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 - программы бакалавриата
по направлению подготовки
02.03.02 Фундаментальная информатика и
информационные технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита информации

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Техническая защита информации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих задач.

Основными задачами дисциплины являются:

- Сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- Проведение проектных расчетов элементов систем обеспечения технической защиты информации;
- Участие в разработке технологической и эксплуатационной документации;
- Проведение предварительного технико-экономического обоснования проектных расчетов
- Осуществление организационно-правового обеспечения технической защиты объекта информатизации;
- Организация работы малых коллективов исполнителей с учетом требований защиты информации;
- Совершенствование системы управления технической защиты информации;
- Изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;
- Контроль эффективности реализации политики технической защиты информации
- Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;
- Участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации.

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения технической защиты информации с учетом установленных требований;

- администрирование подсистем технической защиты объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите автоматизированных систем.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-8 - Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты и принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

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

Знать:

- концепцию инженерно-технической защиты информации;
- нормативно-правовые документы обеспечения информационной безопасности;
- технические каналы утечки информации;
- физические принципы утечки информации по техническим каналам;
- методы обнаружения и защиты информации в технических каналах от ее утечки.

Уметь:

- применять методы инженерно-технической защиты информации;
- анализировать возможные уязвимые места технической защиты информации;
- проводить предварительный сбор данных о технических уязвимостях;
- проектировать системы защиты и проводить анализ рисков утечки информации по техническим каналам.

Владеть:

