

ИНСТИТУТ ЯДЕРНОЙ ФИЗИКИ И ТЕХНОЛОГИЙ
КАФЕДРА ТЕОРЕТИЧЕСКОЙ И ЭКСПЕРИМЕНТАЛЬНОЙ ФИЗИКИ ЯДЕРНЫХ
РЕАКТОРОВ

ОДОБРЕНО
УМС ИИКС Протокол №УМС-575/01-1 от 30.08.2021 г.
УМС ИФТЭБ Протокол №545-1 от 30.08.2021 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	108	32	0	16		24	0	Э
Итого	3	108	32	0	16	0	24	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 ОПК-1.4 [1] – Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Код и наименование индикатора достижения компетенции З-ОПК-1.4 [1] – знать нормативными и корпоративными требованиями по безопасности компьютерных систем и сетей У-ОПК-1.4 [1] – уметь применять нормативные и корпоративные требованиями по безопасности компьютерных систем и сетей В-ОПК-1.4 [1] – владеть методами оценки уровня безопасности компьютерных систем и сетей
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-8 [1] – Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	З-ОПК-8 [1] – знать различные способы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач У-ОПК-8 [1] – уметь осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач

	В-ОПК-8 [1] – владеть принципами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач
--	--

Профессиональные компетенции в соответствии 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 <i>Основание:</i> 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
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-1.2 [1] - способен разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-1.2[1] - знать алгоритмы решения профессиональных задач; У-ПК-1.2[1] - уметь разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах; В-ПК-1.2[1] - владеть принципами разработки и анализа алгоритмов решения

			профессиональных задач
организационно-управленческий			
организация работы по эксплуатации системы защиты информации	системы защиты информации	ПК-4 [1] - способен разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации <i>Основание:</i> 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

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания Профессиональное воспитание	Задачи воспитания (код) Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Воспитательный потенциал дисциплин Использование воспитательного потенциала дисциплин профессионального модуля для формирования 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/ Практи. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>5 Семестр</i>						
1	Цели, задачи и организация технической разведки.	1-8			25	КИ-8	3-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, 3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-1.2, У-ПК-1.2, В-ПК-1.2, 3-ПК-4, У-ПК-4, В-ПК-4, 3-ОПК-4, У-ОПК-4, В-ОПК-4, 3-ОПК-8, У-ОПК-

							8, В- ОПК- 8
2	Характеристика видов технической разведки.	9-16			25	КИ-16	3- ОПК- 1.4, У- ОПК- 1.4, В- ОПК- 1.4, 3-ПК- 1, У- ПК-1, В- ПК-1, 3-ПК- 1.2, У- ПК- 1.2, В- ПК- 1.2, 3-ПК- 4, У- ПК-4, В- ПК-4, 3- ОПК- 4, У- ОПК- 4, В- ОПК- 4, 3- ОПК- 8, У- ОПК- 8, В- ОПК- 8
	<i>Итого за 5 Семестр</i>		32/0/16		50		

	Контрольные мероприятия за 5 Семестр				50	Э	
--	---	--	--	--	----	---	--

* – 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

Неделя	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>5 Семестр</i>	32	0	16
1-8	Цели, задачи и организация технической разведки.	16		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		2
		Онлайн		
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 принципы инженерно-технической защиты информации. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	Всего аудиторных часов		
		2		2
		Онлайн		
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		2
		Онлайн		
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		
		Онлайн		
5 - 7	Характеристики детерминированных сигналов.	Всего аудиторных часов		

	Энергетические характеристики детерминированных сигналов. Спектральные характеристики периодических сигналов. Спектральные характеристики непериодических характеристик. Свойства спектральной плотности непериодических сигналов.	2		2
		Онлайн		
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 магнитного излучателя (дальняя зона). Излучающие способности элементарных излучателей. Утечка информации вследствие взаимного влияния между цепями технических средств.	Всего аудиторных часов		
		6		
		Онлайн		
9-16	Характеристика видов технической разведки.	16		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		2
		Онлайн		
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 сигналов. Случайные антенны. Виды опасных сигналов в помещении.	Всего аудиторных часов		
		2		2
		Онлайн		
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		
		Онлайн		
12	Элементы теории оптимального приема сигналов Основные задачи оптимального приема. Обнаружение и различие сигналов. Оценка параметров сигнала	Всего аудиторных часов		
		2		
		Онлайн		
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		2
		Онлайн		
14 - 15	Средства технической разведки	Всего аудиторных часов		

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	6		2
	Онлайн		

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
	<i>5 Семестр</i>
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

Лабораторные работы, самостоятельная работа, контроль знаний проходят в учебно-лабораторном комплексе кафедры, который состоит из трех специализированных лабораторий: «Контроль защищенности ЛВС от несанкционированного доступа», «Защита информации от утечки по техническим каналам в ЛВС и помещениях (ПЭМИН)», «Защита речевой информации от утечки за счет недостаточной звуко- и виброизоляции помещений».

