МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором 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 РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

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-13 - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;

ПК-3 - Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности;

ПК-26 - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Уметь:

Производит проверки технического состояния и профилактические осмотры технических средств защиты информации.

Уметь:

Производит проверки технического состояния и профилактические осмотры технических средств защиты информации.

Уметь:

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

Уметь:

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

Уметь:

Разрабатывает и анализирует структурные и функциональные схемы защищенных компьютерных систем в сфере профессиональной деятельности.

Знать:

Знать основные методы и подходы к анализу защищенности компьютерных систем.

Уметь:

Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

Владеть:

Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

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):	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	34	34

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 76 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
2	Цели и задачи дисциплины. Общие принципы построения защищенной корпоративной сети
3	Концепция инженерно-технической защиты информации
4	Характеристика инженерно-технической защиты информации как области информационной безопасности. Представление сил и средств защиты информации в виде системы.
5	Теоретические основы инженерно-технической защиты информации
6	Особенности информации как предмета защиты. Виды, источники и носители защищаемой информации.
7	Демаскирующие признаки объектов наблюдения, сигналов и веществ. Основные и вспомогательные технические средства, и системы как источники опасных сигналов.
8	Физические основы инженерно-технической защиты информации
9	Акустоэлектрические преобразователи. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах.
10	Виды паразитных связей и наводок. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
11	Технические средства добывания и инженерно-технической защиты информации
12	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.

№ п/п	Тематика лекционных занятий / краткое содержание
13	Средства звукоизоляции и звукопоглащения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления
14	Организационные основы инженерно-технической защиты информации
15	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.
16	Аттестация объектов, лицензирование деятельности по защите информации и сертифицированные ее средства. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты.
17	Методическое обеспечение инженерно-технической защиты информации
18	Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирование объектов защиты. Моделирование угроз безопасности информации.
19	Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.
20	Программные средства защиты информации
21	Виртуальные локальные сети VLAN. Протоколы магистральных каналов. Коммутационные массивы. Теггированный трафик на интерфейсах сетевых устройств. Маршрутизация в подсетях. Принципы коммутации подсетей. Определение трансляции сетевых адресов. Списки доступа. Настройка доступа. DMZ Модель прохождения трафика через сетевые интерфейсы. Реализация стека протокола IP. Прохождение пакета через фильтры фаервола.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ-1 Представление сил и средств защиты информации в виде системы.
2	ПЗ-2 Виды, источники и носители защищаемой информации
3	ПЗ-3 Основные и вспомогательные технические средства, и системы как источники опасных сигналов
4	ПЗ-4 Характер электромагнитных излучений в ближней и дальней зонах.

№ п/п	Тематика практических занятий/краткое содержание
5	ПЗ-5 Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
6	ПЗ-6 Текущий контроль ПК1 (РИТМ-МИИТ)
7	ПЗ-7 Средства видеоконтроля и видеоохраны. Автоматический радиокомплекс поиск радио закладок.
8	ПЗ-8 Средства обнаружения, локализации и подавления сигналов закладных устройств. Детектор звукозаписывающих устройств
9	ПЗ-9 Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.
10	ПЗ-10 Аттестация объектов, лицензирование деятельности по защите информации и сертифицированные ее средства
11	ПЗ-11 Моделирование угроз безопасности информации. Средства защиты информации, использующие биометрические параметры
12	ПЗ-12 Средства защиты информации, использующие персональные идентификаторы
13	ПЗ-13 Прохождение пакета через фильтры фаервола.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (2, стр.4) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
2	СР2 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 10-29) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
3	СР3 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 47-98) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
4	СР4 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 47-98) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
5	СР5 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 300-302) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела. 4. Подготовка к тестированию для прохождения первого текущего контроля - (РИТМ-МИИТ) ПК1.

№ п/п	Вид самостоятельной работы
6	СР6 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 300-302) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела. 4. Подготовка к тестированию для прохождения первого текущего контроля - (РИТМ-МИИТ) ПК1
7	СР7 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 402-454) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
8	СР8 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр. 402-454) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
9	СР9 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.721-740) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
10	СР10 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.721-740) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
11	СР11 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.765-811) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела. 4. Подготовка к тестированию для прохождения второго текущего контроля - (РИТМ-МИИТ) ПК2
12	СР12 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.765-811) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела. 4. Подготовка к тестированию для прохождения второго текущего контроля - (РИТМ-МИИТ) ПК2.
13	Выполнение курсового проекта.
14	Подготовка к промежуточной аттестации.
15	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	Инженерно-техническая защита информации А.Г. Лихоносов Книга Юридический институт МИИТа , 2011	ИТБ УЛУПС (Абонемент ЮИ)
2	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)

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

- Вузовские электронно-библиотечные системы учебной литературы http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ - База научно-технической информации ВИНИТИ РАН - Интернет-ресурсы: http://www.fstec.ru - сервер ФСТЭК (Федеральная служба по техническому и экспортному контролю http://www.itsec.ru - информационная безопасность http://www.security.lab.ru - информационный портал в области защиты информации http://www.fstec.ru – материалы сайта фирмы «Лаборатория Касперского» Электронно-библиотечная система должна обеспечивать возможность индивидуального доступа, для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

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

Для проведения лекций и практических занятийтребуется компьютерный класс (локальная сеть, состоящая из 20 рабочих мест (компьютеров), сервера, компьютера преподавателя, проектора, электронная доска). Компьютеры должны быть обеспечены стандартными лицензионными программными продуктами и обязательно программным продуктом Microsoft Office не ниже Microsoft Office 2007 (2013).

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

Для проведения аудиторных занятий и самостоятельной работы требуется:1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения практических занятий:компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

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:

доцент кафедры «Управление и защита информации» Д.В. Павлинов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин