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

ИНСТИТУТ ЯДЕРНОЙ ФИЗИКИ И ТЕХНОЛОГИЙ

КАФЕДРА ТЕОРЕТИЧЕСКОЙ И ЭКСПЕРИМЕНТАЛЬНОЙ ФИЗИКИ ЯДЕРНЫХ РЕАКТОРОВ

ОДОБРЕНО
УМС ИФТЭБ Протокол №545-2/1 от 28.08.2024 г.
УМС ИИКС Протокол №8/1/2025 от 25.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 10.03.01 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**
5	3-4	108-144	32	0	16		24-42	0	Э
Итого	3-4	108-144	32	0	16	0	24-42	0	

АННОТАЦИЯ

Дисциплина обеспечивает приобретение знаний и умений в соответствии с образовательным стандартом, содействует формированию научного мировоззрения и системного мышления; посвящена изучению основных разделов физики, участвующих в процессе переноса информации с помощью технических средств и методам противодействия созданию каналов утечки.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины состоит в подготовке разработчика технических средств защиты информации. В данной дисциплине рассматриваются технические средства различных видов, предназначенные для добывания информации в различных физических полях, а также физические принципы, лежащие в основе существования технических каналов утечки информации.

Данная дисциплина участвует в формировании следующих профессиональных навыков :

• способностью применять нормативные правовые акты в профессиональной деятельности;

• способностью к освоению новых образцов программных, технических средств и информационных технологий;

• способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;

• способностью участвовать в проектировании средств защиты информации автоматизированной системы;

• способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

• способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем;

• способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;

• способностью проводить инструментальный мониторинг защищенности автоматизированных систем и выявлять каналы утечки информации.

Основные задачи дисциплины – дать основы:

• технических средств добывания информации;

• назначение и функции видов разведки;

• принципов построения технических средств разведки;

• принципов защиты конфиденциальной информации техническими средствами.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

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

- знать основные понятия теории информации, математической логики, дискретной математики и информатики, теоретических основ компьютерной безопасности;

- уметь использовать математический аппарат теории вероятностей и дискретной математики;

- владеть основами программирования.

Дисциплины, предшествующие освоению данной дисциплины:

Физические основы защиты информации

Инженерная графика

Электротехника

Электроника и схемотехника

Основы информационной безопасности

Электрорадиоизмерения

Теоретические дисциплины, для которых освоение данной дисциплины необходимо как предшествующее:

Информационная безопасность автоматизированных систем

Аттестация объектов информатизации по требованиям безопасности информации

Программно-аппаратные средства защиты информации

Управление информационной безопасностью

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-2 [1] – Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-ОПК-2 [1] – знать программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач У-ОПК-2 [1] – уметь применять программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач В-ОПК-2 [1] – владеть принципами работы программных средств системного и прикладного назначения, информационно-коммуникационных технологий для решения профессиональных задач
ОПК-4 [1] – Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	З-ОПК-4 [1] – знать основные черты современной естественнонаучной картины мира и физические основы функционирования средств защиты информации У-ОПК-4 [1] – уметь объяснять физические принципы функционирования средств защиты информации В-ОПК-4 [1] – владеть основными принципами функционирования средств защиты информации
ОПК-6 [1] – Способен при решении профессиональных задач организовывать защиту	З-ОПК-6 [1] – знать основные положения нормативных документов по организации защиты информации ограниченного доступа

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	У-ОПК-6 [1] – уметь организовать 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 В-ОПК-6 [1] – владеть принципами организации защиты информации ограниченного доступа

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**
эксплуатационный			
эксплуатация технических и программно-аппаратных средств защиты информации	программно-аппаратные средства защиты информации	ПК-1 [1] - способен устанавливать, настраивать и проводить техническое обслуживание средств защиты информации *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - знать требования к проведению технического обслуживания средств защиты информации ; У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации; В-ПК-1[1] - владеть навыками проведения технического обслуживания средств защиты информации
Решение информационно-аналитических задач в сфере профессиональной деятельности с использованием специальных ИАС	Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга	ПК-1 [1] - способен устанавливать, настраивать и проводить техническое обслуживание средств защиты информации *Основание:* Профессиональный стандарт: 06.033	З-ПК-1[1] - знать требования к проведению технического обслуживания средств защиты информации ; У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации; В-ПК-1[1] - владеть

