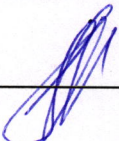


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сахалинский государственный университет»

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.08 Разработка и эксплуатация защищенных автоматизированных
систем**

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)

| Коды компетенции | Содержание компетенций | Код и наименование индикатора достижения компетенции |
|------------------|--|--|
| ПКС–3 | Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем | <p>ПКС-3.1 Знать программно-аппаратные средства защиты информации, современные подходы к разработке и эксплуатации автоматизированных систем, средства управления и защиты автоматизированных систем.</p> <p>ПКС-3.2 Уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска), в том числе средства, осуществляющие непрерывный мониторинг защищенности автоматизированных систем.</p> <p>ПКС-3.3 Владеть навыками выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</p> |

2. Паспорт фонда оценочных средств по дисциплине (модулю)

| № п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|-------|--|---|--|
| 1 | Тема 1. Защищенные автоматизированные системы: понятие и виды | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 2 | Тема 2. Угрозы надежности и безопасности программного обеспечения | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 3 | Тема 3. Основы разработки надежных автоматизированных систем | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 4 | Тема 4. Общие принципы проектирования защищенных автоматизированных систем | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 5 | Тема 5. Качество программного | ПКС-3 | Лабораторный практикум, |

| | | | |
|---|---|-------|--|
| | обеспечения автоматизированных систем | | опрос, контрольные вопросы |
| 6 | Тема 6. Методы и технологии обеспечения безопасности программного обеспечения | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 7 | Тема 7. Основы эксплуатации защищенных автоматизированных систем | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |
| 8 | Тема 8. Диагностика программных и аппаратных средств защиты автоматизированных систем | ПКС-3 | Лабораторный практикум, опрос, контрольные вопросы |

Темы лабораторного практикума

Лабораторная работа 1. Изучение содержания и последовательности работ по защите информации.

Цель работы: изучить содержание и последовательность работ, выполняемых при построении комплексной системы защиты информации (для выбранного объекта информатизации). Закрепить знания, полученные на лекции.

Лабораторная работа 2. Изучение методов комплексного исследования объекта информатизации.

Цель работы: изучить положительные и отрицательные стороны проведения обследования защищенности объекта информатизации (ОИ) посредством существующих стандартов и методик.

Лабораторная работа 3. Изучение информации, циркулирующей в корпоративной информационном системе.

Цель работы: научиться анализировать информацию, циркулирующую в корпоративной информационной системе, научиться строить диаграмму информационных потоков.

Лабораторная работа 4. Изучение построения системы защиты информации на основе нормативных актов и методических указаний.

Цель работы: изучить перечень нормативных документов на основе которых осуществляется построение системы защиты информации.

Лабораторная работа 5. Построение модели угроз персональных данных в информационной системе.

Цель работы: изучить нормативные документы ФСТЭК по построению модели угроз. Построить модель угроз информационной системы персональных данных функционирующей в организации (на выбор).

Лабораторная работа 6. Изучение действующей нормативной документации объекта информатизации.

Цель работы: изучить действующую нормативную документацию выбранного объекта информатизации.

Лабораторная работа 7. Составление плана мероприятий по улучшению защищенности объекта информатизации.

Цель работы: изучить методику составления плана мероприятий по улучшению защищённости объекта информатизации.

Лабораторная работа 8. Разработка политики информационной безопасности.

Цель работы: изучить структуру типовой политики информационной безопасности и научиться составлять частную политику информационной безопасности.

Лабораторная работа 9. Исследование методов выбора рационального варианта системы защиты информации на основе экспертной информации.

Цель работы: изучить метод экспертной оценки информации, изучить методы выбора рационального варианта системы защиты на основе экспертной информации.

Лабораторная работа 10. Исследование методик расчета показателя качества системы защиты информации.

Цель работы: изучить методику расчёта показателя качества системы защиты информации

Лабораторная работа 11. Изучение методов построения комплексной системы организационных и технических мер по защите информации.

Цель работы: изучить методы построения КСЗИ организационных и технических мер по защите информации.

Лабораторная работа 12. Изучение методов построения комплексной защиты сетевой файловой системы.

Цель работы: изучить методы построения защищённой сетевой файловой системы.

Лабораторная работа 13. Комплексная защита электронной почты и документооборота.

Цель работы: изучить методы комплексного построения системы защиты электронной почты и документооборота.

Лабораторная работа 14. Изучение методов построения комплексной защиты сетевых приложений и баз данных.

Цель работы: изучить методы построения комплексной защиты сетевых приложений и баз данных.

Лабораторная работа 15. Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры.

Цель работы: изучить методы построения комплексной защиты телекоммуникационной инфраструктуры.

Лабораторная работа 16. Изучение методов построения комплексной защиты управления информационной безопасностью.

Цель работы: изучить методы построения комплексной защиты управления информационной безопасностью.

Лабораторная работа 17. Изучение методики составления испытаний системы защиты информации.

Цель работы: научиться составлять комплексную методику испытаний системы защиты для выявления недоработок спроектированной системы защиты.

Контрольные вопросы

1. Виды автоматизированных систем (АС).
2. Общая характеристика систем автоматизации управленческой деятельности.

