МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита информации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Техническая защита информации» является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачи дисциплины – дать знания: -по концепции инженерно-технической защиты информации; -по теоретическим основам инженерно-технической защиты информации; -по физическим основам инженерно-технической защиты информации; -по техническим средствам добывания и защиты информации; -по организационным основам инженерно-технической защиты информации; -по методическому обеспечению инженерно-технической защиты информации

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-7 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

ПК-4 - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- Основные методы и подходы к анализу защищенности компьютерных систем, а также принципы разработки компонентов программных и программно-аппаратных средств защиты информации.

- Номенклатуру, характеристики и принципы функционирования программно-аппаратных средств защиты информации, включая инженерно-технические средства.

- Методики проведения анализа эффективности систем защиты информации в объектах информатизации на базе компьютерных систем

Уметь:

- Формировать требования по защите информации, включая использование математического аппарата для решения прикладных задач.

- Составлять планы этапов проведения научно-исследовательских и опытно-конструкторских работ.

- Разрабатывать и анализировать структурные и функциональные схемы защищенных компьютерных систем в сфере профессиональной деятельности.

- Проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

Владеть:

- Навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

- Методами анализа безопасности компонентов программных и программно-аппаратных средств защиты информации.

- Навыками формирования требований к компонентам и методам защиты информации при проектировании.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №9
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 80 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Вводная лекция Рассматриваемые вопросы: - Цели и задачи дисциплины. - Общие принципы построения защищенной корпоративной сети
2	Концепция инженерно-технической защиты информации Рассматриваемые вопросы: - Характеристика инженерно-технической защиты информации как области информационной безопасности. - Представление сил и средств защиты информации в виде системы.
3	Теоретические основы инженерно-технической защиты информации Рассматриваемые вопросы: - Особенности информации как предмета защиты. - Виды, источники и носители защищаемой информации.
4	Демаскирующие признаки объектов наблюдения, сигналов и веществ. Рассматриваемые вопросы: - Основные и вспомогательные технические средства, и системы как источники опасных сигналов.
5	Физические основы инженерно-технической защиты информации Рассматриваемые вопросы: - Акустоэлектрические преобразователи. - Источники побочных излучений. - Характер электромагнитных излучений в ближней и дальней зонах.
6	Виды паразитных связей и наводок. Рассматриваемые вопросы: - Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.

№ п/п	Тематика лекционных занятий / краткое содержание
7	Технические средства добывания и инженерно-технической защиты информации Рассматриваемые вопросы: - Визуально-оптические приборы. - Фотоаппараты. - Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. - Средства управления доступом. - Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. - Средства видеоконтроля и видеоохраны. - Средства маскировки и дезинформирования в оптическом и радиодиапазонах.
8	Средства звукоизоляции и звукопоглащения. Рассматриваемые вопросы: - Средства обнаружения, локализации и подавления сигналов закладных устройств. - Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. - Генераторы линейного и пространственного зашумления
9	Организационные основы инженерно-технической защиты информации Рассматриваемые вопросы: - Основные задачи, структура и характеристика государственной системы противодействия технической разведке. - Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. - Основные организационные и технические меры по защите информации.
10	Аттестация объектов, лицензирование деятельности по защите информации и сертифицированные ее средства. Рассматриваемые вопросы: - Виды контроля эффективности инженерно-технической защиты информации. - Виды зон безопасности. - Методы технического контроля. - Особенности инструментального контроля эффективности инженерно-технической защиты.
11	Методическое обеспечение инженерно-технической защиты информации Рассматриваемые вопросы: - Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. - Принципы моделирование объектов защиты. - Моделирование угроз безопасности информации.
12	Методические рекомендации по выбору рациональных вариантов защиты. Рассматриваемые вопросы: - Пути оптимизации мер инженерно-технической защиты информации.
13	Программные средства защиты информации Рассматриваемые вопросы: - Виртуальные локальные сети VLAN. - Протоколы магистральных каналов. - Коммутационные массивы. - Теггированный трафик на интерфейсах сетевых устройств.
14	Маршрутизация в подсетях. Рассматриваемые вопросы: - Принципы коммутации подсетей. - Определение трансляции сетевых адресов. - Списки доступа. - Настройка доступа. - DMZ Модель прохождения трафика через сетевые интерфейсы.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Реализация стека протокола IP. - Прохождение пакета через фильтры фаервола.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Средства защиты информации В результате выполнения практического задания студент учится представление сил и средств защиты информации в виде системы.
2	Виды, источники и носители защищаемой информации В результате выполнения практического задания студент учится виды, источники и носители защищаемой информации
3	Технические средства В результате выполнения практического задания студент учится основные и вспомогательные технические средства, и системы как источники опасных сигналов
4	Электромагнитные излучений В результате выполнения практического задания студент учится характер электромагнитных излучений в ближней и дальней зонах.
5	Распространение радиосигналов В результате работы на практическом занятии студент отрабатывает умения распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
6	Средства видеоконтроля и видеоохраны В результате выполнения практического задания студент рассматривает средства видеоконтроля и видеоохраны и автоматический радиокомплекс поиск радио закладок.
7	Средства обнаружения, локализации и подавления сигналов закладных устройств. В результате выполнения практического задания студент рассматривает средства обнаружения, локализации и подавления сигналов закладных устройств и детектор звукозаписывающих устройств
8	Нормативные и методические документы по защите информации В результате выполнения практического задания студент рассматривает основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.
9	Аттестация объектов, лицензирование деятельности по защите информации В результате выполнения практического задания студент рассматривает аттестация объектов, лицензирование деятельности по защите информации и сертифицированные ее средства
10	Моделирование угроз безопасности информации В результате работы на практическом занятии студент отрабатывает умения по моделированию угроз безопасности информации и рассматривает средства защиты информации, использующие биометрические параметры
11	Средства защиты информации В результате работы на практическом занятии студент отрабатывает умения работать с средствами защиты информации, использующие персональные идентификаторы
12	Прохождение пакета через фильтры фаервола. В результате работы на практическом занятии студент отрабатывает умения прохождения пакета через фильтры фаервола.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

1. Проводные системы, портативные диктофоны и электронные стетоскопы.

2. Инфракрасные акустические системы съема информации.

3. Сетевые акустические закладки.

4. Закладные устройства типа «телефонного уха»

5. Направленные микрофоны и лазерные акустические системы разведки.

6. Сканерные приемники.

7. Цифровые анализаторы спектра, радио тестеры, частотомеры.

8. Программно-аппаратные комплексы радиотехнической разведки.

9. Средства перехвата пейджерных сообщений и контроля телефонов сотовой связи.

10. Средства компьютерного шпионажа.

11. Средства перехвата телефонных разговоров.

12. Телефонные закладки и средства перехвата факсимильных передач.

13. Средства видеонаблюдения с дальнего расстояния.

14. Средства видеонаблюдения, в том числе телевизионные, с ближнего расстояния.

15. Средства защиты по виброакустическому каналу.

16. Средства защиты по каналу ПЭМИН.

17. Средства акустической защиты переговоров.

18. Средства защиты телефонных переговоров.

19. Средства защиты сети электропитания.

20. Средства защиты от несанкционированного применения сотовых телефонов.

21. Средства защиты от несанкционированного применения диктофонов.

22. Средства защиты от радиопередатчиков.

23. Программно-аппаратные комплексы защиты от НСД.

24. Средства оценки защищенности помещений.

25. Поиск радио закладок: индикаторы поля, поисковые приемники, сканирующие приемники, комплексы радио контроля.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Методы и средства защиты информации Киреева Н. В., Крыжановский А. В., Чупахина Л. Р., Караулова О. А. Методические указания к практическим занятиям М.: Поволжский государственный университет телекоммуникаций и информатики, - 36 с. , 2019	https://reader.lanbook.com/book/255449
2	Техническая защита информации Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О. Учебное пособие Поволжский государственный университет телекоммуникаций и информатики, 96 с. , 2020	https://reader.lanbook.com/book/255575

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).
Операционная система Microsoft Windows.
Microsoft Office.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Курсовой проект в 9 семестре.
Экзамен в 9 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

Д.В. Павлинов

Согласовано:

Заведующий кафедрой ИУиИБ	Л.А. Баранов
Председатель учебно-методической комиссии	Н.А. Андриянова