздел III, п. 3.2). Требуется доступ к современным профессиональным базам данных и информационным справочным системам, состав которых определяется и обновляется в рабочих программах (Раздел IV, п. 4.4, подп. «и»).

Отраженные в таблице закономерности характерны и для остальных вышеуказанных специальностей. Требования отрасли стремительно меняются. В вакансиях и профессиональных стандартах все чаще фигурируют пожелания к знанию основ защиты автоматизированных систем, работы с обновлениями ПО, пониманию сетевых угроз, и образовательные программы должны соответствовать новым требованиям.

Анализ текущего состояния преподавания ИБ в образовательных учреждениях СПО водного транспорта

Контент-анализ типовых учебных планов и рабочих программ ряда морских колледжей (на примере открытых источников и учебно-методической документации) подтверждает выявленный нормативный диссонанс. Основы информационной безопасности, если и присутствуют, то в рамках общих дисциплин «Информатика» или «Информационные технологии». Их содержание ограничивается базовыми понятиями о вирусах и антивирусах, что абсолютно недостаточно для морского контекста. Часов, выделяемых на эти темы, катастрофически мало.

Можно выделить следующие ключевые проблемы практического характера:

1. Отсутствие отраслевой специфики: общие знания по ИБ не привязаны к реальным судовым системам, процедурам и регламентам.
2. Дефицит практики: полностью отсутствуют лабораторные работы или тренажеры, моделирующие кибератаки на контуры судовой автоматизации или навигации. Нет разбора реальных отраслевых кейсов.
3. Кадровый дефицит: преподаватели информатики редко обладают глубокими знаниями о морском оборудовании, а преподаватели специальных дисциплин зачастую некомпетентны в вопросах современной кибербезопасности.

На основе проведенного анализа авторы предлагают модель поэтапной интеграции ИБ-компонентов, сочетающую в себе как техническую содержательность, так и педагогическую реализуемость. В основе предлагаемой модели лежат следующие принципы:

— Практико-ориентированность: Все знания должны быть применимы в будущей профессиональной деятельности.
— Междисциплинарность: Интеграция тем ИБ в профессиональные модули (навигация, эксплуатация СЭУ, электрооборудование).
— Непрерывность и сквозной характер: Формирование компетенций на протяжении всего срока обучения.
— Соответствие международным стандартам: Опора на документы ИМО и лучшие мировые практики.

Учитывая жесткость ФГОС, наиболее реалистичным и быстрым видится комбинированный поэтапный подход к решению обозначенной проблемы.

На первом этапе (ближайшая перспектива). Разработка и внедрение сквозного интегрированного модуля «Основы кибербезопасности на водном транспорте» объемом 18–24 часа в рамках вариативной части учебного плана. Модуль должен быть адаптивным и включаться в программы разных специальностей.

На втором этапе (стратегическая перспектива). Закрепление в новых поколениях ФГОС СПО отдельной профессиональной компетенции, связанной с обеспечением киберустойчивости рабочих мест, и выделение под ее формирование отдельной учебной дисциплины (36–48 часов).

В качестве возможного варианта содержательного наполнения модуля может быть предложен следующий набор блоков:

— Блок 1. Контекст и нормативное регулирование (4 ч.): Киберугрозы для судоходства. Обзор резолюций ИМО MSC.428(98) и MSC-FAL.1/Circ.3. Ответственность членов экипажа.
— Блок 2. Основы кибергигиены в морской среде (6 ч.): Безопасное использование съемных носителей, email, интернета в море. Социальная инженерия (фишинг) в условиях судна. Политика паролей и обновления ПО. Инциденты с личными устройствами.

— Блок 3. Уязвимости судовых систем (6 ч.): Знакомство с архитектурой сетей на судне (операционные и информационные технологии). Критические системы (ЭКНИС, IBS, PMS, грузовые системы). Физическая безопасность доступа к оборудованию.
— Блок 4. Действия в случае инцидента (2 ч.): Алгоритм действий при подозрении на кибератаку. Кому и как докладывать. Базовые принципы сохранения доказательств.

С учётом необходимости выработки у обучающихся устойчивых навыков в области информационной безопасности, предлагаемый модуль будет неэффективен без детальной проработки практического компонента

Необходимо:

— Разработать виртуальные лабораторные работы на основе симуляторов (например, использование возможностей навигационных тренажеров для демонстрации последствий GPS-спуфинга).
— Внедрить разбор конкретных кейсов (на основе открытых отчетов об инцидентах).
— Создать интерактивные тренажеры по распознаванию фишинговых писем в морском контексте.

Выводы

Проведенный анализ однозначно свидетельствует о наличии значительного пробела в подготовке специалистов среднего звена для водного транспорта в сфере противодействия современным киберугрозам. Требования международного морского права и реалии эксплуатации цифровых судовых систем вступили в противоречие с содержанием действующих учебных программ.

Наиболее оперативным и доступным решением выявленной проблемы может стать инициатива самих образовательных организаций по использованию вариативной части стандартов. Выделение ресурсов для включения специализированного модуля по основам кибербезопасности позволит начать подготовку кадров, отвечающих запросам отрасли, уже сегодня.

Тренды автономного судоходства, интеграции искусственного интеллекта в системы управления и глобального Интернета вещей (IoT) на флоте предъявляют еще более высокие требования к компетенциям будущих специалистов. Образовательная программа должна не только реагировать на текущие вызовы, но и закладывать основы для понимания принципов безопасности систем с высокой степенью автономии. Формирование «культуры кибербезопасности» – не как набора правил, а как неотъемлемого элемента профессионального мышления – должно стать стратегической задачей системы СПО.

В свете вышеизложенного можно порекомендовать образовательным учреждениям водного транспорта:

1. Разработать и утвердить типовой учебно-методический комплекс (УМК) по модулю «Основы кибербезопасности на водном транспорте» для системы СПО.
2. Создать программы повышения квалификации для преподавательского состава морских колледжей совместно с ведущими отраслевыми компаниями (судовладельцами, IT-интеграторами) и профильными вузами.
3. Инициировать проекты по разработке и внедрению в учебный процесс специализированных кибер-полигонов и программных симуляторов, моделирующих судовые сети и системы.
4. Активнее привлекать работодателей к формированию образовательного контента и оценке результатов обучения.

Реализация данных мер будет способствовать созданию кадрового потенциала, способного обеспечить киберустойчивость российского водного транспорта в условиях цифровой экономики.

Список источников

1. Приказ Минобрнауки России от 07.05.2014 № 441 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.03 Судовождение».

2. Приказ Минпросвещения России от 02.12.2020 № 691 (ред. от 03.07.2024) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.03 Судовождение».
3. Приказ Минпросвещения России от 12.12.2024 № 872 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.03 Судовождение».
4. Приказ Минобрнауки России от 07.05.2014 № 443 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.05 Эксплуатация судовых энергетических установок».
5. Приказ Минпросвещения России от 26.11.2020 № 674 (ред. от 01.09.2022) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.05 Эксплуатация судовых энергетических установок».
6. Приказ Минпросвещения России от 12.12.2024 № 873 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.05 Эксплуатация судовых энергетических установок».
7. Приказ Минобрнауки России от 07.05.2014 № 444 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.06 Эксплуатация судового электрооборудования и средств автоматики».
8. Приказ Минпросвещения России от 26.11.2020 № 675 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.06 Эксплуатация судового электрооборудования и средств автоматики».
9. Приказ Минпросвещения России от 13.12.2024 № 893 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 26.02.06 Эксплуатация судового электрооборудования и средств автоматики».
10. Приказ Минобрнауки России от 28.07.2014 № 834 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 38.02.03 Операционная деятельность в логистике».
11. Приказ Минпросвещения России от 21.04.2022 № 257 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 38.02.03 Операционная деятельность в логистике».
12. Резолюция ИМО MSC.428(98) «Меры по повышению безопасности морской отрасли в киберпространстве». ИМО, 2017.
13. *Ривкин Б.С.* Кибербезопасность на море. Навигационный аспект // Гироскопия и навигация. 2023. Т. 31. № 4 (123). – URL: https://elektropribor.spb.ru/wp-content/uploads/2025/10/167-191-%D0%A0%D0%B8%D0%B2%D0%BA%D0%B8%D0%BD.pdf
14. Руководящие указания ИМО MSC-FAL.1/Circ.3/Rev.3 «Руководство по управлению киберрисками на морском транспорте». ИМО, 2025.
15. *Семенов С.А.* Морская кибербезопасность: 01.01.2021 // Морские Вести России. 2020. – URL: https://morvesti.ru/analitika/1692/86359/?ysclid=mj4o8c463170929095
16. MARITIME CYBER PRIORITY 2024/2025 // DNV GL. 2025.

