Федеральное агентство по рыболовству
БГАРФ ФГБОУ ВО «КГТУ»
Калининградский морской рыбопромышленный колледж

Утверждаю
Врио заместителя начальника колледжа
по учебно-методической работе
М.Ю. Никишин

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00861698655D171818D836B833A86412BD
Владелец: НИКИШИН МИХАИЛ ЮРЬЕВИЧ
Действителен: с 13.02.2026 до 09.05.2027

Рабочая программа учебной дисциплины

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

основной профессиональной образовательной программы среднего профессионального образования по специальности

09.02.12 Техническая эксплуатация и сопровождение информационных систем

МО-09 02 12-ОП.06. РП

РАЗРАБОТЧИК	Богатырева Т.Н.
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ	Судьбина Н.А.
ГОД РАЗРАБОТКИ	2026

СОДЕРЖАНИЕ ПРОГРАММЫ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебная дисциплина «ОП.06 Основы информационной безопасности» является обязательной частью общепрофессионального цикла плана ООП СПО в соответствии с ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем

1.1 Цель и место дисциплины в структуре образовательной программы

Цель учебной дисциплины «Основы информационной безопасности»: формирование навыков обучающихся по освоению профессиональных компетенций для цифровой экономики.

1.2 Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения дисциплины обучающийся должен

Код ПК, ОК	**Уметь**	**Знать**	**Владеть навыками**
ОК 01	выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы	структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях	
ОК 02	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации	
ПК 2.2	– Выполнять модульные тесты с использованием инструментов тестирования, в том числе автоматизированного тестирования – Использовать системы контроля дефектов ПО – Составлять отчет о выполнении тестирования ПО Работать в команде со специалистами по тестированию ПО и разработчиками	– Нормативно-технические материалы по вопросам испытания и тестирования ПО – Основные термины и сокращения, используемые в технической документации и принятые в организации – Основы работы в операционной системе, в которой производится тестирование, на уровне, необходимом для тестирования ПО соответствующего типа	– Проверки компонентов инструментария и тестируемого ПО на корректное начальное состояние для начала тестирования – Выполнения тестовых процедур на тестовых данных – Сравнения фактического и ожидаемого результатов выполнения тестовых процедур Формирования и представления отчетности о выполнении процесса тестирования ПО в

		– Основы теории алгоритмов и дискретной математики в объеме полученного профессионального образования Синтаксис языка программирования тестируемого ПО, особенности программирования на этом языке, стандартные библиотеки языка программирования	соответствии с установленными регламентами
ПК 2.5	– Находить и использовать информацию, необходимую для восстановления тестов после сбоя – Взаимодействовать с командой разработчиков при восстановлении системы после сбоя – Применять языки программирования для написания программного кода – Использовать системы автоматизированного тестирования ПО Составлять отчет о восстановлении работоспособности ПО	– Архитектуру тестируемой системы – Основы работы в операционной системе, в которой производится тестирование, на уровне, необходимом для тестирования разработанного ПО – Техники тестирования ПО, базирующиеся на интуиции и опыте инженера – Техники тестирования ПО, базирующиеся на спецификации – Техники тестирования ПО, ориентированные на код – Тестирование ПО, ориентированное на дефекты – Техники тестирования ПО, базирующиеся на условиях использования – Тестирование ПО, базирующееся на надежности инженерного процесса – Техники тестирования ПО, базирующиеся на природе приложения – Принципы регрессионного тестирования ПО – Алгоритмы решения типовых задач, области и способы их применения Основные термины и сокращения, используемые в технической документации и принятые в организации	– Определения причины сбоя системы совместно с разработчиками – Устранения причины сбоя системы, если она находится в компетенции специалиста, либо подготовка отчета руководителю и группе разработчиков – Выполнения настройки для повторного тестирования после сбоя – Восстановления/изменения автоматизированных тестов после сбоя при необходимости в соответствии с планом/регламентом восстановления – Проведения повторного тестирования ПО Формирования и представления отчетности о восстановлении работоспособности ПО в соответствии с установленными регламентами

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	**Объем в часах**	**В т.ч. в форме практ. подготовки**
Учебные занятия	24	
Практические занятия	8	8
Курсовая работа (проект)	-	-
Самостоятельная работа	4	-
Консультации		
Промежуточная аттестация в *форме (зачет, диф.зачет, экзамен)*		
Всего	**36**	**8**

2.2 Содержание дисциплины

Номер занятия *(сквозная нумерация)*	**Наименование разделов и тем учебной дисциплины**	общий объем образовательной программы, час								Средства обучения	Внеаудиторная работа (домашнее задание)	Уровень освоения	Используемые активные и интерактивные формы обучения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
		объем образовательной программы в ак.час.	объем работы обучающихся во взаимодействии с преподавателем, час						Самостоятельная работа					
			в т. ч. по видам занятий											
			Уроки, лекции	лабораторные занятия	практические занятия	Курсовая работа	консультации	Промежуточная аттестация						
	3 Семестр	***36***	***24***		***8***				***4***					
	Основы информационной безопасности													
1	Введение в информационную безопасность. Основные понятия и определения	*2/2*	*2/2*								*Выучить конспект*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
2	Актуальные угрозы и риски в информационной безопасности	*2/4*	*2/4*								*Оформление отчета*	*2*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
3	Нормативно-правовое регулирование в области ИБ	*2/6*	*2/6*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5

4	Практическая работа 1. Политики и процедуры безопасности. Оценка рисков и управление ими.	*2/8*			*2/2*						*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
5	Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	*2/10*	*2/8*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
6	Практическая работа 2. Основы криптографии: симметричные и асимметричные алгоритмы	*2/12*			*2/4*						*Выучить конспект*	*2*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
7	Хэширование и цифровые подписи	*2/14*	*2/10*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
8	Применение криптографии в приложениях	*2/16*	*2/12*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
9	Основы сетевой безопасности	*2/18*	*2/14*								*Оформление отчета*	*2*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
10	Защита от атак (DDoS, MITM и др.)	*2/20*	*2/16*								*Оформление отчета*	*2*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
11	Использование VPN и межсетевых экранов	*2/22*	*2/18*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
12	Уязвимости веб-приложений (OWASP Top Ten)	*2/24*	*2/20*								*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
13	Практическая работа 3. Безопасное программирование: лучшие практики	*2/26*			*2/6*							*2*	*ИЛ-2*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
14	Тестирование на проникновение и анализ уязвимостей	*2/28*	*2/22*								*Оформление отчета*	*2*	*ИЛ-2*	ОК 01, ОК 02, ПК 2,2, ПК 2.5

15	Практическая работа 4. Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	*2/30*			*2/8*						*Оформление отчета*	*1*	*ИЛ-1*	ОК 01, ОК 02, ПК 2,2, ПК 2.5
16	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика	*2/32*	*2/24*		*2/26*						*Оформление отчета*			ОК 01, ОК 02, ПК 2,2, ПК 2.5
17	Самостоятельная работа 1. Кибербезопасность. Промышленный шпионаж. OSINT	*2/34*							*2/2*		*Оформление отчета*			ОК 01, ОК 02, ПК 2,2, ПК 2.5
18	Самостоятельная работа 2. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	*2/36*							*2/4*		*Оформление отчета*			ОК 01, ОК 02, ПК 2,2, ПК 2.5
	ИТОГО по дисциплине	*36*	*24*		*8*				*4*					

3 УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение

Лаборатория № 4233 Программного обеспечения информационных технологий, оснащенная в соответствии с приложением 3 ОПОП-П.

Комплекты мебели для учебного процесса

Мультимедийное оборудование: персональные компьютеры, принтер, проектор, аудиоколонка.

Программноеобеспечение: Windows 10 Professional (Russian); Windows Server 2008 Standart, Enterprise and atacenterwich Service Pack 2 (x86); OfficeProjectProfessional 2007; en_office_visio_professional_2007_cd_x12-19212.

Средства обучения: доска классная, комплект учебно-наглядных пособий.

- компьютер с лицензионным программным обеспечением;
- TV для демонстрации экрана компьютера преподавателя;
- программный комплекс для демонстрации изображения на рабочие места;
-программа удаленного доступа к рабочему месту;
- подключение к Internet

Программное обеспечение: MicrosoftVolumeLicensingServiceCenter, Код соглашения V9002148, с 30.06.2016 по 30.06.2022г; Лицензионный сертифик(ат №17EO-171225-104450-377-871 KasperskyEndpointSecurityc 26.12.2017 по 13.03.2020 г

3.2 Учебно-методическое обеспечение

3.2.1 Основные печатные и/или электронные издания

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2024)

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Знает: - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; -основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с	Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; Знает алгоритмы выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные средства и устройства информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

использованием цифровых средств; - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения данных; - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем;	профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в	

- законодательные и нормативные акты в области безопасности информационных систем; -источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения;	области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; Понимает различные уязвимости и угрозы безопасности, а также способы	

- знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. ***Умеет:*** -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; - определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; - оценивать практическую значимость результатов поиска;	их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части; Умеет определять этапы решения задачи; Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять необходимые ресурсы; Владеет актуальными методами работы в профессиональной и смежных сферах; Может реализовывать составленный план; Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); Умеет определять задачи для поиска информации; Умеет определять необходимые источники информации; Планирует процесс поиска; Умеет структурировать получаемую информацию;	

- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	Может выделить наиболее значимое в перечне информации; Умеет оценивать практическую значимость результатов поиска; Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; Может использовать современное программное обеспечение; Может использовать различные цифровые средства для решения профессиональных задач; Понимает тексты на базовые профессиональные темы; Умеет шифровать данные и обеспечивать их конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	

5 СВЕДЕНИЯ О СОГЛАСОВАНИИ

Рабочая программа рассмотрена и одобрена на заседании методической комиссии «Информационных систем и программирования».
Протокол № 9 от «20» мая 2026 г.

Председатель методической комиссии _____/Т.Н.Богатырева/