Аннотация к рабочей программе дисциплины «Техническая защита информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Техническая защита информации» является ознакомление студентов с основными принципами, способами, методами и техническими средствами защиты информации, применяемыми для защиты источников информации от технических средств обнаружения.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– получить знания об основных способах защиты информации, а также об основных принципах, используемых при организации и проведения мероприятий по защите информации на объектах защиты;

– получить знания о методах защиты информации;

– получить навыки по разработке и проектированию систем защиты помещений на объектах с повышенными требованиями.

Компетенции, формируемые в результате освоения дисциплины

Способен администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

Способен принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

Разделы дисциплины

Технические разведки. Общие сведения. Радиоэлектронная разведка. Оптическая разведка. Акустическая разведка. Компьютерная разведка. Средства технической разведки. Противодействие техническим разведкам. Радиоэлектронное противодействие и радиомаскировка. Противодействие акустической разведке. Противодействие видовой разведке. Защита от внедряемых на объекты разведывательных устройств. Технические средства защиты информации.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«21» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность , одобренного Учёным советом университета, протокол №5 «30» января 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «1» февраля 2017 г.

Зав. кафедрой ИБ Таныгин М.О.
Разработчик программы
Доцент кафедры ИБ Ханис А.Л.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности 28.08.2017, №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №9 «26» марта 2018 г. на заседании кафедры информационной безопасности 29.06.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины "Техническая защита информации" является ознакомление студентов с основными принципами, способами, методами и техническими средствами защиты информации, применяемыми для защиты источников информации от технических средств обнаружения.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания об основных способах защиты информации, а также об основных принципах, используемых при организации и проведения мероприятий по защите информации на объектах защиты;
- получить знания о методах защиты информации;
- получить навыки по разработке и проектированию систем защиты помещений на объектах с повышенными требованиями.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны знать:

– назначение и функции видов добывания конфиденциальной информации

– технические средства добывания конфиденциальной информации и принципы их построения

– тактико-технические характеристики технических средств добывания информации

– основные характеристики каналов утечки информации и способы доступа к источникам конфиденциальной информации

– способы, методы и технические средства защиты конфиденциальной информации

– основные положения РД по защите информации на объектах защиты.

уметь:

– реализовывать требуемую политику безопасности с использованием сертифицированных технических средств защиты информации

– организовать инженерно-техническую защиту на объектах защиты

– осуществлять контроль эффективности мер по защите информации техническими средствами

– анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач;

– применять штатные средства защиты для решения типовых задач;

– квалифицированно оценивать область применения конкретных механизмов защиты;

– грамотно использовать технические средства защиты информации при решении практических задач;

– выявлять уязвимости в эксплуатируемых технических средствах защиты информации.

владеть:

- методами и средствами инженерной защиты и технической охраны объектов;

- методами расчета и инструментального контроля показателей защиты информации.

Процесс изучения дисциплины направлен на формирование следующих компетенций*:*

- ПК-3 - способностью администрировать подсистемы информационной безопасности объекта защиты;

- ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

- ПК-6 - способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

- ПК-12 - способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

2. Указание места дисциплины в структуре образовательной программы

«Техническая защита информации» представляет дисциплину с индексом Б.1.Б.18 базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность.Изучается на 3, 4 курсах в 6, 7 семестрах.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единиц, 180 часов

