

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г., протокол № 8
Исполняющий обязанности
заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.В.ДВ.05.02 Системы анализа уязвимостей ПО

Направление подготовки
10.03.01 Информационная безопасность
профиль
Безопасность автоматизированных систем (по отрасли или в сфере профессиональной
деятельности)

**Уровень высшего образования
БАКАЛАВРИАТ**

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;
ПКС-2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКС-2.1 - Знает основные меры по защите информации в автоматизированных системах; ПКС-2.2 - Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах. Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; ПКС-2.3 - Владеет навыками использования типовых программных средства резервирования и восстановления информации в автоматизированных системах.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1 семестр			
1.	Тема 1. Понятие защищенности ИС	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
2.	Тема 2. Средства анализа защищенности сетевых сервисов	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
3.	Тема 3. Средства анализа защищенности web-приложений	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету
4.	коллоквиумы	ПКС-1, ПКС-2	контрольные вопросы, вопросы к коллоквиуму
5.	зачет	ПКС-1, ПКС-2	контрольные вопросы, вопросы к коллоквиуму, вопросы к зачету

Лабораторное занятие №1 (6 ч.)

Тема Поиск уязвимостей в программной реализации

Вопросы для обсуждения:

1. Понятие защищенности автоматизированной системы.
2. Нормативная база.
3. Методика анализа защищенности. Исходные данные обследуемой ИС.
4. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.
5. Средства анализа параметров защиты.

6. Классификация методов анализа параметров защиты (Security Benchmarks).
7. Спецификации Security Benchmarks.
8. Спецификации первого уровня для базового (минимального) уровня защиты.
9. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.

Лабораторное занятие №2 (12 ч.)

Тема Средства анализа защищенности сетевых сервисов

Вопросы для обсуждения:

1. Уязвимости сетевых протоколов, служб, сервисов.
2. Классификация средств анализа защищенности сетевых сервисов.
3. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС.
4. Функции, методика использования.

Лабораторное занятие №3 (12 ч.)

Тема Средства анализа защищенности web-приложений

Вопросы для обсуждения:

1. Анализ и классификация уязвимостей web-приложений.
2. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).
3. Комплексная оценка защищенности web-приложения.
4. Принцип «черного ящика»
5. Принцип «серого ящика».
6. Принцип «белого ящика».
7. Инструментальные средства анализа защищенности web-приложения.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (зачет)			20	43
Итого за семестр			60	100

Примерные вопросы к зачету

1. Понятие защищенности автоматизированной системы.
2. Нормативная база.
3. Методика анализа защищенности. Исходные данные обследуемой ИС.
4. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.
5. Средства анализа параметров защиты.
6. Классификация методов анализа параметров защиты (Security Benchmarks).
7. Спецификации Security Benchmarks.
8. Спецификации первого уровня для базового (минимального) уровня защиты.

9. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.
10. Уязвимости сетевых протоколов, служб, сервисов.
11. Классификация средств анализа защищенности сетевых сервисов.
12. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС.
13. Функции, методика использования.
14. Анализ и классификация уязвимостей web-приложений.
15. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).
16. Комплексная оценка защищенности web-приложения.
17. Принцип «черного ящика»
18. Принцип «серого ящика».
19. Принцип «белого ящика».
20. Инструментальные средства анализа защищенности web-приложения.

Критерии оценки:

Оценка «зачтено» выставляется:

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями практические задания.

Составитель _____
(подпись)

Вашакидзе Н.С

«13» марта 2024 г.