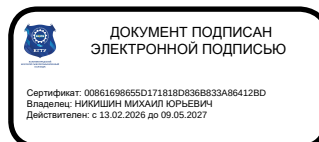




РАЦИОНАЛЬНЫЙ
МОДЕЛЬ ЭКОЛОГИЧЕСКОГО
РАЗВИТИЯ

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

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



Фонд оценочных средств
(приложение к рабочей программе дисциплины)

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

основной профессиональной образовательной программы среднего профессионального образования по специальности

09.02.11 Разработка и управление программным обеспечением

МО-09 02 11-ОП.05.ФОС

РАЗРАБОТЧИК
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ
ГОД РАЗРАБОТКИ

Шварц С-Н.Е.
Судьбина Н.А.
2026

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.2/11

Содержание

1 Паспорт фонда оценочных средств.....	3
1.1 Область применения фонда оценочных средств	3
1.2 Результаты освоения дисциплины	3
2 Перечень оценочных средств и критерии оценивания	3
3 Оценочные средства текущего контроля и промежуточной аттестации	6
4 Сведения о фонде оценочных средств и его согласование	6

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.3/11

1 Паспорт фонда оценочных средств

1.1 Область применения фонда оценочных средств

Фонд оценочных средств предназначен для оценки результатов освоения дисциплины ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1.2 Результаты освоения дисциплины

В результате изучения дисциплины обучающийся должен освоить следующие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, информационные технологии для выполнения задач профессиональной деятельности.

ПК 1.5. Обеспечивать защиту информации и конфиденциальность данных.

ПК 3.3. Анализировать требования безопасности информационных систем.

Перечень оценочных средств и критерии оценивания

Код формируемых компетенций	Индикаторы достижения компетенции	Результат обучения
ОК 01	Способен: 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	Способен: 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 1.5.	– шифровать данные и обеспечивать их конфиденциальность	– принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos и др.); – методы аутентификации и авторизации пользователей (пароли, сертификаты, биометрия); – законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS и др.)
ПК 3.3	– анализ требований безопасности информационных систем	– принципы безопасности информационных систем; – современные методы и технологии в области безопасности информационных систем; – законодательные и нормативные акты в области безопасности информационных систем;

2.1 К оценочным средствам текущего контроля успеваемости относятся:

Документ управляется программными средствами 1С: Колледж
Проверь актуальность версии по оригиналу, хранящемуся в 1С: Колледж

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.4/11

- тестовые задания открытого и закрытого типа;
- защита отчетов по практическим работам;

2.2 К оценочным средствам для промежуточной аттестации относятся:

- вопросы для подготовки к зачету;
- практические задания для подготовки к зачету;
- тестовые задания для подготовки к зачету.

2.3 Критерии оценки результатов освоения дисциплины

Критерии оценивания теоретических знаний:

«Отлично» - ставится, если обучающийся:

- а) точно формулирует ответы на поставленные в задании вопросы;
- б) дает правильные формулировки понятий и терминов по изученной дисциплине;

в) демонстрирует понимание материала, что выражается в умении обосновать свой ответ;

г) свободно обобщает и дифференцирует признаки и понятия;

д) правильно отвечает на дополнительные вопросы;

е) свободно владеет речью (демонстрирует связанность и последовательность в изложении) и т.п.

«Хорошо» - ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для отметки «отлично», но допускает единичные ошибки, которые сам же исправляет после замечания преподавателя.

«Удовлетворительно» - ставится, если обучающийся демонстрирует знание и понимание основных положений данной темы, но:

а) неточно и неуверенно воспроизводит ответы на поставленные в задании вопросы;

б) дает неточные формулировки понятий и терминов;

в) затрудняется обосновать свой ответ;

г) затрудняется обобщить или дифференцировать признаки и понятия;

д) затрудняется при ответах на дополнительные вопросы;

е) излагает материал недостаточно связно и последовательно с частыми заминками и перерывами и т.п.

«Неудовлетворительно» - ставится, если обучающийся демонстрирует незнание или непонимание большей части соответствующего раздела.

Критерии оценивания практических умений:

*Документ управляется программными средствами 1С: Колледж
Проверь актуальность версии по оригиналу, хранящемуся в 1С: Колледж*

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.5/11

«Отлично» ставится, если обучающийся:

- а) умеет подтвердить на примерах свое умение по выполнению полученного практического задания;
- б) умеет аргументировать свои действия при выполнении практического задания;
- в) целесообразно использует теоретический материал для выполнения задания;
- г) правильно использует необходимые приемы, методы, инструменты и другие ресурсы;
- д) демонстрирует умение действовать в стандартных и нестандартных профессиональных ситуациях;
- е) грамотное составление документов, относящихся к профессиональной деятельности и т.п.