Таблица 3.1 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72

Виды учебной работы	Всего, часов
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	0
Самостоятельная работа обучающихся (всего)	79,75
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,25
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
6 семестр		
1.	Технические разведки. Общие сведения.	Демаскирующие признаки и каналы утечки информации. Виды технических разведок. Классификация технических разведок по видам носителей аппаратуры разведки. Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.
2.	Радиоэлектронная разведка.	Общие сведения о радиоэлектронной разведке. Выбор стратегий разведки и маскировки. Схема конфликтного взаимодействия средств разведки и маскировки. Сложная сигнальная обстановка. Радио и радиотехническая разведки. Способы определения частоты сигналов РЭС. Пеленгация радиоэлектронных средств. Принцип работы доплеровского пеленгатора. Радиолокационная разведка. Радиотепловая разведка. Разведка побочных электромагнитных излучений и наводок
3.	Оптическая разведка.	Общие сведения об оптической разведке. Визуально-оптическая разведка. Фотографическая и фототелевизионная разведки. Тепловидение. Оптическая (лазерная) локация
4.	Акустическая разведка.	Инструментарий акустической разведки. Обработка речевых сигналов. Акустические закладные устройства
5.	Компьютерная разведка.	Методы взлома компьютерных систем. Программы шпионы. Парольные взломщики. Криптоаналитические атаки.
6.	Средства технической разведки	Средства космической разведки. Средства воздушной разведки. Средства морской разведки. Автоматические устройства технической разведки кабельных линий связи. Портативная техника для разведслужб

7 семестр		
7.	Противодействие техническим разведкам	Общие сведения о противодействии техническим разведкам. Меры противодействия. Пути противодействия распознаванию типа объекта.
8.	Радиоэлектронное противодействие и радиомаскировка	Радиомаскировка. Экранирование. Фильтрация сигналов. Требования к заземлению технических средств. Специальные помещения. Специальные кабельные системы. Маскировка от средств РЛР. Активная радиомаскировка. Активное подавление РЛС
9.	Противодействие акустической разведке	Характеристики октавных полос частотного диапазона речи. Пассивные методы акустической защиты. Звукоизоляция. Оценка звукоизоляции объекта. Активные методы акустической защиты
10.	Противодействие видовой разведке	Защита от видовой РЛР. Защита от оптической и оптикоэлектронной разведок.
11.	Защита от внедряемых на объекты разведывательных устройств	Оценка степени угрозы объекту от возможного агентурного проникновения на охраняемую территорию Контроль радиоэфира. Проверка на наличие металл**а.** Рентгеноскопия. Поисковые приборы. Краткие сравнительные характеристики
12.	Технические средства защиты информации.	Электромагнитные материалы, используемые для экранирования, и их характеристики. Помехоподавляющие фильтры. Поисковая техника Линейные помехоподавляющие фильтры

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Технические средства разведки. Общие сведения.	2	-	-	У-1, У-2, У-3-У-10	УО - 2	ПК-3, ПК-5, ПК-6, ПК-12
2	Радиоэлектронная разведка.	2	-	-	У-1, У-2, У-3-У-10	УО - 3	ПК-3, ПК-5, ПК-6, ПК-12
3	Оптическая разведка.	2	1,2	-	У-1, У-2, У-3-У-10 МУ-1, 3	УО -4, ЗЛР - 4	ПК-3, ПК-5, ПК-6, ПК-12
4	Акустическая разведка.	2	-	-	У-1, У-2, У-3-У-10	УО – 5	ПК-3, ПК-5, ПК-6, ПК-12
	Компьютерная разведка.	2	-	-	У-1, У-2, У-3-	УО -6	ПК-3, ПК-5, ПК-6, ПК-12

5					У-10		
6	Средства технической разведки.	2	3,4	-	У-1, У-2, У-3-У-10	УО – 7 ЗЛР – 7,8	ПК-3, ПК-5, ПК-6, ПК-12
7	Противодействие техническим разведкам.	4	-	-	У-1, У-2, У-3-У-10	УО - 8	ПК-3, ПК-5, ПК-6, ПК-12
8	Радиоэлектронное противодействие и радиомаскировка.	4	-	-	У-1, У-2, У-3-У-10 МУ-2,3	УО – 10 ЗЛР – 10,12	ПК-3, ПК-5, ПК-6, ПК-12
9	Противодействие акустической разведке.	4	-	-	У-1, У-2, У-3-У-10	УО - 12	ПК-3, ПК-5, ПК-6, ПК-12
10	Противодействие видовой разведке.	4	-	-	У-1, У-2, У-3-У-10	УО - 14	ПК-3, ПК-5, ПК-6, ПК-12
11	Защита от внедряемых на объекты разведывательных устройств.	4	5	-	У-1, У-2, У-3-У-10 МУ-4	УО – 16 ЗЛР – 14,16	ПК-3, ПК-5, ПК-6, ПК-12
12	Технические средства защиты информации.	4	6,7	-	У-1, У-2, У-3-У-10 МУ-5,6	УО – 18 ЗЛР – 16,18	ПК-3, ПК-5, ПК-6, ПК-12
	Всего	36	-	-			