Структура автоматизированных систем по видам обеспечения.

3. Безопасность информации в автоматизированных системах.
4. Классификационные схемы объектов защиты в автоматизированных (компьютерных) системах.
5. Объекты защиты в защищенных автоматизированных системах.
6. Общая характеристика стандартов безопасности компьютерных систем.
7. Жизненный цикл защищенных автоматизированных систем – создание, эксплуатация и развитие, вывод из эксплуатации.
8. Общие положения по эксплуатации изделий, комплексов, средств деятельности.
9. Понятие эксплуатации и системы эксплуатации изделий.
10. Организационные мероприятия по эксплуатации, их содержание и общая характеристика.
11. Технические мероприятия по эксплуатации защищенных автоматизированных систем - применение по назначению, техническое обслуживание, ремонт, хранение, сбережение, транспортирование, консервация.
12. Понятие, содержание и виды технического обслуживания (регламентных работ).
13. Составляющие эксплуатации защищенных автоматизированных систем.
14. Особенности эксплуатации защищенных автоматизированных систем.
15. Угрозы безопасности на стадии эксплуатации и сопровождения АС.
16. Органы системы управления эксплуатацией защищенных автоматизированных систем.
17. Функции и компетенции инженерно-технических, информационно-технологических и обеспечивающих подразделений, подразделений по защите информации.
18. Планирование эксплуатации защищенных автоматизированных систем.
19. Мониторинг, контроль, аудит безопасности в защищенных автоматизированных системах.
20. Конструкторские эксплуатационные документы.
21. Эксплуатационные документы организации – организационно-распорядительная документация (положения, инструкции, приказы) и учетно-отчетная документации по вопросам эксплуатации.

Критерии оценивания:

Оценка **«отлично»** 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.

Оценка **«хорошо»** выставляется 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.

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

Примерный перечень вопросов к экзамену

1. Понятие общей надежности автоматизированных систем.
2. Виды автоматизированных систем.
3. Общая характеристика систем автоматизации управленческой деятельности.
4. Информационные технологии, используемые в автоматизированных системах.
5. Жизненный цикл автоматизированных систем.
6. Основные угрозы безопасности информации в автоматизированных системах.
7. Модели нарушителя в автоматизированных системах.
8. Уязвимости программного обеспечения автоматизированных систем.
9. Угрозы безопасности на стадии эксплуатации и сопровождения автоматизированных систем.
10. Ошибки в программном обеспечении.
11. Характерные недостатки эксплуатируемых программ.
12. Вредоносные программы.
13. Последовательность и содержание этапов разработки автоматизированных систем.
14. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.
15. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
16. Критерии оценки защищенности автоматизированных систем.
17. Методы обеспечения информационной безопасности автоматизированных систем.
18. Проектирование защищенных автоматизированных систем.
19. Методы проектирования.
20. Содержание этапов проектирования.
21. Основы ведения конструкторской документации.
22. Структура и содержание технического задания.
23. Построение комплексной защиты автоматизированных систем.
24. Основы проектирования комплексной защиты информационной безопасности от несанкционированного доступа.
25. Средства обеспечения надежности защищенных автоматизированных систем.
26. Технологии создания отказоустойчивых систем.
27. Модели качества программного обеспечения.
28. Метрики качества программного обеспечения.
29. Классификация метрик качества программ.
30. Классификация метрик сложности программ.
31. Обеспечение надежности и безопасности программного обеспечения на различных этапах жизненного цикла.
32. Жизненный цикл функциональной надежности программного обеспечения.
33. Жизненный цикл обеспечения безопасности автоматизированных систем.
34. Спецификация требований к программному обеспечению.
35. Технология разработки архитектуры надежной программы.
36. Классификация методов построения архитектуры надежной программы.
37. Проектирование надежного программного обеспечения и его реализация.
38. Интеграция программного обеспечения с аппаратными средствами.
39. Спецификация требований к функциональной надежности автоматизированных систем.
40. Аттестация автоматизированных систем по требованиям безопасности.
41. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации.
42. Особенности эксплуатации автоматизированных систем на объекте защиты.

43. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.
44. Технические и программные средства защиты автоматизированных систем от несанкционированного доступа.
45. Организация технического обслуживания защищенных автоматизированных систем.
46. Содержание и порядок ведения эксплуатационной документации.
47. Методы проверки защищенных автоматизированных систем.
48. Содержание и порядок ведения эксплуатационной документации.
49. Средства диагностирования защищенных автоматизированных систем.
50. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств автоматизированных систем.
51. Технологическое оборудование для ремонта аппаратных средств автоматизированных систем.
52. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования.
53. Аппаратнопрограммные средства диагностики автоматизированных систем.
54. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.
55. Диагностика программных и аппаратных средств автоматизированных систем.

Критерии оценивания экзамена

– Оценка **«отлично»** выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, показывает владение теорией, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

– Оценка **«хорошо»** выставляется 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.

– Оценка **«удовлетворительно»** выставляется 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 **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Составитель
«12» марта 2024 г.



к.п.н., доцент Корнева О.С.