


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.25 Защита информации от утечки по техническим каналам

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация
бакалавр

Форма обучения
очная

Южно-Сахалинск
2024 г.

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

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-4.	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1 - Знает основные физические законы, физическую сущность явлений и процессов; ОПК-4.2 - Умеет использовать математические модели физических явлений и процессов; ОПК-4.3 - Владеет практическими навыками решения типовых прикладных физических задач.
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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 - Знает основные понятия криптографии и криптографические методы защиты информации; ОПК-9.2 - Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации; ОПК-9.3 - Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности.
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных,	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной

	программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы
ОПК-4.4	Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации; ОПК-4.4.2 - Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, а также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы; ОПК-4.4.3 - Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств.

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. Введение в техническую защиту информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
2.	Тема 2. Технические каналы утечки информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3,	Устный опрос по теме лекции Выполнение

		ОПК-4.4	практического задания Тестирование
3.	Тема 3. Демаскирующие признаки объектов	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
4.	Тема 4. Средства выявления каналов утечки информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
5.	Тема 5. Защита информации от утечки по техническим каналам	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
6.	Тема 6. Методы и средства инженерной защиты информации и технической охраны объектов	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
7.	Тема 7. Аттестация объектов информатизации по требованиям безопасности информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
8.	Тема 8. Мероприятия по выявлению и оценке свойств каналов утечки информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование
9.	Тема 9. Технический контроль эффективности мер защиты информации	ОПК-4, ОПК-6, ОПК-9, ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания Тестирование

3. Оценочные средства

Форма контроля для очной формы обучения – **экзамены**

Примеры заданий для текущего контроля и промежуточных заданий по различным темам:

Примерный перечень тестовых заданий

Примерный перечень тестовых заданий

Примерный перечень тестовых заданий

1. Устройство, используемое для проведения измерений ТС на побочные электромагнитные излучения (ПЭМИ)?

- 1) Анализатор спектра
- 2) Шумомер
- 3) Низкочастотный анализатор
- 4) Все варианты

2. Устройства, подлежащие исследованию на побочные электромагнитные излучения и наводки (ПЭМИН)?

- 1) Накопители на жестких дисках
- 2) Принтер
- 3) Клавиатура
- 4) Все варианты

3. Что изучается при определении значений сигналов АЭП речевого диапазона частот в отходящей от ВТСС линии, выходящей за пределы КЗ?

- 1) Телефония
- 2) Система сигнализации
- 3) Цепи электропитания
- 4) Все перечисленное

4. Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации обрабатываемой в технических средствах?
- 1) Акустоэлектрический
 - 2) Параметрический
 - 3) Электрический
 - 4) Электромагнитный
5. Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации, обрабатываемой в технических средствах?
- 1) Акустоэлектрический
 - 2) Параметрический
 - 3) Электрический
 - 4) Электромагнитный
6. Как называется устройство про помощи которого выполняется измерение ограждающих конструкций при проведении виброакустических измерений разборчивости речи?
- 1) Акселерометр
 - 2) Микрофон
 - 3) Акустический излучатель
 - 4) Лучевая трубка
7. Каким каналом утечки речевой информации является дверь в выделенное помещение?
- 1) Параметрический
 - 2) Видовой
 - 3) Акустический
 - 4) Оптико-электронный
8. При превышении какого значения разборчивости речи можно говорить о достижении уровня непреднамеренного прослушивания?
- 1) 10%
 - 2) 20%
 - 3) 30%
 - 4) 40%
9. Какая из среднегеометрических частот не входит в стандартные октавные полосы?
- 1) 250 Гц
 - 2) 1 кГц
 - 3) 500 Гц
 - 4) 750 Гц
10. При передаче информации по каналам связи, какой канал утечки информации возникает в результате возникновения вокруг высокочастотного кабеля электромагнитного поля?
- 1) Электромагнитный канал
 - 2) Индукционный канал
 - 3) Паразитные связи
 - 4) Электрический канал

Примерные вопросы к экзамену

1. Понятие «информация». Виды информации. Концептуальные основы защиты информации.
2. Понятие «информация». Виды информации. Задача защиты информации.
3. Технические каналы утечки информации. Основные и вспомогательные технические средства и системы. Понятие контролируемой и опасных зон. Принцип перехват информации с помощью технических средств разведки.
4. Технические каналы утечки информации, обрабатываемой ОТСС. Пояснить принципы перехвата информации и привести примеры.