«Хорошо» - ставится, если обучающийся демонстрирует практические умения, удовлетворяющие тем же требованиям, что и для отметки «отлично», но допускает единичные негрубые ошибки, которые сам же исправляет после замечания преподавателя.

«Удовлетворительно» - ставится, если обучающийся обнаруживает практические умения, но:

- а) затрудняется привести примеры, подтверждающие его умения, использованные в процессе выполнения практического задания;
- б) непоследовательно аргументирует свои действия, предпринятые им в процессе выполнения практического задания; аргументы, объясняющие его действия, предпринятые им в процессе выполнения практического задания;
- в) нецелесообразно использует теоретический материал для составления плана выполнения практического задания;
- г) излагает материал недостаточно связано и с последовательно с частыми заминками и перерывами;
- д) испытывает затруднения в действиях при нестандартных профессиональных ситуациях и т.п.

«Неудовлетворительно» - ставится, если обучающийся допускает грубые нарушения алгоритма действия или ошибки, влекущие за собой возникновение отрицательных последствий для оборудования, окружающей среды и экипажа судна, или (и) отсутствие умения действовать в стандартных профессиональных ситуациях,

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.6/11

или(и) демонстрирует незнание или непонимание большей части соответствующего раздела.

Критерии оценивания по дисциплине в форме тестирования:

«Отлично» - 81-100 % правильных ответов;

«Хорошо» - 61-80 % правильных ответов;

«Удовлетворительно» - 41-60% правильных ответов;

«Неудовлетворительно» - 0-40% правильных ответов.

3 Оценочные средства текущего контроля и промежуточной аттестации

Тестовые задания открытого и закрытого типа

Ключи правильных ответов выделены жирным шрифтом.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ: ОК 01, ОК 02, ПК 1.5, ПК 3.3.

Задания открытого типа

1. Наука о методах обеспечения конфиденциальности, целостности и доступности информации называется ... криптографией.
2. Свойство информации, заключающееся в её доступности только для authorised пользователей, — ... конфиденциальность.
3. Свойство информации, заключающееся в её защите от несанкционированного изменения, — ... целостность.
4. Свойство информации, заключающееся в её доступности для authorised пользователей в нужное время, — ... доступность.
5. Метод шифрования, при котором используется один ключ для шифрования и расшифровки, называется ... симметричным.
6. Метод шифрования, при котором используются два ключа (открытый и закрытый), называется ... асимметричным.
7. Преобразование данных в строку фиксированной длины с помощью математической функции называется ... хешированием.
8. Электронная подпись, подтверждающая авторство и целостность документа, называется ... цифровой подписью.
9. Атака, при которой злоумышленник перехватывает и изменяет сообщения между двумя сторонами, называется ... MITM (Man-in-the-Middle).
10. Атака, направленная на отказ в обслуживании путём перегрузки сервера запросами, называется ... DDoS-атакой.

Задания закрытого типа

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.7/11

Вопрос	Дистракторы	Ответ
1. Что такое конфиденциальность?	1) доступность только для authorised пользователей 2) защита от изменения 3) доступность в нужное время 4) шифрование данных	1
2. Что такое целостность информации?	1) защита от несанкционированного изменения 2) доступность только для authorised пользователей 3) доступность в нужное время 4) шифрование данных	1
3. Что такое доступность информации?	1) доступность для authorised пользователей в нужное время 2) защита от изменения 3) доступность только для authorised пользователей 4) шифрование данных	1
4. Что такое симметричное шифрование?	1) один ключ для шифрования и расшифровки 2) два ключа 3) хеширование 4) цифровая подпись	1
5. Что такое асимметричное шифрование?	1) два ключа (открытый и закрытый) 2) один ключ 3) хеширование 4) цифровая подпись	1

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.8/11

6. Что такое хеширование?	1) преобразование данных в строку фиксированной длины 2) шифрование с открытым ключом 3) сжатие данных 4) формат передачи	1
7. Что такое цифровая подпись?	1) электронная подпись, подтверждающая авторство и целостность 2) пароль 3) тип шифрования 4) формат данных	1
8. Что такое MITM-атака?	1) перехват и изменение сообщений между сторонами 2) отказ в обслуживании 3) внедрение SQL-кода 4) межсайтовый скриптинг	1
9. Что такое DDoS-атака?	1) отказ в обслуживании путём перегрузки сервера 2) перехват сообщений 3) внедрение вредоносного кода 4) кража паролей	1
10. Что такое SSL/TLS?	1) протоколы безопасности для защиты передачи данных 2) языки программирования 3) базы данных 4) системы управления версиями	1

Вопросы для подготовки к зачету

1. Введение в информационную безопасность. Основные понятия и определения.
2. Актуальные угрозы и риски в информационной безопасности.
3. Нормативно-правовое регулирование в области информационной безопасности.
4. Политики и процедуры безопасности. Оценка рисков и управление ими.

