Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ФИЗИЧЕСКИЕ ОСНОВЫ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
2	2	72	8	22	0		42	0	З
Итого	2	72	8	22	0	2	42	0	

АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ связанными со знаниями физических основ технических средств обеспечения информационной безопасности.

Задачи дисциплины:

- ознакомление с физическими моделями и принципами работы технических устройств на физической ступени абстракции;
- обучение решению физических задач, использованию современных информационных технологий с целью поиска, приобретения и переработки информации физического содержания и оценки ее достоверности;
- совершенствование навыков наблюдения, планирования, выполнения и обработки результатов измерений физического эксперимента;
- обучение основам классической и релятивистской механики, молекулярной физики и термодинамики, электричества и магнетизма, оптики, квантовой физики и физики твердого тела связанной с физическими основами технических средств обеспечения информационной безопасности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Физические основы технических каналов утечки информации» является теоретическая и практическая подготовка «специалистов» к деятельности, связанной с физическими основами технических средств обеспечения информационной безопасности.

Задачи дисциплины ознакомить с физическими моделями и принципами работы технических устройств на физической ступени абстракции; обучить решению физических задач, использованию современных информационных технологий с целью поиска, приобретения и переработки информации физического содержания и оценки ее достоверности; совершенствование навыков наблюдения, планирования, выполнения и обработки результатов измерений физического эксперимента; ознакомить с основам классической и релятивистской механики, молекулярной физики и термодинамики, электричества и магнетизма, оптики, квантовой физики и физики твердого тела связанной с физическими основами технических средств обеспечения информационной безопасности.

В результате обучения студенты должны ознакомиться с:

- физическими моделями и принципами работы технических устройств на физической ступени абстракции;
- физическими задачами (решение), использованием современных информационных технологий с целью поиска, приобретения и переработки информации физического содержания и оценки ее достоверности;
- навыков наблюдения, планирования, выполнения и обработки результатов измерений физического эксперимента;
- основам классической и релятивистской механики, молекулярной физики и термодинамики, электричества и магнетизма, оптики, квантовой физики и физики твердого тела связанной с физическими основами технических средств обеспечения информационной безопасности.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

- знать программы (физика, математика) общеобразовательной школы и высших учебных заведений;
- уметь использовать математический (теории вероятностей и дискретной математики) аппарат и решать физические задачи;
- владеть основами общей физики, высшей математики, электротехники.

В результате изучения дисциплины студент должен:

знать:

- физические основы функционирования технических средств и систем обработки и передачи информации;
- физические основы образования технических каналов утечки информации;

уметь:

- использовать физические эффекты для обеспечения технической защиты информации;
- применять на практике методы физики при исследовании технических каналов утечки информации;

владеть:

- методами проведения физического эксперимента при выявлении технических каналов утечки информации.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности	Средства и технологии обеспечения безопасности значимых объектов критической	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки

(СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	информационной инфраструктуры	информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям

			электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного

			обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации

			работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения

			сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки

			протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	2 Семестр						
1	Физические основы технических систем	1-8	4/12/0		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1
2	Физические основы	9-15	4/10/0		25	КИ-15	З-ПК-

	защиты информации от технических средств разведки						1, У-ПК-1, В-ПК-1
	Итого за 2 Семестр		8/22/0		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	8	22	0
1-8	**Физические основы технических систем**	4	12	0
1 - 2	**Тема 1. Введение в курс. Физические основы образования каналов утечки информации.** Использование физических эффектов в технических системах. Общие физические основы технических систем. Основы теории электромагнитного поля. Основы прикладной акустики. Основы прикладной оптики. Основы процессов модуляции и возникновения ПВЧГ. Закономерность проявления физических эффектов в ТС и их применение. Закономерность технической реализации физических эффектов.	Всего аудиторных часов		
		1	3	0
		Онлайн		
		0	0	0
3 - 4	**Тема 2. Технические каналы утечки информации. Физические основы образования каналов утечки информации** Классификация технических каналов утечки информации. Роль физических эффектов в образовании каналов утечки	Всего аудиторных часов		
		1	3	0
		Онлайн		
		0	0	0

	информации. Классификация акустических каналов утечки информации. Прямой акустический канал. Используемые технические средства. Акустовибрационный канал. Используемые технические средства. Акустоэлектрический канал утечки информации. Используемые технические средства. Акусторадиоэлектронный канал. Используемые технические средства. Акустопараметрический канал. Используемые технические средства. Акустооптический канал. Используемые технические средства.			
5 - 6	**Тема 3. Физические основы электрических каналов утечки информации. Физические основы оптических каналов утечки информации.** Классификация электрических каналов утечки информации. Канал утечки информации по телефонной линии. Контактные способы подключения. Бесконтактные способы подключения. Методы выявления утечки информации по телефонной линии. Канал утечки информации по цепям электропитания. Канал утечки информации по цепям заземления. Классификация оптических каналов утечки информации. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконно-оптический канал.	Всего аудиторных часов		
		1	3	0
		Онлайн		
		0	0	0
7 - 8	**Тема 4. Электромагнитные излучения. Электромагнитные излучения в образовании каналов утечки информации. Электромагнитные явления и эффекты в создании каналов утечки информации.** Классификация электромагнитных каналов утечки информации. Перехват сигналов связных радиостанций. Перехват радиотелефонных сигналов. Радиомаяки. Радиозакладки. Источники электромагнитных излучений и наводок. Использование эффектов паразитных связей. Использование эффектов электромагнитных наводок. Использование эффектов для образования случайных антенн. Структура схемы образования комплексных каналов утечки информации.	Всего аудиторных часов		
		1	3	0
		Онлайн		
		0	0	0
9-15	**Физические основы защиты информации от технических средств разведки**	4	10	0
9 - 10	**Тема 5. Методы и средства защиты речевой информации от акустической речевой разведки** Методы и средства защиты речевой информации от акустической речевой разведки	Всего аудиторных часов		
		1	4	0
		Онлайн		
		0	0	0
11 - 12	**Тема 6. Методы и средства защиты информации в линиях связи, электропитания и заземления** Методы и средства защиты информации в линиях связи, электропитания и заземления	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0
13 - 14	**Тема 7. Методы и средства защиты информации от фотографической, телевизи-онной и оптико-электронной разведок** Методы и средства защиты информации от фотографической, телевизи-онной и оптико-электронной разведок	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0

15 - 16	**Тема 8. Методы и средства защиты информации от радиотехнической разведки** Методы и средства защиты информации от радиотехнической разведки	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	2 Семестр
	Физические основы образования каналов утечки информации. Физические основы образования каналов утечки информации. Использование физических эффектов в технических системах. Общие физические основы технических систем. Основы теории электромагнитного поля. Основы прикладной акустики. Основы прикладной оптики. Основы процессов модуляции и возникновения ПВЧГ. Закономерность проявления физических эффектов в ТС и их применение. Закономерность технической реализации физических эффектов. Решение задач.
	Технические каналы утечки информации. Физические основы акустических каналов утечки информации. Классификация технических каналов утечки информации. Роль физических эффектов в образовании каналов утечки информации. Классификация акустических каналов утечки информации. Прямой акустический канал. Используемые технические средства. Акустовибрационный канал. Используемые технические средства. Акустоэлектрический канал утечки информации. Используемые технические средства. Акусторадиоэлектронный канал. Используемые технические средства. Акустопараметрический канал. Используемые технические средства. Акустооптический канал. Используемые технические средства. Решение задач.
	Физические основы электрических каналов утечки