- навыками работы с программным обеспечением по оценки рисков утечки информации по техническим каналам и программно-аппаратными комплексами по выявлению каналов утечки информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №7
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 44 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	Введение в техническую защиту информации Содержание учебного материала: - Введение. - Информация. и защита данных.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Конфиденциальность информации. - Целостность информации. - Доступность информации. - Служебная информация. - Личные данные. - Государственные структуры, отвечающие за защиту данных. - Определение служебной тайны. - Законодательство РФ в области информационной безопасности. - Информационная безопасность коммерческой структуры. -Типовой набор должностей, связанных с защитой данных на предприятии. - Международные стандартизирующие организации. - Стандарты РФ в области информационной безопасности.
2	Угрозы информационной безопасности Содержание учебного материала: - Природа возникновения угроз. - Классификация угроз по преднамеренности проявления. - Классификация по источнику угрозы. - Классификация по степени воздействия на информационную систему. - По способам доступа к ресурсам информационной системы. - Угрозы безопасности информационной системы. - Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.
3	Политика безопасности Содержание учебного материала: - Структура политики безопасности. - Базовая политика безопасности. - Специализированные политики безопасности.
4	Криптографическая защита Содержание учебного материала: - Классификация криптографических алгоритмов. - Основные определения. - Назначение шифрования. - Принципы криптографического закрытия информации. - Простые методы шифрования. - Таблица Вижинера. - Шифрование с открытым и закрытым ключами. - Основные виды атак на криптоалгоритмы. - Симметричные криптоалгоритмы. - Алгоритм DES. - Алгоритм 3DES. - Алгоритм AES. - Вопросы стойкости криптоалгоритмов. проблема распределения ключей. - Достоинства и недостатки симметричного шифрования. - Асимметричные криптоалгоритмы. - Алгоритм RSA. - Алгоритм Диффи-Хэлмана. - Электронно-цифровая подпись. - Достоинства и недостатки асимметричного шифрования и область его применения.
5	Защита от несанкционированного доступа Содержание учебного материала: - Аутентификация, авторизация и администрирование действий пользователей. - Основные принципы системы AAA.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Методы аутентификации: пароли, PIN и биометрические данные. - Авторизация. Accounting. - Сервер AAA. - Фильтрация трафика. - Списки доступа. - Инспекция трафика. - Традиционный межсетевой экран.
6	Защита информации в глобальной сети Содержание учебного материала: - Защита http-трафика. - Характерные угрозы. - Защищенный протокол httpd. - Цифровые сертификаты. - Виртуальная частная сеть.
7	Классификация и общая характеристика технических средств добывания информации Содержание учебного материала: - Специальные технические средства. - Основные тактико-технические параметры средств информационной разведки. - Технологическая классификация специальных технических средств (СТС).
8	Назначение и функции видов разведки Содержание учебного материала: - Основные понятия. - Характеристика разведывательной деятельности. - Формы разведывательной информации. - Каналы распространения информации. - Структура разведывательных служб бывшего Советского Союза. - Структура КГБ СССР. - Структура службы внешней разведки.
9	Спецслужбы США Содержание учебного материала: - Разведывательное сообщество США. ЦРУ (CIA). РУМО (DIA) АНБ (NSA). НУВКР (NRO). ФБР (FBI).
10	Оптическая разведка Содержание учебного материала: - Оптические каналы утечки информации. - Принципы оптической разведки. - Технические характеристики средств оптической разведки. - Общие характеристики человеческого глаза. - Характеристики объективов. - Характеристики визуально-оптических приборов. - Характеристики фото- и киноаппаратов. - Технические характеристики средств телевизионной разведки . - Характеристики приборов ночного видения. - Характеристики тепловизоров.
11	Радиоэлектронная разведка Содержание учебного материала: - Общая характеристика радиоэлектронной разведки. - Особенности, целевое назначение, источники и технические средства.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Целевое назначение. - Источники. - Технические средства радиоэлектронной разведки.
12	Перехват информации после 2000 года Содержание учебного материала: - Проблемы перехвата информации. - Оборудование систем перехвата информации. - Радиоэлектронные каналы утечки информации. - Основные показатели.
13	Излучатели электромагнитных полей Содержание учебного материала: - Основные понятия. - Антенны. - Случайные излучатели. - Электрический диполь. - Магнитный диполь. - Сравнительный анализ полей электрического и магнитного диполя. - Краткая формулировка результатов сравнительного анализа.
14	Акустическая разведка Содержание учебного материала: - Акустические каналы утечки информации. - Общая характеристика. - Прямой акустический канал. - Виброакустический канал . - Оптико-акустический канал. - Электроакустический канал. - Технические средства акустической разведки. - Функции технических средств.
15	Микрофоны Содержание учебного материала: - Принцип действия микрофонов. - Принцип действия случайных электроакустических преобразователей. - Характеристика известных технических средств. - Способы и средства добывания информации о радиоактивных веществах. - Доступ к информации без нарушения государственной границы и проникновения на объект защиты.
16	Особые случаи утечки информации Содержание учебного материала: - Добывание информации без физического проникновении в контролируемую зону. - Доступ к источникам информации без нарушения государственной границы. - Комплексное использование технических средств разведки.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Введение в информационную безопасность. Стандарты и организации, работающие в области информационной безопасности В результате выполнения лабораторной работы студент получит практические навыки поиска нормативной информации в глобальной сети, работы с нормативными актами в сфере ИБ, навыки выявления и учета информационных активов защищаемой организации.
2	Угрозы информационной безопасности В результате выполнения лабораторной работы студент получит навыки создания списка информационных активов, определения актуальных угроз информационной безопасности, классификации источников угроз и защищаемой информации в соответствии с существующей нормативной базой.
3	Политика безопасности. Разработка политики безопасности В результате выполнения лабораторной работы студент получит практические навыки разработки политики информационной безопасности предприятия.
4	Криптографическая защита. Шифрование и расшифрование данных В результате выполнения лабораторной работы студент приобретает навыки работы с базовыми криптографическими алгоритмами и совершенствует свои навыки программирования на языках высокого уровня.
5	Изучение оборудования стенда «Системы контроля и управления доступом» В результате выполнения лабораторной работы студент изучает состав лабораторного оборудования, технику безопасности при работе с ним и готовится к выполнению последующих лабораторных работ.
6	Изучение интерфейса связи Dallas Touch Memory (iButton) В результате выполнения лабораторной работы студент приобретает навыки работы с нормативной и технической документацией и подготовке к работе интерфейса связи iButton.
7	Контроль доступа с помощью считывателя iButton и контролера СКУД в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение с помощью считывателя iButton, включая программирование ключей и ведение базы данных пользователей.
8	Изучение интерфейса связи Wiegand В результате выполнения лабораторной работы студент приобретает навыки работы с нормативной и технической документацией и подготовке к работе интерфейса связи Wiegand.
9	Изучение RFID-технологии и стандартов карт доступа В результате выполнения лабораторной работы студент приобретает навыки использования нормативной документации - стандартов на карты доступа и выполняет подготовку к работе с RFID-оборудованием.
10	Контроль доступа с помощью RFID-считывателя и контролера СКУД в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение с помощью считывателя карт доступа по RFID-технологии, включая программирование карт и ведение базы данных пользователей.
11	Контроль доступа с помощью контролера СКУД в сетевом режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение в сетевом режиме работы контроллера СКУД.

№ п/п	Наименование лабораторных работ / краткое содержание
12	Изучение технологии считывания биометрических данных В результате выполнения лабораторной работы студент приобретает навыки с технической документацией, изучает состав оборудования считывания биометрических данных и готовится к его использованию.
13	Конфигурирование биометрического считывателя в автономном режиме В результате выполнения лабораторной работы студент приобретает навыки контроля доступа в помещение или к рабочему месту с помощью анализа его биометрических данных – отпечатков пальца.
14	Установка устройства контроля доступа к компьютеру «Соболь» В результате выполнения лабораторной работы студент изучает устройство «Соболь», технику безопасности при работе с ним и устанавливает его на компьютер.
15	Защита от несанкционированного доступа В результате выполнения лабораторной работы студент получит базовые навыки защиты информации от НСД: обеспечение безопасности персонального компьютера средствами операционной системы и с помощью USB-ключей.
16	Защита информации в глобальной сети В результате выполнения лабораторной работы студент получит навыки безопасного использования сети Internet.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Основные положения и принципы построения технической защиты информации.

2. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.

3. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

4. Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

5. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

6. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

7. Методы защиты видовых демаскирующих признаков от технических средств разведок.

8. Методы защиты сигнальных демаскирующих признаков от технических средств разведок.

9. Методы защиты радиосигналов от перехвата техническими средствами разведок.

10. Методы защиты электрических сигналов от перехвата техническими средствами разведок.

11.Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок.

12.Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

13.Технические средства наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

14.Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.

15.Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей.

16.Методы и технические средства съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.

17. Методы и технические средства съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.

18. Технические средства подслушивания, методы и средства противодействия средствам подслушивания.

19. Технические средства анализа демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства.

20. Технические средства контроля, обнаружения, уничтожение закладных устройств, порядок проведения ЗПМ.

21.Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ.

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

№ п/п	Библиографическое описание	Место доступа
1	Голдовский Я.М., Желенков Б.В., Сафонова И.Е.Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. :МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. (в пер.)	https://library.miit.ru/bookscatalog/metod/03-42764.pdf
2	Голдовский Я.М. ,Желенков Б.В., Цыганова Н.А. Маршрутизация в компьютерных сетях : [Электронный ресурс] : учеб. пособие по дисц. "Сети и телекоммуникации" для студ. напр. "Информатика и вычислительная техника" ; МИИТ. Каф. "Вычислительные системы и сети". - М. : РУТ(МИИТ), 2017. - 114 с.	https://library.miit.ru/bookscatalog/metod/DC-407.pdf
3	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с. : ил. - Библиогр.: с. 26.	https://library.miit.ru/bookscatalog/metod/04-46051.pdf
4	Желенков Борис Владимирович. Канальный уровень модели OSI : метод. указ. к лаб. раб. по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", напр. "Информатика и вычислительная техника" / Б.В. Желенков ; МИИТ. Каф.	https://library.miit.ru/bookscatalog/metod/03-41547.pdf

	"Вычислительные системы и сети". - М. : МИИТ, 2011. - 50 с. : ил. с. 49. - Текст : непосредственный	
5	Защищенные беспроводные и мобильные коммуникации: Учеб. пособие для студ., обуч. по магистерской программе Безопасность и защита инф-ции напр. Информатика и выч. тех.; МИИТ. Центр компетентности Защита и безопасность информации / В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев. - М.: МИИТ, 2007. - 121 с. : ил. - Библиогр.: с. 120	https://library.miit.ru/miitpublishing/04-35015.pdf

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

ФСТЭК России

https://fstec.ru/component/tags/tag/tzi

Справочно-правовая система по информационной безопасности

https://sps-ib.ru/materialy:tzi

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

Интернет-браузер (Yandex и др.)

Microsoft Windows.

Microsoft Office

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

1. Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ, курсового проектирования (выполнения курсовых работ):

- компьютер преподавателя, рабочие станции студентов, СКУД, мульимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

2. Учебная аудитория для проведения учебных занятий (защищённое помещение для проведения лабораторных работ):

- компьютер преподавателя, СКУД, мультимедийное оборудование, доска.

9. Форма промежуточной аттестации:

Зачет в 7 семестре.
Курсовая работа в 7 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова