ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)

УТВЕРЖДАЮ
Директор ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)
_____ С.И. Василиади
«10» января 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Кибербезопасность морского транспорта и готовность к сертификации»

Вид: дополнительная профессиональная программа повышения квалификации.

Показатель	Значение
Объём	72 учебных часов
Форма обучения	Заочная, с применением электронного обучения и дистанционных образовательных технологий
Способ реализации	Дистанционно: электронные материалы, консультации, практические задания и дистанционный контроль
Категория слушателей	Ответственные за кибербезопасность судоходных организаций, специалисты береговых служб, технические руководители и аудиторы систем управления безопасностью.
Порядок допуска	Лица, имеющие или получающие среднее профессиональное и (или) высшее образование (ч. 3 ст. 76 № 273-ФЗ).
Итоговый документ	Удостоверение о повышении квалификации при успешной итоговой аттестации

1. Общая характеристика и цель

Цель: Совершенствование компетенций по управлению киберрисками морского транспорта, проверке готовности к внешней оценке и подготовке свидетельств выполнения требований.

Продолжительность и учебный график устанавливаются настоящей программой; даты проведения занятий определяются расписанием конкретной группы. Учёт трудоёмкости ведётся в учебных часах. Для занятий применяется академический час 45 минут.

Нормативная основа: Федеральный закон от 29.12.2012 № 273-ФЗ; приказ Минобрнауки России от 24.03.2025 № 266; постановление Правительства РФ от 11.10.2023 № 1678. Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024) применяется в части специальных требований к ДПП в области информационной безопасности.

Содержание учитывает характер профессиональной деятельности и необходимые квалификационные требования к заявленной категории слушателей; освоение программы не присваивает новую квалификацию.

2. Планируемые результаты

Формируемые и совершенствуемые компетенции:

- ПК1. Соотносить требования и рекомендации отрасли с судовыми и береговыми процессами.
- ПК2. Формировать перечень киберрисков, мер защиты и подтверждающих документов.
- ПК3. Проводить внутреннюю проверку готовности и планировать устранение несоответствий.

По завершении обучения слушатель должен знать: специфику управления киберрисками на судах и в береговой инфраструктуре, принципы документирования мер и организации внутреннего аудита.

По завершении обучения слушатель должен уметь: составлять матрицу требований, программу самооценки, перечень свидетельств и план корректирующих действий.

3. Учебный план

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
1	Отраслевые требования и модель управления	14	5	6	3	Текущий контроль
2	Оценка киберрисков судна и береговых служб	16	5	6	5	Текущий контроль
3	Технические и организационные меры	16	5	6	5	Текущий контроль
4	Реагирование, непрерывность и обучение	12	4	5	3	Текущий контроль
5	Внутренняя оценка и готовность к сертификации	10	3	4	3	Текущий контроль
	Итоговая аттестация	4	0	4	0	Тест и кейс
	ВСЕГО	72	22	31	19	

Теор. — теоретическое освоение материала; практ. — практические занятия и задания с обратной связью; самост. — самостоятельная работа. Итоговый контроль включён в общую трудоёмкость.

4. Календарный учебный график

Период	Объём, ч.	Модули/контроль (№ и часы)
Неделя 1	30	1 (14 ч.); 2 (16 ч.)
Неделя 2	30	3 (16 ч.); 4 (12 ч.); 5 (2 ч.)
Неделя 3	12	5 (8 ч.); 6 (4 ч.)

График рассчитан из условной нагрузки не более 30 учебных часов в неделю. При формировании учебной группы конкретные даты и распределение занятий утверждаются расписанием без изменения общей трудоёмкости и итоговых результатов.

5. Рабочие программы дисциплин (модулей)

Модуль 1. Отраслевые требования и модель управления — 14 ч.

Содержание: ИМО и подход к управлению морскими киберрисками; Обязанности судовладельца и экипажа; Интеграция киберрисков в судовую систему управления.

Практическая работа: Составить матрицу применимых обязательств и рекомендаций.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 2. Оценка киберрисков судна и береговых служб — 16 ч.

Содержание: Активы, процессы и технологические связи; Сценарии нарушений безопасности и последствия; Реестр рисков и решения по их обработке.

Практическая работа: Подготовить часть реестра рисков по учебному судну.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 3. Технические и организационные меры — 16 ч.

Содержание: Сетевое разделение, доступ и защита данных; Взаимодействие судовых и береговых сетей; Управление подрядчиками и изменениями.

Практическая работа: Сформировать матрицу мер и ответственных исполнителей.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 4. Реагирование, непрерывность и обучение — 12 ч.

Содержание: Планы действий при киберинциденте; Резервирование, восстановление и учения; Порядок документирования событий и обучения экипажа.

Практическая работа: Разработать сценарий учения по инциденту.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 5. Внутренняя оценка и готовность к сертификации — 10 ч.

Содержание: План самооценки и контрольный лист; Свидетельства, несоответствия и корректирующие действия; Подготовка к внешнему аудиту без подмены процедуры сертификации.

Практическая работа: Составить итоговый перечень доказательств и план устранения замечаний.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

6. Организационно-педагогические условия

Обучение организуется в электронной образовательной среде с индивидуальным доступом слушателя к учебным материалам, заданиям и средствам связи с преподавателем. Взаимодействие возможно синхронно и асинхронно. Результаты работ и контроля фиксируются в электронной среде или в учётных ведомостях.

Кадровое обеспечение: преподаватели (специалисты), имеющие образование, профессиональную подготовку и опыт деятельности, соответствующие тематике преподаваемых модулей; при необходимости привлекаются практикующие специалисты.

Материально-техническое и информационное обеспечение: компьютер с доступом к сети Интернет, программные средства чтения учебных материалов, демонстрационные материалы, тестовая среда и учебные кейсы. Для практических заданий используются учебные данные, демонстрационные конфигурации, симуляторы или специально выделенные стенды по тематике курса.

Методическое обеспечение: конспекты и презентации, нормативные и эксплуатационные материалы из раздела 8, задания для самостоятельной работы, инструкции к практическим работам, контрольные вопросы и критерии оценивания.

Особенности ИБ: программа не предполагает использование сведений, составляющих государственную тайну, либо реальных ключей, паролей и конфиденциальных данных обучающихся или заказчиков. Дистанционно изучаются материалы и выполняются учебные задачи с применением стендов/симуляторов. Если конкретная практическая работа требует физического доступа к защищаемому оборудованию или иного режима, она проводится лишь при обеспечении соответствующих условий; возможность полностью дистанционного освоения проверяется до начала реализации.

Порядок актуализации и передачи: изменения содержания вносятся после проверки применимых требований законодательства и утверждаются директором. Передача программы сторонней образовательной организации допускается по оформленному соглашению с соблюдением прав на материалы и режима доступа; сведения ограниченного доступа в программу не включаются.

7. Контроль результатов и оценочные материалы

Текущий контроль проводится по заданиям модулей с результатом «зачтено/не зачтено». Слушатель получает комментарии к ошибкам и возможность повторного выполнения задания в пределах срока обучения.

Итоговый контроль: дистанционный тест и практико-ориентированный кейс. Тест содержит не менее 10 заданий по содержанию всех модулей. Для положительного результата требуется не менее 70% верных ответов и выполнение ключевых требований практического кейса. Допускается повторная проверка в порядке, предусмотренном локальными актами.

Типовые контрольные вопросы:

1. Что включает реестр морских киберрисков?

2. Какими документами может подтверждаться выполнение меры защиты?

3. Как распределяются функции судна и берегового офиса?

4. Как оформляется корректирующее действие по замечанию аудита?

5. Почему завершение учебной программы не заменяет внешнюю сертификацию?

Практическое итоговое задание: По учебной модели судоходной компании составить матрицу применимых требований, чек-лист самооценки готовности к внешнему аудиту и план устранения двух выявленных несоответствий.

Критерии оценки кейса: (1) корректно выделены исходные условия и риски; (2) действия и документы предложены последовательно; (3) применены уместные технические и организационные меры; (4) не предложены действия, противоречащие требованиям безопасности. Результат «зачтено» — выполнение не менее трёх из четырёх критериев при обязательном соблюдении критерия 4.

Освоение завершается итоговой аттестацией. Успешно прошедшему итоговую аттестацию слушателю выдаётся удостоверение о повышении квалификации в установленном организацией порядке. При неудовлетворительном результате действуют правила выдачи справки об обучении.

8. Основные нормативные и методические источники

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Приказ Минобрнауки России от 24.03.2025 № 266.
- Постановление Правительства РФ от 11.10.2023 № 1678.
- Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024).
- Документы Международной морской организации (ИМО) по киберрискам и управлению безопасностью судна.
- Применимые правила классификационных обществ и стандарты систем управления ИБ — в зависимости от объекта оценки.

Учебные и справочные материалы актуализируются перед реализацией очередной группы с учётом действующих редакций нормативных документов.