УО – устный опрос, ЗЛР – лабораторная работа

4.2. Лабораторные работы и практические занятия

Таблица 4.2.1 - Лабораторные работы

№п/п	Наименование лабораторной работы	Объем, час.
1	Анализ технических средств перехвата информации в оптическом диапазоне	4
2	Анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах	4
3	Анализ технических средств перехвата информации в акустическом диапазоне	4
4	Анализ технических средств перехвата информации в	6

	каналах, образованных средствами вычислительной техники	
5	Анализ технических средств перехвата информации в материально-вещественном канале утечки	6
6	Моделирование объекта защиты	6
7	Моделирование технических каналов утечки информации	6
Итого		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
6 семестр			
1.	Технические разведки. Общие сведения.	4 неделя	6
2.	Радиоэлектронная разведка.	6 неделя	6
3.	Оптическая разведка.	10 неделя	6
4.	Акустическая разведка.	12 неделя	6
5.	Компьютерная разведка.	14 неделя	6
6.	Средства технической разведки	18 неделя	6
7 семестр			
7.	Противодействие техническим разведкам	2 неделя	6
8.	Радиоэлектронное противодействие и радиомаскировка	6 неделя	6
9.	Противодействие акустической разведке	10 неделя	6
10.	Противодействие видовой разведке	12 неделя	7
11.	Защита от внедряемых на объекты разведывательных устройств	16 неделя	8
12.	Технические средства защиты информации.	18 неделя	8,75
Итого			79,75

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической,

возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– вопросов к зачету и экзамену;

–методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 19 декабря 2013 г. № 1367 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 22,2% от аудиторных занятий согласно УП.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
6 семестр			
1	Лабораторная работа№1	Анализ конкретных ситуаций	2
2	Лабораторная работа№2	Анализ конкретных ситуаций	2
3	Лабораторная работа№3	Анализ конкретных ситуаций	2
4	Лабораторная работа№4	Анализ конкретных ситуаций	2
7 семестр			
5	Лабораторная работа№6	Анализ конкретных ситуаций	3
6	Лабораторная работа№7	Анализ конкретных	3

		ситуаций	
Итого			14

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	Информационные технологии	Техническая защита информации; Безопасность операционных систем; Технические средства охраны; Системы контроля доступа и видеонаблюдения	Эксплуатационная практика; Техническая защита информации;
Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	Техническая защита информации; Технологическая практика		Инженерно-техническая защита информации; Эксплуатационная практика; Техническая защита информации;
Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	Методы защиты программного обеспечения Основы риверсинжениринга программных	Техническая защита информации;	Программно-аппаратные средства защиты информации; Техническая защита информации; Защита

	средств		информационных процессов в компьютерных системах; Эксплуатационная практика
Способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	Элементы алгебры и теории чисел; Теория графов; Практика по получению первичных профессиональных умений и навыков и навыков	Техническая защита информации; Метрология и электрорадиоизмерения; Измерение физических параметров; Учебно-исследовательская работа студентов	Техническая защита информации;

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-3/ основной и завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять	**Знать**: функционал администратора подсистемы и её компонентов **Уметь**: выполнять администрирующие инструкции в современных подсистемах ИБ **Владеть навыками**: эксплуатации различных компонентов современных подсистем ИБ	**Знать**: принципы организации современных подсистем ИБ **Уметь**: настраивать компоненты современных подсистем ИБ **Владеть навыками**: администрирования компонентов современных подсистем ИБ	**Знать**: критерии соответствия функционала подсистем угрозам для современных подсистем ИБ **Уметь**: выбирать требуемы политики безопасности при настройке оборудования современных подсистем ИБ **Владеть навыками**: реагировании на нештатные ситуации,