References

1. Order of the Ministry of Education and Science of the Russian Federation dated 05/07/2014 No. 441 «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.03 Navigation».
2. Order of the Ministry of Education of the Russian Federation dated 02.12.2020 No. 691 (as amended on 03.07.2024) «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.03 Navigation».

3. Order of the Ministry of Education of the Russian Federation No. 872 dated 12.12.2024 «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.03 Navigation».
4. Order of the Ministry of Education and Science of the Russian Federation dated 05/07/2014 No. 443 «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.05 Operation of marine power plants».
5. Order of the Ministry of Education of the Russian Federation dated 11/26/2020 No. 674 (as amended on 09/01/2022) «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.05 Operation of marine power plants».
6. Order of the Ministry of Education of the Russian Federation dated 12/12/2024 No. 873 «On approval of the Federal State educational standard of secondary vocational education in the specialty 26.02.05 Operation of marine power plants».
7. Order of the Ministry of Education and Science of Russia dated 07.05.2014 No. 444 «On Approval of the Federal State Educational Standard of Secondary Professional Education for Specialty 26.02.06 Operation of Shipborne Electrical Equipment and Automation Means».
8. Order of the Ministry of Education of Russia dated 26.11.2020 No. 675 «On Approval of the Federal State Educational Standard of Secondary Professional Education for Specialty 26.02.06 Operation of Shipborne Electrical Equipment and Automation Means».
9. Order of the Ministry of Education of Russia dated 13.12.2024 No. 893 «On Approval of the Federal State Educational Standard of Secondary Professional Education for Specialty 26.02.06 Operation of Shipborne Electrical Equipment and Automation Means».
10. Order of the Ministry of Education and Science of Russia dated 28.07.2014 No. 834 «On Approval of the Federal State Educational Standard of Secondary Professional Education for Specialty 38.02.03 Operational Activities in Logistics».
11. Order of the Ministry of Education of Russia dated 21.04.2022 No. 257 «On Approval of the Federal State Educational Standard of Secondary Professional Education for Specialty 38.02.03 Operational Activities in Logistics».
12. IMO resolution MSC.428(98) «Measures to enhance the security of the maritime industry in cyberspace». IMO, 2017.
13. *Rivkin B.S.* Cybersecurity at sea. Navigation aspect // Gyroscopy and navigation. 2023. Tom 31. No. 4 (123). – URL: https://elektropribor.spb.ru/wp-content/uploads/2025/10/167-191-%D0%A0%D0%B8%D0%B2%D0%BA%D0%B8%D0%BD.pdf
14. IMO Guidelines MSC-FAL.1/Circ.3/Rev.3 «Guidelines for managing cyber risks in maritime transport». – IMO, 2025.
15. *Semenov S.A.* Marine cybersecurity: 01.01.2021 // Maritime News of Russia. 2020. – URL: https://morvesti.ru/analitika/1692/86359/?ysclid=mj4o8c463170929095
16. MARITIME CYBER PRIORITY 2024/2025 // DNV GL. 2025.

Статья поступила в редакцию 28.12.2025; одобрена после рецензирования 12.01.2026; принята к публикации 12.01.2026.
The article was submitted 28.12.2025; approved after reviewing 12.01.2026; accepted for publication 12.01.2026.