Каждая из трех специализированных лабораторий ТУЛК состоит из восьми автоматизированных рабочих мест студентов (АРМ-У), автоматизированного рабочего места преподавателя (АРМ-П), автоматизированного рабочего места администратора на двух серверах (АРМ-Адм), интерактивной доски (ИД), средств измерений и средств защиты информации, объединенных в локальную вычислительную сеть (ЛВС).

Учебно-лабораторный комплекс реализует полный цикл учебно-методических задач (используются обучающие технологии в режиме интрасеть) по практической подготовке

специалистов по технической защите информации под управлением специального программного обеспечения, которое управляет ходом выполнения типовых лабораторных практикумов (входными данными от «заказчика» в виде вариантов выполнения лабораторной работы, входными данными от «эксперта», в роли которого выступает студент, ограничениями в виде параметров требований нормативных документов, выходными данными, выполнением условий перехода к выполнению следующей лабораторной работы и оформления отчета о выполнении ТЛП) в каждой из трех специализированных лабораторий.

В состав СПО входят следующие программные функциональные модули: «Центральная база данных, приложений и архивов учебных материалов», реализованная на серверах; АРМ-П «Преподаватель» (с ним связаны четыре вспомогательные функциональные подсистемы – «Дизайнер интерфейса ТЛП», «Тесты», «Назначение Лабораторных работ/Консультаций», «Статистика»), АРМ-У «Студент», АРМ-Адм «Администратор», «Измерительный комплекс, СЗИ».

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-1.4	З-ОПК-1.4	КИ-8, КИ-16
	У-ОПК-1.4	КИ-8, КИ-16
	В-ОПК-1.4	КИ-8, КИ-16
ОПК-4	З-ОПК-4	КИ-8, КИ-16
	У-ОПК-4	КИ-8, КИ-16
	В-ОПК-4	КИ-8, КИ-16
ОПК-8	З-ОПК-8	КИ-8, КИ-16
	У-ОПК-8	КИ-8, КИ-16
	В-ОПК-8	КИ-8, КИ-16
ПК-1	З-ПК-1	КИ-8, КИ-16
	У-ПК-1	КИ-8, КИ-16
	В-ПК-1	КИ-8, КИ-16
ПК-1.2	З-ПК-1.2	КИ-8, КИ-16
	У-ПК-1.2	КИ-8, КИ-16
	В-ПК-1.2	КИ-8, КИ-16
ПК-4	З-ПК-4	КИ-8, КИ-16
	У-ПК-4	КИ-8, КИ-16
	В-ПК-4	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»	E	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			
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.

Оценочные средства приведены в Приложении.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014
2. ЭИ Ш 22 Защита компьютерной информации : учебное пособие, Москва: ДМК Пресс, 2010

3. 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, Москва: НИЯУ МИФИ, 2014

4. 004 К79 Технические средства и методы защиты информации : учебное пособие, Москва: МЭСИ, 2010

5. 621.39 С61 Антенно-фидерные устройства : учебное пособие для вузов, А. М. Сомов, В. В. Старостин, Р. В. Кабетов, Москва: Горячая линия-Телеком, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 З-40 Защита информации : учебное пособие, Москва: РИОР, 2015

2. 004 Е60 Защита информации в персональном компьютере : учебное пособие, 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.

6 семестр

Введение.

Предмет, цели, задачи и содержание курса технической защиты информации (ТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Раздел 1. 1. Цели, задачи и организация технической разведки.

Тема 1.1. Цели и задачи технической разведки.

О содержании стратегических и оперативных планов вооруженных сил; о направлениях развития вооружения и военной техники, научно-исследовательских и опытно-конструкторских работах по созданию и модернизации образцов вооружения и военной техники; о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники; о дислокации, численности и технической оснащенности войск и сил флота; о степени подготовки территории страны к ведению боевых действий; об объемах поставок и запасах стратегических видов сырья и материальных ресурсов; о функционировании промышленности, транспорта и связи; об объемах, планах государственного оборонного заказа, выпуске и поставках вооружения, военной техники и другой оборонной продукции; о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих

важное оборонное или экономическое значение; о сельском хозяйстве, финансах, торговле; о системе правительственной и иных видов специальной связи, о государственных шифрах.

Тема 1.2. Принципы организации и ведения технической разведки

Основные принципы организации ТР: целенаправленность, централизация руководства, размещение технических средств разведки (ТСР) вблизи государственных границ и на территории разведываемой страны, использование неразведывательных систем и средств, формирование целевых систем разведки, коллективное использование добытой информации ТСР, привлечение ученых к обработке информации. Основные принципы ведения ТР: комплексность, оперативность, не-прерывность, глобальность, плановость и скрытность.