5. Технические каналы утечки информации, при передачи ее по каналам связи. Понятие канала связи. Пояснить принципы перехвата информации и привести примеры.
6. Технические каналы утечки речевой информации. Пояснить принципы перехвата информации и привести примеры.
7. Технические каналы утечки видовой информации. Пояснить принципы перехвата информации и привести примеры.
8. Контроль и прослушивание телефонных каналов связи.
9. Утечка информации за счёт паразитных связей.
10. Акустический и виброакустический каналы утечки информации.
11. Акустический канал утечки информации. Виды направленных микрофонов.
12. Демаскирующие признаки. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок
13. Демаскирующие признаки. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».
14. Средства выявления каналов утечки информации. Состав автоматизированных программно-аппаратных комплексов. Пояснить назначение каждого из компонентов.
15. Средства выявления каналов утечки информации. Методы автоматизации программно-аппаратных комплексов.
16. Средства выявления каналов утечки информации. Многофункциональные комплексы выявления каналов утечки информации. Описание и основные характеристики.
17. Средства выявления каналов утечки информации. Многофункциональные комплексы выявления каналов утечки информации. Использование приборов для выявления каналов утечки информации в радиочастотном диапазоне.
18. Средства выявления каналов утечки информации. Многофункциональные комплексы выявления каналов утечки информации. Использование прибора для выявления каналов утечки информации по проводным линиям различного назначения, в инфракрасном диапазоне, из-за низкочастотных магнитных полей.
19. Средства выявления каналов утечки информации. Особенности выявления каналов утечки информации с помощью многофункциональных комплексов. Схемы и основные принципы.
20. Комплексы измерения характеристик акустических сигналов «Спрут», «Шепот». Состав и принцип организации измерений.
21. Локаторы нелинейности. Принцип действия. Повышение достоверности обнаружения полупроводниковых устройств.
22. Скрытие и защита информации от утечки по техническим каналам. Концепция и методы инженерно-технической защиты информации.
23. Скрытие и защита информации от утечки по техническим каналам. Экранирование электромагнитных волн. Экранирование устройств и помещений.
24. Скрытие и защита информации от утечки по техническим каналам. Заземление технических средств и фильтрация информационных сигналов.
25. Скрытие и защита информации от утечки по техническим каналам. Пространственное и линейное зашумление.
26. Скрытие и защита информации от утечки по техническим каналам. Способы предотвращения утечки информации через ПЭМИН ПК.
27. Скрытие и защита информации от утечки по техническим каналам. Устройства контроля и защиты слаботочных и сетевых линий. Схемы контроля.
28. Скрытие и защита информации от утечки по техническим каналам. Устройства контроля и защиты слаботочных и сетевых линий. Примеры устройств.
29. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.

30. Защита конфиденциальной информации в автоматизированных системах.
31. Методы и средства инженерной защиты и технической охраны объектов. Общие принципы обеспечения безопасности объектов.
32. Методы и средства инженерной защиты и технической охраны объектов. Состав системы обеспечения безопасности объектов. Состав каждой из систем с примерами.
33. Методы и средства инженерной защиты и технической охраны объектов. Системы периметровой охраны.
34. Аттестация объектов информатизации по требованиям безопасности информации. Основные положения Приказа ФСТЭК «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».
35. Мероприятия по выявлению и оценке свойств каналов утечки информации. Общие принципы специальных проверок, специальных обследований и специальные исследований.
36. Мероприятия по выявлению и оценке свойств каналов утечки информации. Специальные исследования акустических и виброакустических каналов.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,5	1	8	16
Подготовка к занятию, выполнение домашнего задания	0,5	1	8	16
выполнение практических заданий по темам	3	5	27	45
Промежуточная аттестация (зачет)	10	23	10	23
Итого за семестр			53	100

Система оценивания планируемых результатов обучения

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.

Составитель


(подпись)

Филиппова
преподаватель
информатики

Г.В., старший
кафедры

«12 » марта 2024 г