	знания, умения, навыки в типовых и нестандартных ситуациях			возникающие при эксплуатации компонентов современных подсистем ИБ
ПК-5/ основной и завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: -компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности. **Уметь**: - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; **Владеть навыками**: - методами определения источников и носителей защищаемой информации.	**Знать**: -компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности. - угрозы информационной безопасности. **Уметь**: - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации. **Владеть навыками**: - методами определения источников и носителей защищаемой информации, демаскирующих признаков объектов и сигналов.	**Знать**: -компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности. - угрозы информационной безопасности. - современные подходы к построению систем защиты информации. **Уметь**: - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации. - анализировать общие характеристики систем защиты информации. **Владеть навыками**: - методами определения источников и носителей защищаемой информации, демаскирующих признаков объектов и сигналов. - методами

				описания и моделирования объекты защиты.
ПК-6/ основной и завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: принципы организации проверок технических СЗИ **Уметь**: анализировать нормативную документацию для проведения проверок технических СЗИ **Владеть навыками**: организации контрольных проверок технических СЗИ	**Знать**: инструментальные средства проведения проверок технических СЗИ **Уметь**: выполнять декомпозицию информационных систем **Владеть навыками**: - инжиниринга технических средств	**Знать**: основные угрозы, предотвращаемые техническими СЗИ **Уметь**: выявлять недекларируемые возможности техничских систем **Владеть навыками**: проведения атак на разнообразные СЗИ
ПК-12/ основной и завершающий	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых	**Знать:** особенности проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - принципы оценки средств информационной безопасности. **Уметь:** проводить работы в системе защиты информации с учетом требований по обеспечению	**Знать:** особенности проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; 6 - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Уметь:**	**Знать:** особенности проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Уметь:** проводить работы в системе защиты

	и нестандартных ситуациях	информационной безопасности; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеть:** навыками проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - необходимым объемом знаний.	проводить работы в системе защиты информации с учетом требований по обеспечению информационной безопасности; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеть:** навыками проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы.	информации с учетом требований по обеспечению информационной безопасности; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - применять принципы разработки и внедрения АСЗИ. **Владеть:** навыками проведения работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Технические средства разведки. Общие сведения	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
2	Радиоэлектронная разведка	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
3	Оптическая разведка	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС, Лабораторная работа	Вопросы для устного опроса КВЗЛР №1 КВЗЛР №2	1-10 1-10 1-10	Согласно таблице 7.2
4	Акустическая разведка	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
5	Компьютерная разведка	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
6	Средства технической разведки	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС, Лабораторная работа	Вопросы для устного опроса КВЗЛР №3 КВЗЛР №4	1-10 1-10 1-10	Согласно таблице 7.2
7	Противодействие техническим разведкам	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
8	Радиоэлектронное	ПК-3, ПК-5, ПК-6,	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2

	противодействие и радиомаскировка	ПК-12				
9	Противодействие акустической разведке	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
10	Противодействие видовой разведке	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
11	Защита от внедряемых на объекты разведывательных устройств	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС, Лабораторная работа	Вопросы для устного опроса КВЗЛР №5	1-10 1-10	Согласно таблице 7.2
12	Технические средства защиты информации	ПК-3, ПК-5, ПК-6, ПК-12	Лекция, СРС, Лабораторная работа	Вопросы для устного опроса КВЗЛР №6 КВЗЛР №7	1-10 1-10 1-10	Согласно таблице 7.2

КВЗЛР – контрольные вопросы для защиты лабораторных работ.

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу 1 «Тема 1. Технические разведки. Общие сведения»

1. Элементы, содержащиеся в любой системе технической разведки.
2. Реализация обнаружения и анализа демаскирующих признаков в системе технической разведки.
3. Операции выполнения ДП по физической сути.
4. Прямые и побочные каналы утечки информации.

Специальные технические средства и решения, формирующие каналы утечки информации

Вопросы для защиты лабораторной работы № 1 «Тема 1. Технические разведки. Общие сведения»

1) Перечислите характеристики технического канала утечки информации.
2) Перечислите показатели, характеризующие оптический прибор перехвата.
3) Перечислите принципы выявления закладных устройств оптического перехвата.
4) Каковы основные способом борьбы с утечкой информации по оптическим каналам?

5) Какие мероприятия должны быть предусмотрены при построении системы защиты оптических каналов?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета и экзамена. Зачет и экзамен проводятся в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

… - Совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

(1) несанкционированный канал утечки информации
(2) технический канал утечки информации
(3) параметрический канал утечки информации
(4) физический канал утечки информации

Задание в открытой форме:

Перехват акустических сигналов по виброакустическим техническимканалам осуществляется …….

Задание на установление правильной последовательности,
Установить этапы разработки модели:
1. Построение модели
2. Объект
3. Корректировка модели
4. Анализ результатов
5. Исследование модели на компьютере

Задание на установление соответствия:
Установить соответствие между каналами связи

1	Электромагнитные каналы	А	модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи)
2	Электрические каналы	Б	подключение к линиям связи
3	Индукционный канал	В	эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов
		Г	емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации

Компетентностно-ориентированная задача:

Разработать модель реализации преднамеренного инцидента информационной безопасности, с учетом:

- перечня злоумышленников;
- целей злоумышленников;
- методов и средств реализации информационного воздействия;
- действий злоумышленников;
- объектов информационного воздействия.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
6 семестр				
Выполнение лабораторной работы №1-2	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Выполнение лабораторной работы №3	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Выполнение лабораторной работы №4	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Устный опрос по темам 1-6	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
ИТОГО				

7 семестр				
Выполнение лабораторной работы №5	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Выполнение лабораторной работы №6	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Выполнение лабораторной работы №7	6	Выполнил, доля правильных ответов от 50% до 90%	12	Выполнил,доля правильных ответов более 90%
Устный опрос по темам 7-12	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Мтого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
ИТОГО				

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

8. Учебно-методическое и информационное обеспечение учебной дисциплины

8.1 Основная учебная литература

1. Котенко В. В. Теория информации: учебное пособие / В.В. Котенко. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 240 с. // Режим доступа - https://biblioclub.ru/index.php?page=book&id=561095. – Текст: электронный.

2. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : [16+] / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный

федеральный университет, 2019. – 128 с. :– URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 20.08.2021). Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3. Зайцев А.П. Технические средства и методы защиты информации [Текст]: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

4. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=208567

5. Меньшаков Ю.К. Основы защиты от технических разведок[Текст]: учебное пособие / Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2011. – 478 с.

6. Меньшаков Ю.К. Виды и средства иностранных технических средств разведок[Текст]: учебное пособие Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2009. – 656 с.

7. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=90753

8. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=429070

9. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

10. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

8.3 Перечень методических указаний

1 Защита информации от утечки по техническим каналам: Методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун- т; сост.: Е.А. Кулешова. Курск, 2023. 53 с. – Текст: электронный.

2 Защита информации от утечки по техническим каналам: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 23 с.. – Текст: электронный

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/

4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/

5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru

7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

8) База данных "Патенты России"

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Техническая защита информации» являются лекции, лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Техническая защита информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных

консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Техническая защита информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Audacity (Свободное ПО, лицензия GNU GPL 2).

12. Материально - техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью:

- Универсальный имитатор сигналов "Test -031

Универсальный имитатор сигналов "Test -031

Прибор ИМФ-2Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”

Индикатор поля "Ekostate"
Комбинированный поисковый прибор “D008”
Тестовый приемник “XPLORER”
Универсальный поисковый прибор "СРМ-700"
Генератор шума Соната-С1
- проекционный экран на штативе;
- мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb/160Gb, проектор inFocusIN24+.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего
	изменённых	заменённых	аннулиро ван- ных	новых			