МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.17
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации

(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: 5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	7	**Итого**
Форма контроля / **Вид занятий**	экзамен	
Лекции	16	16
Лабораторные	24	24
Практические	24	24
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,35	0,35
Контактная работа	64,35	64,35
Самостоятельная работа	80	80
Контроль Экзамен	35,65	35,65
Итого	180	180

Рабочую программу составил(и):

Додонов Алексей Владимирович

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☐ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Целью освоения дисциплины «Техническая защита информации» является формирование у студентов знаний инженерно-технической защиты информации, развитие системного мышления в области защиты информации техническими средствами, навыков предотвращения утечки информации по техническим каналам и посредством побочных электромагнитных излучений и наводок. В ходе изучения дисциплины рассматриваются различные методы технических разведок, а также способы и средства обеспечения безопасности информации и противодействия разведкам.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:
- Программно-аппаратные средства защиты информации;
- Компьютерные сети.

Полученные знания используются при изучении следующих дисциплин:
- Аудит защищенности информационных систем;
- Безопасность веб-приложений.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование) [1]	**Планируемые результаты обучения**
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.4 Использует знания методов и средств контроля технической защиты информации	Знать: - возможности технических разведок; - методы и средства контроля технической защиты информации
		Уметь: - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации
		Владеть: - основами поиска закладных устройств утечки информации; - методиками проверки защищённости объектов информатизации на соответствие требованиям нормативных документов
	ПК-11.5 Умеет проектировать системы защиты информации от утечек по техническим каналам	Знать: - технические каналы утечки информации
		Уметь: - проектировать системы защиты информации от утечек по техническим каналам
		Владеть: - навыками работы с программным обеспечением технической защиты информации

[1] Для программ по ФГОС 3, 3+ – индикаторы достижения компетенций не указываются, ставится прочерк «–», указываются только компетенции и планируемые результаты обучения.

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование) [1]	**Планируемые результаты обучения**
	ПК-11.6 Владеет навыками работы с программно-аппаратными комплексами защиты информации по техническим каналам	Знать: - способы и средства защиты информации от утечек по техническим каналам
		Уметь: - измерять физические параметры сигнала и определять комплекс мер по защите сигнала от утечек
		Владеть: - навыками работы с программно-аппаратными комплексами защиты информации по техническим каналам

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Системный подход к защите информации техническими средствами Основные положения технической защиты информации. Цели защиты информации. Системы защиты информации. Инструменты технической защиты информации как часть системы защиты информации. Оценка эффективности защиты информации. Требования защиты информации техническими средствами. Классификация способов и средств защиты информации. Проблемы технической защиты информации. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок. Основные и вспомогательные технические средства и системы.	7	2		-	
Модуль 1	Пр	Тема 1 Информация как предмет защиты техническими средствами	7	2			Отчёт по практической работе №1

		Практическая работа 1. Анализ угроз информации в зависимости от её вида, источника и носителя					
Модуль 1	Ср	Тема 1 Системный подход к защите информации техническими средствами	7	10			
Модуль 1	Лек	Тема 2 Технические каналы утечки информации Понятие утечки информации. Классификация и характеристики основных каналов утечки информации. Выявление каналов утечки информации.	7	2			
Модуль 1	Лаб	Тема 2 Технические каналы утечки информации Лабораторная работа 1. Выявление каналов утечки информации	7	2			
Модуль 1	Пр	Тема 2 Технические каналы утечки информации Практическая работа 2. Изучение характеристик каналов утечки информации	7	4			Отчёт по практической работе №2
Модуль 1	Ср	Тема 2 Технические каналы утечки информации	7	10			
Модуль 1	Лек	Тема 3 Принципы и содержание технических разведок Задачи технической разведки. Виды и характеристики технических разведок. Организации, ведущие технические разведки. Средства технической разведки и несанкционированного доступа к информации. Основные технические разведки Виды и свойства оптических разведок, инструменты ведения оптических разведок. Виды и свойства акустических разведок, инструменты ведения акустических разведок. Виды и свойства радиоэлектронных разведок. Побочные электромагнитные излучения и наводки. Специальные разведки.	7	2			
Модуль 1	Пр	Тема 3 Основные технические разведки	7	2			Отчёт по практической работе №3

		Практическая работа 3. Средства технических разведок. Методы несанцкионированного доступа к информации					
Модуль 1	Лаб	Тема 3 Основные технические разведки Лабораторная работа 2. Изучение средств технических разведок	7	4			
Модуль 1	Ср	Тема 3 Основные технические разведки	7	10			
Модуль 1	Лек	Тема 4 Утечка информации посредством побочных электромагнитных излучений Физические основы побочных электромагнитных излучений. Выделение информационного сигнала в побочных излучениях. Паразитные излучения и наводки. Характеристики аппаратуры, используемой для измерения параметров побочных излучений и наводок. Способы преобразования речевой информации. Скрытие вибрационных сигналов. Экранирование и зашумление сигнала. Средства обнаружения и подавления закладных устройств. Генераторы шума.	7	2			
Модуль 1	Лаб	Тема 4 Утечка информации посредством побочных электромагнитных излучений Лабораторная работа 3. Измерение физических параметров сигнала	7	2			
Модуль 1	Лаб	Тема 4 Утечка информации посредством побочных электромагнитных излучений Лабораторная работа 4. Генерация зашумления речевого сигнала	7	4			
Модуль 1	Пр	Тема 4 Утечка информации посредством побочных электромагнитных излучений Практическая работа 4. Удаление шума в информационном сигнале	7	4			Отчёт по практической работе №4
Модуль 1	Пр	Тема 4 Утечка информации посредством побочных электромагнитных излучений	7	4			Отчёт по практической работе №5

