

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 магистратуры
по направлению подготовки
09.04.03 Прикладная информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Технические средства и методы защиты информации

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль): Прикладная информатика в обеспечении безопасности бизнеса

Форма обучения: Заочная

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: 166642
Подписал: заведующий кафедрой Маслова Мария Валерьевна
Дата: 07.06.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Технические средства и методы защиты информации» является формирование у обучающихся компетенций в соответствии

с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по направлению «Прикладная информатика» и приобретение ими:

- знаний о видах, источниках и носителях защищаемой информации, концепции инженерно-технической защиты информации, порядке организации инженерно-технической защиты информации;

- умений выявлять угрозы и технические каналы утечки информации; описывать (моделировать) объекты защиты и угрозы безопасности информации; применять наиболее эффективные методы и средства инженерно-технической защиты информации;

- навыков инженерного расчета размеров контролируемой зоны.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-54 - Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий.

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

Знать:

о видах, источниках и носителях защищаемой информации, концепции инженерно-технической защиты информации, порядке организации инженерно-технической защиты информации;

Уметь:

выявлять угрозы и технические каналы утечки информации; описывать (моделировать) объекты защиты и угрозы безопасности информации; применять наиболее эффективные методы и средства инженерно-технической защиты информации;

Владеть:

инженерного расчета размеров контролируемой зоны.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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 №2
Контактная работа при проведении учебных занятий (всего):	16	16
В том числе:		
Занятия лекционного типа	8	8
Занятия семинарского типа	8	8

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 200 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	Раздел 1 Раздел 1. Технические каналы утечки информации. Теория защищаемой информации. Информация, виды, ценность, демаскирующие признаки. Термины и определения в области технической защиты информации. Классификация технических каналов утечки информации.

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>Место технической защиты информации в государственной системе защиты информации в Российской Федерации.</p> <p>Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.</p> <p>Технические каналы утечки информации, возникающей за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений.</p> <p>Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Электромагнитный, электрический и индукционный каналы утечки информации по каналам связи.</p> <p>Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации</p> <p>Теоретические основы инженерно-технической защиты информации</p> <p>Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности</p> <p>Раздел 2. Способы и средства защиты информации от утечки по техническим каналам.</p> <p>Задачи и принципы и методы инженерно-технической защиты информации.</p> <p>Классификация средств защиты информации и требования к ним.</p> <p>Методы и средства защиты информации от визуально-оптических фотографических и оптико-электронных средств разведки</p> <p>Организация защиты информации от утечки по техническим каналам/ Физические основы защиты информации</p> <p>Акустоэлектрические преобразования. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.</p> <p>Раздел 3. Методы и средства контроля эффективности технической защиты информации.</p> <p>Аппаратура для выявления и параметризации опасных сигналов электромагнитной природы и измерения акустических сигналов. Визуально-оптические приборы. Фотоаппараты.</p> <p>Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства. Средства ВЧ-навязывания и лазерного подслушивания.</p> <p>Автономные средства разведки.</p> <p>Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны.</p> <p>Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей,</p>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>фильтрации и заземления. Генераторы линейного и пространственного зашумления. Технический контроль эффективности принимаемых мер защиты. Назначение, содержание, вид и методы технического контроля. Основные средства технического контроля.</p> <p>Порядок проведения контроля защищенности информации на объекте ВТ от утечки ПЭМИН по различным каналам.</p> <p>Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.</p> <p>Раздел 4. Организация технической защиты информации.</p> <p>Система защиты информации и этапы ее построения.</p> <p>Основные организационно-технические мероприятия по защите информации. Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации. Аттестация объекта информатизации/ Организационно-технические мероприятия и технические способы защиты информации выделенного защищаемого помещения.</p> <p>Концепция инженерно-технической защиты информации</p> <p>Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.</p>

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1 Изучение борьбы с каналы утечки информации.
2	Практическое занятие 2 изучение способов и средств защиты информации от утечки по техническим каналам.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом; работа со справочной и специальной литературой; выполнение курсовой работы
2	Выполнение курсового проекта.
3	Подготовка к промежуточной аттестации.

4.4. Примерный перечень тем курсовых проектов

Курсовая работа по дисциплине «Технические средства и методы защиты информации» - это комплексная самостоятельная работа обучающегося. Темой курсовой работы является «Исследование методов и

технических средств защиты информации в соответствии с вариантом задания». Варианты заданий представлены в ФОС учебной дисциплины.

?

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

№ п/п	Библиографическое описание	Место доступа
1	Технические средства и методы защиты информации: Учебник для вузов Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова М.: ООО «Издательство Машиностроение» , 2009	http://e.lanbook.com/
2	Информационная безопасность: Учебник для студентов вузов. Ярочкин В.И. М.: Академический Проект; Гаудеамус,	библиотека РОАТ

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

Официальный сайт РУТ (МИИТ) (<http://miit.ru/>)

Электронно-библиотечная система Научно-технической библиотеки МИИТ (<http://library.miit.ru/>)

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

Электронно-библиотечная система РОАТ (<http://biblioteka.rgotups.ru/jirbis2/>)

Образовательная платформа ЮРАЙТ (<https://urait.ru/>)

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

- Программное обеспечение для выполнения практических заданий включает в себя специализированное прикладное программное обеспечение, а также программные продукты общего применения

- Программное обеспечение для проведения лекций, демонстрации презентаций и ведения интерактивных занятий: Microsoft Office 2003 и выше.

- Программное обеспечение, необходимое для оформления отчетов и

иной документации: Microsoft Office 2003 и выше.

- Программное обеспечение для выполнения текущего контроля успеваемости: Браузер Internet Explorer 6.0 и выше.

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 с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

4. Для проведения практических и лабораторных занятий: компьютерный класс; кондиционер; компьютеры с минимальными требованиями - Pentium 4, ОЗУ 4 Гб, HDD 100 Гб, USB 2.0.

Технические требования к оборудованию для осуществления учебного процесса с использованием дистанционных образовательных технологий:

колонки, наушники или встроенный динамик (для участия в аудиоконференции); микрофон или гарнитура (для участия в аудиоконференции); веб-камеры (для участия в видеоконференции);

для ведущего: компьютер с процессором Intel Core 2 Duo от 2 ГГц (или аналог) и выше, от 2 Гб свободной оперативной памяти.

9. Форма промежуточной аттестации:

Курсовой проект во 2 семестре.

Экзамен во 2 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, профессор,
д.н. кафедры «Системы управления
транспортной инфраструктурой»

А.В. Горелик

Согласовано:

Заведующий кафедрой СУТИ РОАТ

А.В. Горелик

Заведующий кафедрой ПК РОАТ

М.В. Маслова

Председатель учебно-методической
комиссии

С.Н. Климов