	информации. Физические основы оптических каналов утечки информации. Физические основы электрических каналов утечки информации. Физические основы оптических каналов утечки информации. Классификация электрических каналов утечки информации. Канал утечки информации по телефонной линии. Контактные способы подключения. Бесконтактные способы подключения. Методы выявления утечки информации по телефонной линии. Канал утечки информации по цепям электропитания. Канал утечки информации по цепям заземления. Классификация оптических каналов утечки информации. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконно-оптический канал. Решение задач.
	Электромагнитные излучения. Электромагнитные излучения в образовании каналов утечки информации. Электромагнитные явления и эффекты в создании каналов утечки информации. Классификация электромагнитных каналов утечки информации. Перехват сигналов связных радиостанций. Перехват радиотелефонных сигналов. Радиомаяки. Радиозакладки. Источники электромагнитных излучений и наводок. Использование эффектов паразитных связей. Использование эффектов электромагнитных наводок. Использование эффектов для образования случайных антенн. Структура схемы образования комплексных каналов утечки информации. Решение задач.
	Физические основы образования технических каналов утечки информации. Взаимосвязь между параметрами технической системы и параметрами физического эффекта. Уменьшение числа и значений параметров побочных результатов воздействия. Уменьшение влияния окружающей среды на техническую реализацию физических эффектов и условия их проявления. Некоторые особенности построения физических систем. Место физических систем. База данных по физическим эффектам. Решение задач.
	Технические каналы утечки информации. Физические основы акустических каналов утечки информации. Прямой акустический канал. Средства противодействия перехвату информации по прямому акустическому каналу. Акустовибрационный канал. Средства противодействия перехвату информации по акустовибрационному каналу. Акустоэлектрический канал утечки информации. Средства противодействия перехвату информации по акустоэлектрическому каналу. Акусторадиоэлектронный канал утечки информации. Технические средства обнаружения радиомикрофонов. Технические средства подавления радиомикрофонов. Акустопараметрический канал. Технические средства обнаружения утечки

	информации по параметрическому каналу. Технические средства подавления утечки информации по параметрическому каналу. Акустооптический канал. Средства противодействия перехвату информации по акустооптическому каналу. Технические средства обнаружения утечки информации по акустооптическому каналу. Решение задач.
	Физические основы электрических каналов утечки информации. Физические основы оптических каналов утечки информации. Канал утечки информации по телефонной линии. Способы перехвата речевой информации из телефонной линии. Предотвращение утечки информации по телефонной линии. Предотвращение утечки информации по цепям электропитания. Средства контроля цепей электропитания для предотвращения утечки информации. Канал утечки информации по цепям заземления. Предотвращение утечки информации по цепям заземления. Средства контроля цепей заземления для предотвращения утечки информации. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконно-оптический канал. Системы обнаружения оптических устройств. Средства противодействия утечке информации по оптическим каналам. Решение задач.
	Электромагнитные излучения. Электромагнитные излучения в образовании каналов утечки информации. Электромагнитные явления и эффекты в создании каналов утечки информации. Перехват сигналов связных радиостанций и радиотелефонных сигналов. Радиомаяки. Радиозакладки. Методы и средства предотвращения утечки информации по радиотехническим каналам. Методы и средства контроля утечки информации по радиоканалам. Методы защиты информации от утечки через ПЭМИН. Методы пассивной защиты. Методы активной защиты. Методы и средства контроля побочных электромагнитных излучений и наводок. Решение задач.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по атомной энергетике и обеспечение требованиям кибербезопасности. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических занятиях

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-1	З-ПК-1	З, КИ-8, КИ-15
	В-ПК-1	З, КИ-8, КИ-15
	У-ПК-1	З, КИ-8, КИ-15
ПК-4	З-ПК-4	З
	У-ПК-4	З
	В-ПК-4	З

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает
75-84		C	

70-74		D	материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Москва: НИЯУ МИФИ, 2015

2. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

3. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

4. 004 Т61 Инженерно-техническая защита информации : учеб. пособие для вузов, А. А. Торокин, М.: Гелиос АРВ, 2005

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 621.39 Б 90 Выявление специальных технических средств несанкционированного получения информации : , Москва: Горячая линия - Телеком, 2019

2. 004 Д84 Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2015

3. 004 К65 Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

4. 534 П30 Элементы физики и техники инфраультравизуализации : учебное пособие для магистрантов, Москва: Academia, 2014

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. портал по безопасности информационной инфраструктуры (http://www.void.ru)

2. Сервер компании НИП «Информзащита» (http://www.infosec.ru)

3. Информационный бюллетень «Jet Info» с тематическим разделом по безопасности значимых объектов критич (http://www.jetinfo.ru)

4. Проектирование и дизайн - ЭМИ и защита помещений по стандартам ТЕМПЕСТ (1. www.usace.army.mill/inet/usace-docs/eng-pamphlets/ep1110-3-2/toc.htm)

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Лабораторные работы не выполняются.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических и семинарских занятиях.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия по физическим основам технических каналов утечки информации, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения

сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы в данном курсе не предусмотрены.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических и семинарских занятиях.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную (основную) и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимания следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций.

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему. На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен/зачет.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Гавдан Григорий Петрович

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):
Горбатов В.С.