Тема 1.3. Классификация технической разведки

Классификация ТР по видам используемой аппаратуры. Космическая (КР), воздушная (ВР), морская(МР) и наземная(НР).

Классификация ТР по используемой аппаратуре. Оптическая (ОР), оптико-электронная (ОЭР), радиоэлектронная (РЭР), гидроакустическая (ГАР), акустическая (АР), химическая (ХР), радиационная (РДР), сейсмическая (СР) и магнитометрическая (ММР), компьютерная (КР), телевизионная разведка (ТВР), инфракрасная разведка (ИКР), лазерная разведка и разведка лазерных излучений, разведка побочных ЭМИ и наводок

Тема 1.4. Оптико-электронная разведка (ОЭР)

Задачи ОЭР. Аппаратура ОЭР. Принцип работы аппаратуры ОЭР. Пассивная аппаратура разведки. Активная аппаратура разведки. Оценка предельных возможностей фотоприемников аппаратуры ОЭР. Диапазон длины волн ОЭР. Разрешающая способность аппаратуры ОЭР. Телевизионная разведка. Инфракрасная разведка (ИКР). Лазерная разведка и разведка лазерных излучений.

Тема 1.5. Радиоэлектронная разведка

Физические основы процесса получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами (РЭС). ЭМИ, создаваемые объектами разведки. Задачи РЭР: обнаруживать объекты, определять их местоположение и параметры движения; определять параметры объектов и характер их изменения во времени; определять назначение объектов и их типы, перехватывать передаваемую по каналам связи информацию. Диапазон спектра радиочастот средства РЭР. Особенности РЭР.

По применяемым принципам и объектам разведки она подразделяется на: радиоразведку (РР); радиотехническую разведку (РТР); радиолокационную разведку (РЛР), видовую и параметрическую; радиотепловую разведку; разведку побочных электромагнитных излучений и наводок (ПЭМИН).

Тема 1.6. Гидроакустическая разведка

Разведка гидроакустических шумовых полей, создаваемых работающими гребными винтами, различными двигателями и механизмами надводных кораблей и подводных лодок. Гидролокационная видовая разведка, обеспечивающая добывание информации, содержащейся в изображениях дна и объектов и получаемой из принимаемых отраженных сигналов. Гидролокационная параметрическая разведка, обеспечивающая получение информации,

содержащейся в пространственных, скоростных и других характеристиках объектов и получаемой из принимаемых отраженных сигналов. Разведка гидроакустических сигналов, создаваемых различными работающими средствами гидроакустического вооружения надводных кораблей и подводных лодок. Разведка звукоподводной связи с целью перехвата сообщений (информационных потоков), передаваемой по каналам этой связи. Определение тактических и технических характеристик систем звукоподводной связи.

Тема 1.7. Акустическая разведка (АР)

Получение информации путем приема и анализа акустических сигналов инфразвукового, звукового ультразвукового диапазонов, распространяющихся в воздушной среде от объектов разведки. Задачи АР. Аппаратура АР. Информационная ценность полученной речевой информации. Основные физические характеристики речи, определяющие ее сущность. Полоса звуковых частот, занимаемая речевым сигналом. Обработка и анализ принятых акустических сигналов.

Тема 1.8. Радиационная разведка (РДР)

РДР - процесс получения информации в результате приема и анализа радиоактивных излучений, связанных с выбросами и отходами атомного производства, хранением и транспортировкой радиоактивных материалов, ядерных зарядов и боеприпасов, производством и эксплуатацией ядерных реакторов, двигателей и радиоактивным заражением местности. Задачи РДР. Аппаратура дистанционной РДР. Дозиметры. Радиометры. Рентгенометры. Спектрометры.

Раздел 2.2. Характеристика видов технической разведки.

Тема 2.1. Космическая разведка.

Основные принципы ведения космической разведки (КР). Основные задачи КР. Аппаратура КР. Оптико-электронная разведка на КА. Радио- и радиотехническая разведка из космоса. Обнаружение пусков стратегических ракет.

Тема 2.2. Воздушная разведка.

Средства ведения воздушной разведки (ВР). Основные задачи ВР.

Использование разнообразных средств и способов ведения ВР.

Тема 2.3. Морская разведка

Технические средства ведения морской разведки (МР). Основные задачи МР. Специализированные разведывательные корабли. Корабли слежения за воздушно-космическими объектами.

Тема 2.4. Наземная разведка.

Средства ведения наземной разведки (НР). Основные задачи НР.