			навыками проведения технического обслуживания средств защиты информации
организационно-управленческий			
организация работы по эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределённых информационных систем	системы защиты информации, программно-аппаратные комплексы и распределённые информационные системы	ПК-4 [1] - способен разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации *Основание:* Профессиональный стандарт: 06.032	З-ПК-4[1] - знать методы построения системы управления безопасностью информации ; У-ПК-4[1] - уметь разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации; В-ПК-4[1] - владеть принципами построения системы управления безопасностью информации
Организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ; организация управления информационной безопасностью; организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России; организация и выполнение работ по созданию, монтажу,	Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга	ПК-4 [1] - способен разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации *Основание:* Профессиональный стандарт: 06.033	З-ПК-4[1] - знать методы построения системы управления безопасностью информации ; У-ПК-4[1] - уметь разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации; В-ПК-4[1] - владеть принципами построения системы управления безопасностью информации

наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности; разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; управление процессами сбора и обработки информации об операциях, подлежащих контролю в соответствии с законодательством РФ; разработка нормативных документов, относящихся к процессам финансового мониторинга.			

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном

		уроне пользователям.

5. 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
	5 Семестр						
1	Цели, задачи и организация технической разведки.	1-8	16/0/8		25	КИ-8	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-4, У-ПК-4, В-ПК-4
2	Характеристика видов технической разведки.	9-16	16/0/8		25	КИ-16	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-4,

							У-ПК-4, В-ПК-4
	Итого за 5 Семестр		32/0/16		50		
	Контрольные мероприятия за 5 Семестр				50	Э	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-4, У-ПК-4, В-ПК-4, 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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	5 Семестр	32	0	16
1-8	**Цели, задачи и организация технической разведки.**	16	0	8
1	**Введение** Цель и назначение курса. Краткое содержание курса. Перечень требований к базовым знаниям, необходимым для успешного освоения технических методов и средств обеспечения безопасности информации при ее обработке средствами вычислительной техники.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
2	**Концепция инженерно-технической защиты информации** Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные задачи инженерно-технической защиты информации. Факторы, влияющие на эффективность инженерно-технической защиты информации. Базовые	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0

	принципы инженерно-технической защиты информации. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.			
3	**Информации как предмет защиты** Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
4	**Элементы теории сигналов** Определение термина «сигнал» в совокупности с терминами «информация», «сообщение». Классификация сигналов по физической природе и с учетом различных моделей представления сигналов. Связь формы сигнала со структурой автоматизированной системы.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
5 - 7	Характеристики детерминированных сигналов. Энергетические характеристики детерминированных сигналов. Спектральные характеристики периодических сигналов. Спектральные характеристики непериодических характеристик. Свойства спектральной плотности непериодических сигналов.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
8	**Физические принципы утечки информации (элементы теории электростатики и** электродинамики)Электрическое, магнитное, электромагнитное поля. Уравнения Максвелла. Перенос энергии электромагнитным полем. Поле элементарного электрического излучателя (ближняя зона). Поле элементарного электрического излучателя (дальняя зона). Поле элементарного магнитного излучателя (ближняя зона). Поле элементарного магнитная излучателя (дальняя зона). Излучающие способности элементарных излучателей. Утечка информации вследствие взаимного влияния между цепями технических средств.	Всего аудиторных часов		
		6	0	0
		Онлайн		
		0	0	0
9-16	**Характеристика видов технической разведки.**	16	0	8
9	**Элементы теории радиотехнических цепей** Классификация радиотехнических цепей (линейные, параметрические, нелинейные). Характеристики сигналов при прохождении через различные радиотехнические цепи. Характеристики цепей с распределенными параметрами. Характеристики длинных линий. Прохождение сигналов через длинные линии. Антенны. Паразитные связи. Понятие об электромагнитной совместимости технических средств.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
10	**Источники опасных сигналов** Определение технического канала утечки информации (ТКУИ). Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы, их классификация и характеристика. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований. Виды побочных электромагнитных излучений. Паразитные связи и наводки опасных	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0

	сигналов. Случайные антенны. Виды опасных сигналов в помещении.			
11	**Общее представление о технической разведке** Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
12	**Элементы теории оптимального приема сигналов** Основные задачи оптимального приема. Обнаружение и различие сигналов. Оценка параметров сигнала	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
13	**Характеристика технической разведки** Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Основные направления развития технической разведки. Модель иностранной технической разведки.	Всего аудиторных часов		
		2	0	2
		Онлайн		
		0	0	0
14 - 15	**Средства технической разведки** Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства	Всего аудиторных часов		
		6	0	2
		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 ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	5 Семестр
1 - 4	**Акустические каналы.** Исследование акустических каналов.
5 - 8	**Акусто-вибрационные каналы.** Исследование акусто-вибрационных каналов.
9 - 12	**Акусто-электрические каналы.** Исследование акусто-электрических НЧ каналов
13 - 15	**Акусто-электрические каналы.** Исследование акусто-электрических ВЧ каналов

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Лекционные занятия, лабораторные работы, самостоятельная работа, контроль знаний проходят в лабораториях: «Технические средства охраны и защиты от несанкционированного доступа», «Оценка эффективности системы физической защиты».

7. 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)**
ОПК-2	З-ОПК-2	Э, КИ-8, КИ-16
	У-ОПК-2	Э, КИ-8, КИ-16
	В-ОПК-2	Э, КИ-8, КИ-16
ОПК-6	З-ОПК-6	Э, КИ-8, КИ-16
	У-ОПК-6	Э, КИ-8, КИ-16
	В-ОПК-6	Э, КИ-8, КИ-16
ПК-1	З-ПК-1	Э, КИ-8, КИ-16
	У-ПК-1	Э, КИ-8, КИ-16
	В-ПК-1	Э, КИ-8, КИ-16
ПК-4	З-ПК-4	Э, КИ-8, КИ-16
	У-ПК-4	Э, КИ-8, КИ-16
	В-ПК-4	Э, КИ-8, КИ-16
ПК-1	З-ПК-1	Э, КИ-8, КИ-16
	У-ПК-1	Э, КИ-8, КИ-16
	В-ПК-1	Э, КИ-8, КИ-16
ПК-4	З-ПК-4	Э, КИ-8, КИ-16
	У-ПК-4	Э, КИ-8, КИ-16
	В-ПК-4	Э, КИ-8, КИ-16

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 материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
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.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 621.39 С61 Антенно-фидерные устройства : учебное пособие для вузов, Старостин В.В., Кабетов Р.В., Сомов А.М., Москва: Горячая линия-Телеком, 2011

2. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2014

3. ЭИ Ш 22 Защита компьютерной информации : учебное пособие, Шаньгин В. Ф., Москва: ДМК Пресс, 2010

4. 004 К65 Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации : учебное пособие, Чистяков М.С. [и др.], Москва: НИЯУ МИФИ, 2014

5. 004 К79 Технические средства и методы защиты информации : учебное пособие, Креопалов В.В., Москва: МЭСИ, 2010

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 З-40 Защита информации : учебное пособие, Жук Е.П. [и др.], Москва: РИОР, 2015

2. 004 Е60 Защита информации в персональном компьютере : учебное пособие, Партыка Т.Л., Попов И.И., Емельянова Н.З., Москва: Форум, 2015

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Цель дисциплины состоит в подготовке разработчика технических средств защиты информации. В данной дисциплине рассматриваются технические средства различных видов, предназначенные для добывания информации в различных физических полях, а также физические принципы, лежащие в основе существования технических каналов утечки информации.

Основные задачи дисциплины – дать основы:

- технических средств добывания информации;
- назначение и функции видов разведки;
- принципов построения технических средств разведки;
- принципов защиты конфиденциальной информации техническими средствами.

В результате изучения дисциплины студенты должны:

иметь представление: о целях, задачах и принципах технических средств защиты информации; о перспективных направлениях развития технических средств разведки и систем охраны объектов; о принципах организации работ по технической защите информации;

знать: основные демаскирующие признаки объектов защиты и носителей информации; технические каналы утечки информации; технические средства разведки; способы и средства защиты конфиденциальной информации; основы организации работ по разработке технических средств защиты информации; основные руководящие документы по защите предприятий и учреждений от иностранной технической разведки.

уметь: моделировать объекты защиты; выявлять и оценивать угрозы безопасности информации на конкретных объектах; определять рациональные меры защиты на объектах и оценивать их эффективность; контролировать эффективности мер по защите информации техническими средствами.

иметь навыки: формальной постановки и решения задач эффективного применения технических средств защиты информации; применения полученных знаний на практике.

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 - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы 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.

Студенты должны, используя прослушанный на лекциях материал, научиться решать конкретные абстрактные и прикладные задачи технической защиты информации от технических разведок с помощью изучаемых методов.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

1. Определить место предмета изучения в общем поле технической безопасности, отметить границы применения, отличия от компьютерной информационной безопасности.

2. Уделять особое внимание физическому описанию явлений, лежащих в основе образования каналов утечки информации.

Автор(ы):

Краснобородько Андрей Альбертович