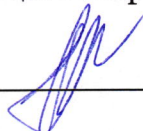


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

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.О.28 Комплексное обеспечение защиты информации объекта
информатизации**

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

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знать основные методы принятия обоснованных экономических решений в профессиональной деятельности УК-9.2 Уметь принимать обоснованные экономические решения в различных областях жизнедеятельности УК-9.3 Иметь навыки принятия обоснованных экономических решений в различных областях жизнедеятельности
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа.
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 - Знает принципы формирования политики информационной безопасности автоматизированных систем; ОПК-10.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; ОПК-10.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 - Знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных автоматизированных систем; ОПК-12.2 - Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-12.3 - Владеет навыками проектирования элементов защищенных автоматизированных

		систем и разработки необходимой технической документации в области проектирования защищенных автоматизированных систем с учетом действующих нормативных и методических документов.
ОПК-4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 - Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; ОПК-4.1.2 - Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; ОПК-4.1.3 - Владеет навыками разработки политики безопасности информации автоматизированных систем.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)	УК-9; ОПК-6; ОПК-10; ОПК-12; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
2.	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	УК-9; ОПК-6; ОПК-10; ОПК-12; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
3.	Типовая структура комплексной системы информационной безопасности (КСИБ); методы проектирования и оценки качества КСИБ	УК-9; ОПК-6; ОПК-10; ОПК-12; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
4.	Этапы проектирования КСИБ и требования к ним	УК-9; ОПК-6; ОПК-10; ОПК-12; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету
5.	Структура политики информационной безопасности организации	УК-9; ОПК-6; ОПК-10; ОПК-12; ОПК-4.1	Задания к лабораторным работам, контрольные вопросы, вопросы к зачету

Лабораторное занятие №1 (5 ч.)

Тема **Постановка задачи комплексного обеспечения информационной безопасности автоматизированных систем (ИБ АС)**

Вопросы для обсуждения:

1. Инвентаризация АС в соответствии с Руководящими документами Гостехкомиссии при Президенте Российской Федерации (рд ГТК РФ)
2. Инфраструктура
3. Технические ресурсы
4. Программные ресурсы

5. Информационные ресурсы.

Лабораторное занятие №2 (5 ч.)

Тема Методология формирования задач защиты; интеграция средств защиты в технологическую среду

Вопросы для обсуждения:

1. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре на базе учебных лабораторий.
2. Построение моделей угроз и нарушителя.
3. Разработка и содержание аварийного плана действий в случае нарушения информационной безопасности автоматизированной системы

Лабораторное занятие №3 (5 ч.)

Тема Типовая структура КСИБ; методы проектирования и оценки качества КСИБ

Вопросы для обсуждения:

1. Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий.
2. Интеграция средств защиты информации в технологическую среду АС.
3. Требования к составу проектной и эксплуатационной документации.
4. Разработка порядка подготовки и проведения аттестации АС.

Лабораторное занятие №4 (5 ч.)

Тема Этапы проектирования КСИБ и требования к ним

Вопросы для обсуждения:

1. Разработка контрмер.
2. Экономическая оценка затрат на защиту информации (на базе учебных лабораторий).
3. Разработка эскизного проекта КСИБ.
4. Моделирование процедуры.

Лабораторное занятие №5 (4 ч.)

Тема Структура политики информационной безопасности организации (ПИБ)

Вопросы для обсуждения:

1. Выбор концепции, определяющей миссию и ключевые цели политики.
2. Определение стандартов, принципов обеспечения безопасности.
3. Перечень конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
4. Порядок работы с носителями данных.
5. Правила доступа к корпоративным документам и другим важным ресурсам.
6. Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.
7. Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств.

Задания для текущего контроля

№ раздела дисципли ны	Наименование лабораторных работ
1.	Классификация автоматизированных систем (АС) Требования по защите информации от несанкционированного доступа для АС. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре.
2.	Построение моделей угроз и нарушителя. Разработка и содержание аварийного плана действий
3.	Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий. Интеграция средств защиты информации в технологическую среду АС. Требования к составу проектной и эксплуатационной документации
4.	Разработка контрмер. Экономическая оценка затрат на защиту информации. Разработка проекта КСИБ. Моделирование процедур.
5.	Методики формирования политики информационной безопасности. Типовой перечень задач службы информационной безопасности. Организационно-технические и режимные меры.