Использование разнообразных средств и способов ведения НР. Стационарные, возимые, носимые (портативные) средства НР. Характеристики технических средств НР.

Тема 2.5. Обработка разведывательной информации

Основные этапы процесса добывания разведывательной информации техническими средствами разведки (ТСР). Первичные разведданные. Обработка первичных разведданных, полученных средством разведки. Оценка полноты и достоверности разведсведений. Комплексная обработка разведсведений. Подготовка итоговой разведывательной информации для различных категорий потребителей в соответствии с их запросами.

7 семестр

Раздел 3. Методические основы защиты информации от радиотехнической разведки.

Тема 3.1. Основные характеристики каналов утечки информации применительно к радиотехнической разведке

Основные характеристики канала утечки информации применительно к РТР. Основные характеристики РЭС, существенно влияющие на возможности разведки. Основные характеристики среды, существенно влияющие на возможности разведки. Основные характеристики разведприемника, существенно влияющие на возможности разведки.

Тема 3.2. Математическая модель канала утечки информации применительно к радиотехнической разведке

Три основных блока математической модели канала утечки информации применительно к радиотехнической разведке: блок расчета отношения сигнал/шум на входе разведприемника при разведке РЭС в заданных условиях; блок описания процесса преобразования принятого входного сигнала элементами разведприемника; блок расчета информационного показателя, характеризующего эффективность работы разведприемника в процессе разведки.

Тема 3.3. Методы и средства защиты информации от радиотехнической разведки

Организационные мероприятия. Сектор запрета в угломестной плоскости. Сектор запрета в азимутальной плоскости. Продолжительность запрета в зависимости от высоты полета ИСЗ разведчика. Маскировка излучений РЭС. Технические меры, обеспечивающие скрытие излучений РЭС.

Раздел 4. Методические основы защиты информации от фотографической и оптико-электронной разведок.

Тема 4.1. Основные характеристики канала утечки информации применительно к фоторазведке

Процесс получения изображения. Характеристики, параметры. Освещенность.

Экспозиция. Мира. Пространственная частота. Частотно - контрастная характеристика (ЧКХ). Особенности канала утечки информации применительно к ФР. Математическая модель канала ФР.

Тема 4.2. Математическая модель канала утечки информации применительно к фотографической разведке

Информационные показатели статистических дуэльных ситуаций в ФР. Оценка возможностей аппаратуры фотографической разведки (АФР). Расчет вероятности обнаружения объекта АФР. Критерий обнаружения объектов на фоне случайных шумов (критерий Розелла-Вильсона).

Тема 4.3. Основные характеристики канала утечки информации применительно к телевизионной разведке.

Понятие телевизионной разведкой (ТВР). Добывание информации с помощью аппаратуры, осуществляющей прием сигналов в видимом и ближнем инфракрасных (ИК) диапазонах. Обобщенный канал утечки информации при телевизионной разведке. Принципиальные различия ТВР от ФР.

Тема 4.4. Математическая модель канала утечки информации применительно к телевизионной разведке

Подход к оценке возможностей аппаратуры телевизионной разведки (АТР). Расчет отношения сигнал/шум при дешифрировании изображений, полученных АТР. Оценка внутренних шумов приемника.

Тема 4.5. Основные характеристики канала утечки информации применительно к инфракрасной разведке

Прием и анализ электромагнитных сигналов ИК диапазона волн, излученных или отраженных объектами и предметами окружающей местности. Видовая ИКР. Параметрическая ИКР. Основные особенности канала утечки информации применительно к ИКР.

Тема 4.6. Математическая модель канала утечки информации применительно к инфракрасной разведке

Особенности отношения «сигнал/шум» в ИК диапазоне. Тепловизоры. Коэффициент теплового излучения. Измерение пространственной частоты.

Тема 4.7. Методы и средства защиты информации от визуально-оптических, фотографических и оптико-электронных средств разведки

Защита от фотографических средств разведки. Условия получения маскировочного эффекта при скрытии объектов от фотографической разведки. Использование естественных условий маскировки. Методы растительной маскировки. Скрытие объектов с помощью дымомаскировки (аэрозольные образования).

Тема 4.8. Методические основы защиты информации от радиолокационной видовой разведки

Основные характеристики канала утечки информации применительно к радиолокационной разведке. Принципы работы радиолокационных станций бокового обзора и особенности получаемых изображений.

Заключение.

Защита от технических средств разведки - неотъемлемая и составная часть научной и производственной деятельности предприятий, учреждений и организаций оборонной промышленности, а также обеспечения боевой деятельности войск и сил флота. Мероприятия по защите от ТСР. В данном курсе исследованы такие виды разведок, как радиотехническая, фото-графическая, телевизионная, инфракрасная и радиолокационная.

