


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

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы

 Буинцев Д.Н.
«_24_» сентября 2024 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

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

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Защита информации от утечки по техническим каналам составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

Г.В. Филиппова, старший преподаватель кафедры информатики



Рабочая программа дисциплины Защита информации от утечки по техническим каналам утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности
заведующего кафедрой

Г.С. Осипов



1. Цель и задачи дисциплины

Цель дисциплины

Целями освоения дисциплины «*Защита информации от утечки по техническим каналам*» являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по основам защиты информации от утечки по техническим каналам достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. Формирование комплекса базовых навыков по оценке защищенности информации от утечки по техническим каналам; по установке, настройке и эксплуатации аппаратно-программных комплексов для выявления технических каналов утечки информации; по поиску оптимальных решений при проектировании системы защиты информации; по настройке систем управления информационной безопасностью объектов
2. Приобретение навыков применения физических законов и моделей для оценки защищенности информации от утечки по техническим каналам. а также поиску оптимальных решений при проектировании системы защиты информации объекта информатизации.
3. Приобретение навыков использования средства технической защиты информации при установке, настройке и эксплуатации аппаратно-программных комплексов для выявления технических каналов утечки информации и настройке систем управления информационной безопасностью объектов.

Место дисциплины в структуре образовательной программы

Дисциплина «*Защита информации от утечки по техническим каналам*» относится к обязательной части Блока 1 Дисциплины (модули) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знаниях, полученных в результате изучения таких дисциплин как Основы информационной безопасности, Физика, Разработка и эксплуатация защищенных автоматизированных систем, Методы и средства криптографической защиты информации, Основы управления информационной безопасностью

Изучение данной дисциплины проходит параллельно с изучением такой дисциплины, как «Программно-аппаратные средства защиты информации» и базируется на знаниях, полученных в результате изучения этой дисциплины.

Постреквизиты дисциплины:

Знания и умения, полученные студентами при изучении дисциплины, применяются ими во время учебной и преддипломной практик и в их профессиональной деятельности.

2. Формируемые компетенции и индикаторы их достижения по дисциплине

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

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	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной 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.

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единиц (288 академических часов).

Вид работы	Трудоемкость, акад. часов		
	7 семестр	8 семестр	всего
Общая трудоемкость	144	144	288
Контактная работа:	52	52	144
Лекции	22	22	44
Лабораторные работы (Лаб)	24	24	48
Контактная работа в период теоретического обучения (КонтТО) (<i>Проведение текущих консультаций и индивидуальная работа со студентами</i>)	5	5	10
	1	1	2
Промежуточная аттестация (экзамен)	35	35	70
Самостоятельная работа:	57	57	114
- <i>самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий);</i>	27	24	51
- <i>подготовка к лабораторным занятиям;</i>	30	25	55
<i>подготовка к экзамену</i>		8	8

3.2. Распределение видов работы и их трудоемкости по разделам дисциплины

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
		контактная			Самостоятельная работа	
		Лекции	Практические занятия	Лабораторные занятия		
7 семестр						
1.	Тема 1.Введение в техническую защиту информации	2			4	Устный опрос по теме лекции Тестирование
2.	Тема 2.Технические каналы утечки информации	4			10	Устный опрос по теме лекции Выполнение практического задания Тестирование
3.	Тема 3. Демаскирующие признаки объектов	2			10	Устный опрос по теме лекции Выполнение практического задания Тестирование
4.	Тема 4. Средства выявления каналов утечки информации	6		20	18	Устный опрос по теме лекции Выполнение практического задания Тестирование
5.	Тема 5. Защита информации от утечки по техническим каналам	8		4	15	Устный опрос по теме лекции Выполнение практического задания Тестирование
	Итого за 7 семестр	22		24	57	
8 семестр						
6.	Тема 6. Методы и средства инженерной защиты информации и технической охраны объектов	10		18	28	Устный опрос по теме лекции Выполнение практического задания Тестирование
7.	Тема 7. Аттестация объектов информатизации по требованиям безопасности информации	4		2	10	Устный опрос по теме лекции Выполнение практического задания Тестирование
8.	Тема 8. Мероприятия по выявлению и оценке свойств каналов утечки информации	4		2	10	Устный опрос по теме лекции Выполнение практического задания Тестирование
9.	Тема 9. Технический контроль эффективности мер защиты информации	4		2	9	Устный опрос по теме лекции Выполнение практического задания Тестирование
	итого:	22		24	57	

3.3. Содержание разделов дисциплины

Тема 1. Введение в техническую защиту информации

Концептуальные основы защиты информации (Стратегия и Доктрина информационной безопасности). Нормативные документы в области ТЗИ. Задача защиты информации.