Примерные темы самостоятельной работы

1. Инвентаризация АС в соответствии с Руководящими документами Гостехкомиссии при Президенте Российской Федерации (рд ГТК РФ)
2. Анализ угроз информационным ресурсам и обеспечивающей инфраструктуре на базе учебных лабораторий.
3. Построение моделей угроз и нарушителя.
4. Разработка и содержание аварийного плана действий в случае нарушения информационной безопасности автоматизированной системы
5. Оценка рисков информационной безопасности автоматизированной системы на базе учебных лабораторий.
6. Интеграция средств защиты информации в технологическую среду АС.
7. Требования к составу проектной и эксплуатационной документации.
8. Разработка порядка подготовки и проведения аттестации АС.
9. Экономическая оценка затрат на защиту информации
10. Выбор концепции, определяющей миссию и ключевые цели политики.
11. Определение стандартов, принципов обеспечения безопасности.
12. Определение списка конкретных действий, которые сотрудники должны совершать в процессе взаимодействия с конфиденциальными данными организации.
13. Порядок работы с носителями данных.
14. Правила доступа к корпоративным документам и другим важным ресурсам.
15. Инструкции, касающиеся реализации методов защиты и применения принятых стандартов.
16. Аварийные планы — порядок действий по реагированию и оперативному восстановлению информационных систем в случае непредвиденных обстоятельств

Примерные темы рефератов:

1. Понятие о комплексном обеспечении информационной безопасности
2. Угрозы информационной безопасности и уязвимости информационной системы
3. Изучение методов комплексного исследования объекта информатизации
4. Изучение информации циркулирующей в корпоративной информационной системе
5. Изучение построения системы защиты информации на основе нормативных актов и методических указаний
6. Информационные риски. Оценка рисков информационной безопасности
7. Построение модели угроз информационной системы
8. Виды защиты информации. Организационно-правовые основы технической защиты информации
9. Физическая защита информации
10. Изучение действующей нормативной документации объекта информатизации
11. Составление плана мероприятий по улучшению защищённости объекта информатизации
12. Разработка политики информационной безопасности
13. Исследование методов выбора рационального варианта системы защиты информации на основе экспертной информации
14. Исследование методик расчета показателя качества системы защиты информации
15. Изучение методов построения комплексной системы организационных и технических мер по защите информации
16. Изучение методов построения комплексной защиты сетевой файловой системы
17. Комплексная защита электронной почты и документооборота
18. Понятие о менеджменте информационной безопасности. Серия ГОСТ Р ИСО/МЭК 2700х
19. Изучение методов построения комплексной защиты сетевых приложений и баз данных
20. Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры
21. Изучение методов построения комплексной защиты управления информационной безопасностью
22. Изучение методики составления испытаний системы защиты информации

Примерные вопросы к экзамену.

1. Основные понятия и определения информационной безопасности. Общие цели и задачи защиты информации.
2. Принципы организации комплексной системы защиты информации. Системно-концептуальный подход к защите информации.
3. Основные требования и основные задачи защиты информации в автоматизированных системах.
4. Действующие стандарты в области информационной безопасности. Содержание и основные позиции. Документационное сопровождение комплексной информационной безопасности автоматизированных систем (КИБ АС).
5. Направления работ по созданию КИБ АС. Аспекты планирования инженерно-технического обеспечения КСЗИ.
6. Этапы работ по созданию КИБ АС. Определение и анализ объектов защиты. Базовые понятия и элементы. Формализация описания архитектуры автоматизированной системы.
7. Определение и анализ объектов защиты. Определение исходного уровня защищенности.
8. Классификация защищенности АС в соответствии с РД. Основные требования.
9. Оценка угроз ИБ. Выявление способов НСД и каналов утечки информации.
10. Объективные и субъективные факторы, воздействующие на информацию (по ГОСТ).
11. Виды угроз и основные последствия их реализации.
12. Понятие «нарушителя» и модели нарушителя. Классификации.
13. Модель угроз и принцип ее формирования. Базовая модель угроз безопасности персональных данных (ФСТЭК).
14. Модель угроз и принцип ее формирования. Методология формирования модели угроз в соответствии с рекомендациями ФСБ.
15. Методики оценки рисков. Применяемые на практике подходы.

16. Структура процесса управления рисками.
17. Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
18. Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
19. Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
20. Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
21. Планирование мероприятий КСЗИ.
22. Контроль мероприятий КИБ АС. Основные аспекты.
23. Оценка эффективности КИБ АС. Общая характеристика применяемых методов.
24. Оценка эффективности КИБ АС. Оценочные подходы.

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

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический экзамен по вопросам.

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, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

16. Структура процесса управления рисками.
17. Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
18. Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
19. Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
20. Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
21. Планирование мероприятий КСЗИ.
22. Контроль мероприятий КИБ АС. Основные аспекты.
23. Оценка эффективности КИБ АС. Общая характеристика применяемых методов.
24. Оценка эффективности КИБ АС. Оценочные подходы.

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

Критерии оценивания:

Критерием оценивания является выполнение самостоятельных заданий, контрольных и лабораторных работ.

Самостоятельные задания, контрольные и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

- своевременное выполнение работы;
- полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический экзамен по вопросам.

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, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

Составитель _____

Мазур И. К.