*Документ управляется программными средствами 1С: Колледж
Проверь актуальность версии по оригиналу, хранящемуся в 1С: Колледж*

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.9/11

5. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.).
6. Основы криптографии: симметричные и асимметричные алгоритмы.
7. Хэширование и цифровые подписи.
8. Применение криптографии в приложениях.
9. Основы сетевой безопасности.
10. Защита от атак (DDoS, MITM и др.).
11. Использование VPN и межсетевых экранов.
12. Уязвимости веб-приложений (OWASP Top Ten).
13. Безопасное программирование: лучшие практики.
14. Тестирование на проникновение и анализ уязвимостей.
15. Шифрование данных в покое и в транзите.
16. Резервное копирование и восстановление данных.
17. Управление доступом к данным.
18. Реакция на инциденты и управление ими.
19. Анализ инцидентов и цифровая криминалистика.
20. Кибербезопасность. Промышленный шпионаж. OSINT.
21. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн).
22. Этические аспекты информационной безопасности.

Практические задания для подготовки к зачету

1. Разработать политику безопасности для условной организации.
2. Провести оценку рисков информационной безопасности.
3. Зашифровать данные симметричным алгоритмом.
4. Зашифровать данные асимметричным алгоритмом.
5. Вычислить хеш-сумму файла.
6. Создать цифровую подпись документа.
7. Настроить VPN-подключение.
8. Настроить межсетевой экран.
9. Провести анализ уязвимостей веб-приложения (OWASP Top Ten).
10. Разработать безопасный код (защита от SQL-инъекций).
11. Провести тестирование на проникновение (базовый уровень).
12. Зашифровать данные в покое и в транзите.
13. Настроить резервное копирование данных.
14. Настроить управление доступом к данным.
15. Разработать план реагирования на инциденты.
16. Провести анализ инцидента и цифровую криминалистику.
17. Настроить хэширование паролей и двухфакторную аутентификацию.
18. Провести анализ безопасности мобильного приложения.

Тестовые задания для подготовки к зачету

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.10/11

Вопрос	Дистракторы	Ответ
1. Что такое конфиденциальность?	1) доступность только для authorised пользователей 2) защита от изменения 3) доступность в нужное время 4) шифрование данных	1
2. Что такое целостность информации?	1) защита от несанкционированного изменения 2) доступность только для authorised пользователей 3) доступность в нужное время 4) шифрование данных	1
3. Что такое доступность информации?	1) доступность для authorised пользователей в нужное время 2) защита от изменения 3) доступность только для authorised пользователей 4) шифрование данных	1
4. Что такое симметричное шифрование?	1) один ключ для шифрования и расшифровки 2) два ключа 3) хеширование 4) цифровая подпись	1
5. Что такое асимметричное шифрование?	1) два ключа (открытый и закрытый) 2) один ключ 3) хеширование 4) цифровая подпись	1
6. Что такое хеширование?	1) преобразование данных в строку фиксированной длины 2) шифрование с открытым ключом 3) сжатие данных 4) формат передачи	1

МО-09 02 11-ОП.05.ФОС	КМРК БГАРФ ФГБОУ ВО «КГТУ»	
	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	С.11/11

7. Что такое цифровая подпись?	1) электронная подпись, подтверждающая авторство и целостность 2) пароль 3) тип шифрования 4) формат данных	1
8. Что такое MITM-атака?	1) перехват и изменение сообщений между сторонами 2) отказ в обслуживании 3) внедрение SQL-кода 4) межсайтовый скриптинг	1
9. Что такое DDoS-атака?	1) отказ в обслуживании путём перегрузки сервера 2) перехват сообщений 3) внедрение вредоносного кода 4) кража паролей	1
10. Что такое SSL/TLS?	1) протоколы безопасности для защиты передачи данных 2) языки программирования 3) базы данных 4) системы управления версиями	1

4 Сведения о фонде оценочных средств и его согласование

Фонд оценочных средств для аттестации по дисциплине ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ представляет собой компонент основной образовательной программы среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением.

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии «Информационных систем и программирования»

Протокол № 9 от «20» мая 2026 г

Председатель методической комиссии _____/Т.Н. Богатырева/