Тема 2. Технические каналы утечки информации

Каналы утечки информации, обрабатываемой ОТСС. Каналы утечки информации при передаче ее по каналам связи. Каналы утечки информации за счет паразитных связей. Каналы утечки речевой информации

Тема 3. Демаскирующие признаки объектов

Демаскирующие признаки объектов в видимом и инфракрасном диапазоне электромагнитного спектра. Демаскирующие признаки радиоэлектронных средств. Демаскирующие признаки закладных устройств.

Тема 4. Средства выявления каналов утечки информации

Методы автоматизации обнаружения гармонических составляющих тестового сигнала, измерения уровней сигналов, измерения наводок в сети питания, линиях и коммуникациях. Индикаторы электромагнитного поля. Сканирующие радиоприемники, анализаторы спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. Комплексы для сканирования радиодиапазона. Комплексы измерения побочных электромагнитных излучений и наводок. Локаторы нелинейности. Комплексы измерения характеристик акустических сигналов. Металлодетекторы, портативные рентгенотелевизионные установки, Специальный досмотровый комплект эндоскопов.

Тема 5. Защита информации от утечки по техническим каналам

Скрытие и защита информации от утечки по техническим каналам. Концепция и методы инженерно-технической защиты информации. Пассивное сккрытие: экранирование электромагнитных волн, заземление технических средств и подавление информационных сигналов в цепях заземления, фильтрация информационных сигналов. Принцип действия типовых устройств. Способы предотвращения утечки информации через ПЭМИН ПК. Контроль и защита слаботочных и сетевых линий. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Защита конфиденциальной информации в автоматизированных системах: программный комплекс для защиты информации от несанкционированного доступа, программно-аппаратный комплекс «Соболь», применение смарт-карт и USB-ключей, технология Proximity, устройства быстрого уничтожения информации на жестких магнитных носителях.

Тема 6. Методы и средства инженерной защиты информации и технической охраны объектов

Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов Система охранной и пожарной сигнализации. Система контроля и управления доступом. Телевизионные системы (видеонаблюдение). Периметровая охрана: тепловизионные системы Инфракрасные системы, ёмкостные системы, радиолучевые системы, радиоволновые системы, электрошоковые системы.

Тема 7. Аттестация объектов информатизации по требованиям безопасности информации

Нормативные документы по аттестации объектов информатизации. Стороны, участвующие в аттестации. Приказ ФСТЭК России № 77. Организация работ по аттестации объектов информатизации.

Тема 8. Мероприятия по выявлению и оценке свойств каналов утечки информации

Перечень работ по выявлению каналов утечки информации предусматривает. Специальные проверки. Специальные обследования. Специальные исследования. Специальные исследования акустических и виброакустических каналов. Специальные исследования технических средств и систем на возможность утечки информации за счет ПЭМИН. Специальные исследования акустоэлектрических преобразований.

Тема 9. Технический контроль эффективности мер защиты информации

Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте вычислительной техники от утечки по каналу ПЭМИН. Методы испытаний персональных компьютеров. Методы контроля ПЭМИН генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Порядок проведения контроля защищенности автоматизированных систем от несанкционированного доступа.

Темы и планы лабораторных занятий

Лабораторное занятие №1 -10 (20 ч.)

Тема. Средства выявления каналов утечки информации

Вопросы для обсуждения:

1. Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.
2. Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.
3. Оценка защищенности помещения от утечки информации по акустическому и виброакустическому каналу.
4. Нелинейная локация.

Лабораторное занятие №11-12 (4 ч.)

Тема. Защита информации от утечки по техническим каналам

Вопросы для обсуждения:

1. Принципы построения и работы пассивных фильтров на основе сосредоточенных компонентов.
2. Разработка систем защиты от утечек за счет побочных электромагнитных излучений и наводок

Лабораторное занятие №13-21 (18 ч)

Тема. Методы и средства инженерной защиты информации и технической охраны объектов.

Вопросы для обсуждения:

1. Разработка пространственной модели объекта информационной защиты. Описание угроз утечки информации по техническим каналам.
2. Разработка системы видеонаблюдения объекта.
3. Знакомство с принципами функционирования и эксплуатации пожарно-охранной сигнализации
4. Сборка пожарно-охранных шлейфов, конфигурирование, работа с кодовой панелью.
5. Изучение функциональных возможностей турникета.
6. Изучение функциональных возможностей биометрического считывателя-контроллера.
7. Видеорегистратор, основные настройки и функции

Лабораторное занятие №22 (2 ч)

Тема. Аттестация объектов информатизации по требованиям безопасности информации

Вопросы для обсуждения:

1. Организационные мероприятия по подготовке и проведению аттестации объектов информатизации по требованиям безопасности информации.,

Лабораторное занятие №23 (2 ч)

Тема. Мероприятия по выявлению и оценке свойств каналов утечки информации

Вопросы для обсуждения:

1. Методическое обеспечение проведения аттестации объектов информатизации по требованиям безопасности. Расчёт опасных зон I и II.

Лабораторное занятие №24 (2 ч)

Тема. «Технический контроль эффективности мер защиты информации»

Вопросы для обсуждения:

1. Порядок проведения контроля защищенности информации на объекте вычислительной техники от утечки по каналу ПЭМИН. Методы испытаний персональных компьютеров. Методы контроля ПЭМИН генераторов технических средств

4. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

5. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Тема 1. Введение в техническую защиту информации	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
2.	Тема 2. Технические каналы утечки информации	Лекция 1 Лекция 2	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
3.	Тема 3. Демаскирующие признаки объектов	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
4.	Тема 4. Средства выявления каналов утечки информации	Лекция 1 Лекция 2 Лекция 3	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2 Лабораторное занятие 3 Лабораторное занятие 4 Лабораторное занятие 5 Лабораторное занятие 6 Лабораторное занятие 7 Лабораторное занятие 8 Лабораторное занятие 9 Лабораторное занятие 10	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
5.	Тема 5. Защита информации от утечки по техническим каналам	Лекция 1 Лекция 2 Лекция 3	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
6.	Тема 6. Методы и средства инженерной защиты информации и технической охраны объектов	Лекция 1 Лекция 2 Лекция 3 Лекция 4 Лекция 5	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие 1 Лабораторное занятие 2 Лабораторное занятие 3 Лабораторное занятие 4 Лабораторное занятие 5 Лабораторное занятие 6 Лабораторное занятие 7 Лабораторное занятие 8 Лабораторное занятие 9	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.

7.	Тема 7. Аттестация объектов информатизации по требованиям безопасности информации	Лекция 1	Традиционная лекция в ауд. с мультимедиа проектором
		Лекция 2	
		Лабораторное занятие	Лабораторное занятие в компьютерном классе
8.	Тема 8. Мероприятия по выявлению и оценке свойств каналов утечки информации	Самостоятельная работа	Повторение материала, подготовка домашнего задания.
		Лекция 1	Традиционная лекция в ауд. с мультимедиа проектором
		Лекция 2	
9.	Тема 9. Технический контроль эффективности мер защиты информации	Лабораторное занятие	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
		Лекция 1	Традиционная лекция в ауд. с мультимедиа проектором
		Лекция 2	
		Лабораторное занятие	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.

6. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Форма контроля для очной формы обучения – *экзамен*,

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 передачи 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 шумление.
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.

7. 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.

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

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

а) основная литература:

1. Киренберг, А. Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/135100.html>
2. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/101929.html>
3. Вайц, Е. В. Разработка комплекса организационных и технических мероприятий по защите информации от утечки по техническим каналам на объекте информатизации : методические указания к выполнению курсовой работы / Е. В. Вайц, Ю. В. Грачёва. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2016. — 20 с. — ISBN 978-5-7038-4556-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/134982.html>

8.2.Дополнительная литература

1. Технические средства защиты информации: 1. Учебное пособие / А. А. Титов - 2010. 194 с. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/653>.
2. Технические средства охраны: учеб. пособие: конспект лекций / А.В. Полшков, А.С.Шабуров. - Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2013 - 249 с. [Электронный ресурс]:Режим доступа: <https://reader.lanbook.com/book/160595#2>.
3. Защита информации с использованием смарт-карт и электронных брелоков / Л. К.Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 29 экз.).

8.3.Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. Дистрибутивы Ubuntu GNU/Linux, Debian GNU/Linux
13. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;
14. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
15. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

8.4.Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)

12. Издание о высоких технологиях (www.cnews.ru)
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

9. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;

- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

10. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).