		Практическая работа 5 Оценка защищенности помещений от утечки речевой конфиденциальной информации по каналам высокочастотного облучения и навязывания					
Модуль 1	Ср	Тема 4 Утечка информации посредством побочных электромагнитных излучений	7	10			
Модуль (раздел)	**Вид учебной работы**	**Наименование тем занятий (учебной работы)**	**Семестр**	**Объем, ч.**	**Баллы**	**Интерактив, ч.**	**Формы текущего контроля (наименование оценочного средства)**
Модуль 2	Лек	Тема 5 Предотвращение утечек по оптическим, акустическим, эдектромагнитным каналам Средства маскировки и дезинформации в оптическом диапазоне. Методы обнаружения разведок и противодействие им. Телевизионные системы наблюдения. Фотоаппаратура. Приборы ночного видения. Предотвращение утечек по акустическим и виброакустическим каналам Прослушивание информации радио- и IP-телефонов. Приём информации с радиозакладок. Высокочастотное навязывание и облучение. Пассивные радиозакладки. Побочные электромагнитные излучения в цепях питания и заземления	7	2			
Модуль 2	Лаб	Тема 5 Предотвращение утечек по оптическим, акустическим, эдектромагнитным каналам	7	2			
Модуль 2	Пр	Тема 5 Предотвращение утечек по оптическим, акустическим, эдектромагнитным каналам	7	4			Отчёт по практической работе №6

		Практическая работа 6. Расчёт цепей заземления для обеспечения защиты информации от утечки.					
Модуль 2	Лаб	Тема 5 Предотвращение утечек по оптическим, акустическим, эдектромагнитным каналам Лабораторная работа 6. Определение каналов утечки ПЭМИН	7	4			
Модуль 2	Ср	Тема 5 Предотвращение утечек по оптическим, акустическим, эдектромагнитным каналам	7	10			
Модуль 2	Лек	Тема 6 Предотвращение утечек информации с ЭВМ Обнаружение устройств негласного получения информации. Противодействие закладным устройствам. Средства радиоэлектронного подавления. Контактные и бесконтактные методы съёма информации с линий вычислительных сетей. Аппаратные закладки в оборудовании. Закладки в программном обеспечении. Способы обнаружения закладок. Программные системы защиты информации от несанкционированного доступа	7	2			
Модуль 2	Лаб	Тема 6 Предотвращение утечек информации с ЭВМ Лабораторная работа 7. Поиск аппаратных и программных закладок в оборудовании	7	2			
Модуль 2	Ср	Тема 6 Предотвращение утечек информации с ЭВМ	7	10			
Модуль 2	Лек	Тема 7 Программные системы защиты информации от несанкционированного доступа Средства защиты информации в автоматизированных системах. Электронные идентификаторы пользователя. Мандатное разграничение доступа. Локальные и серверные модели размещения.	7	2			

Модуль 2	Лаб	Тема 7 Программные системы защиты информации от несанкционированного доступа Лабораторная работа 8. Настройка системы защиты от несанкционированного доступа Dallas Lock	7	4			
Модуль 2	Ср	Тема 7 Программные системы защиты информации от несанкционированного доступа	7	10			
Модуль 2	Лек	Тема 8 Организационные меры по технической защите информации Лицензирование деятельности по защите информации. Государственное регулирование технической защиты информации. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Особенности защиты сведений, составляющих государственную тайну.	7	2			
Модуль 2	Пр	Тема 8 Организационные меры по технической защите информации Практическая работа 7. Содержательный анализ основных руководящих документов в области технической защиты информации.	7	4			Отчёт по практической работе №7
Модуль 2	Ср	Тема 8 Организационные меры по технической защите информации	7	10			
		Подготовка к экзамену	7	35,65			
	ПА	Сдача экзамена	7	0,35			Вопросы к экзамену
Итого				180			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Лабораторная работа.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, зачету. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо разобрать их с преподавателем. Подготовку к зачету необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить. Понимать основные подходы в области технических разведок и уметь организовать защиту от них.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7	ПК-11	Отчёты по практическим работам №1-7
		Вопросы к экзамену №1-65

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Выполнение практических заданий

Темы практических работ

№ п/п	Темы
1	Анализ угроз информации в зависимости от её вида, источника и носителя
2	Изучение характеристик каналов утечки информации
3	Средства технических разведок. Методы несанцкионированного доступа к информации
4	Удаление шума в информационном сигнале
5	Оценка защищенности помещений от утечки речевой конфиденциальной информации по каналам высокочастотного облучения и навязывания
6	Расчёт цепей заземления для обеспечения защиты информации от утечки.
7	Содержательный анализ основных руководящих документов в области технической защиты информации.

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты анализируют угрозы информации, изучают каналы утечек информации, средства технических разведок и оборудования для этого, оценивают защищённость выделенных помещений и проектируют средства защиты, знакомятся с материалами для проектирования помещений в защищенном исполнении, методами поиска закладок и обнаружения каналов утечки по ПЭВМИН.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 7

№ п/п	Вопросы к экзамену
1.	Особенности информации как предмета защиты.
2.	Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации
3.	Каналы утечки речевой информации
4.	Каналы утечки информации при ее передаче по каналам связи
5.	Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН
6.	Базовые принципы инженерно-технической защиты информации.
7.	Основные направления инженерно-технической защиты информации.
8.	Методы обнаружения закладных устройств съёма речевой информации
9.	Показатели эффективности инженерно-технической защиты информации.
10.	Индикаторы электромагнитных излучений. Радиочастотомеры
11.	Сканирующие приемники, селективные вольтметры, анализаторы спектра
12.	Автоматизированные поисковые комплексы
13.	Нелинейные локаторы
14.	Досмотровая техника
15.	Методы съёма информации с экранов вычислительной техники
16.	Классификация методов инженерно-технической защиты информации.
17.	Виды защищаемой информации.
18.	Виды угроз безопасности информации.
19.	Классификация информационных сигналов по физической природе.
20.	Основные принципы разведки.
21.	Классификация технической разведки.
22.	Принципы организации и ведения технической разведки.
23.	Методы противодействия наблюдению в оптическом диапазоне.
24.	Методы противодействия подслушиванию.
25.	Технические средства подслушивания.
26.	Средства перехвата сигналов.
27.	Средства противодействия подслушиванию.
28.	Средства противодействия наблюдению.
29.	Виды технических каналов утечки информации и их свойства.
30.	Демаскирующие признаки объекта. Демаскирующие признаки сигналов.
31.	Виды волн в акустическом канале утечки информации.
32.	Эффект маскировки виброакустических сигналов.
33.	Звуковое поле в помещении.
34.	Звукопоглощающие материалы и конструкции.
35.	Звукоизоляция помещений.
36.	Методические подходы к оценке эффективности защиты речевой информации.
37.	Оценка защищенности по виброакустическому каналу.
38.	Основные виды датчиков перехвата информации виброакустического канала и их характеристики.
39.	Направленные и лазерные микрофоны.

40.	Основные направления защиты от съема информации с телефонной линии.
41.	Зоны перехвата информация и виды подключений закладных устройств в каналах телефонной связи.
42.	Методы подавления радиозакладных устройств
43.	Защита информации от утечки в оптоволоконных линиях связи
44.	Паразитная генерация сигнала. Способы защиты от утечек за счёт паразитной генерации.
45.	Способы защиты информации от утечки методом ВЧ-навязывания.
46.	Легендирование объектов защиты.
47.	Фильтрация цепей питания
48.	Принципы работы охранных извещателей
49.	Разделение охранных извещателей по физическому принципу действия.
50.	Экранирование технических средств и помещений
51.	Использование специальных пленок, тканей, эмалей и ферритовых фильтров для защиты информации от утечки по электромагнитным каналам
52.	Защита акустической и речевой информации при помощи маскирующих сигналов
53.	Применение средств генерации радиоэлектронных помех для защиты информации от утечки по электромагнитному каналу
54.	Контактные и бесконтактные методы съёма информации с линий вычислительных сетей
55.	Лицензирование деятельности по технической защите информации
56.	Государственное регулирование в части технической защиты информации
57.	Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке
58.	Особенности защиты сведений, составляющих государственную тайну
59.	Основные возможности программных комплексов защиты от несанкционированного доступа
60.	Настройка мандатного доступа в программных комплексах защиты от несанкционированного доступа
61.	Локальные и серверные модели размещения средств защиты от несанкционированного доступа
62.	Использование систем DLP для защиты сведений, составляющих государственную тайну
63.	Электронные идентификаторы пользователя и их интеграция в системы защиты от НСД
64.	Классификация автоматизированных систем согласно ФСТЭК
65.	Особенности обработки информации, составляющей коммерческую и служебную тайну

7.3.2. Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**	**Критерии и нормы оценки**	
Экзамен (по накопительному рейтингу)		«отлично»	80-100 баллов
		«хорошо»	60-79 баллов
		«удовлетворительно»	40-59 баллов
		«неудовлетворительно»	0-39 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Раков А.С., Маслов О.Н., Губарева О.Ю., Почепцов А.О., Гуреев В.О.	Техническая защита информации: учебное пособие	учебное пособие	2020	
2	Горбачев, А. А.	Техническая защита информации. Поисковые приборы	учебное пособие	2022	

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
3	Рагозин Ю. Н.	Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности	учебное пособие	2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф