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)

Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении

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).

Основной целью изучения дисциплины «Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении» является формирование у обучающегося компетенций для следующих видов деятельности: - проектная; - организационно-управленческая. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): Проектная деятельность: - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; - разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием. Организационно-управленческая деятельность: - осуществление правового, организационного и технического обеспечения защиты информации; - организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации); Специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем": - разработка проектов нормативных правовых актов, руководящих и методических документов предприятия, учреждения, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации. Дисциплина «Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении» имеет целью ознакомление слушателей с нормативными и организационными документами, доктринами, стандартами ФСБ и ФСТЭК. Дисциплина обеспечивает приобретение знаний и умений в области защиты информации по утечке в различных каналах связи и несанкционированному доступу к ней. Задача дисциплины «Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении» – получение основополагающих знаний о методах обеспечения безопасности информации на различных обьектах защет руководящих и нормативных документов, а так же внутренних документов организации, и о каналах утечки защищаемой информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-4 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

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

Знать:

- Роль и место информации, информационных технологий (ИТ) и информационной безопасности (ИБ) в системе национальных интересов и обеспечения национальной безопасности государства.
- Иерархию и систему законодательства Российской Федерации в области информации, ИТ и защиты информации (Конституция РФ, ГК РФ, УК РФ, КоАП РФ, федеральные законы № 149-ФЗ, 152-ФЗ, 187-ФЗ, 98-ФЗ и др.); Систему государственных стандартов (ГОСТ Р ИСО/МЭК серии 27000, ГОСТ Р 57580 и др.) и отраслевых стандартов в области защиты информации.

Уметь:

- Выявлять, оценивать и классифицировать актуальные угрозы информационной безопасности для различных субъектов (граждан, коммерческих организаций, государственных институтов).
- Выявлять противоречия и пробелы в локальной нормативной базе организации и предлагать пути их устранения для обеспечения соответствия федеральным требованиям.

Владеть:

- Навыками критической оценки информационных потоков и медийного контента с точки зрения обеспечения интересов государства и общества.
- Навыками работы со справочно-правовыми системами (КонсультантПлюс, Гарант, Официальный интернет-портал правовой информации) и базами нормативно-технических документов ФСТЭК/ФСБ.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №10
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
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 100 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 Правовые основы обеспечения защиты информации.
2	Меры и средства защиты информации. 1. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Организационная структура системы обеспечения безопасности информационных технологий. Распределение функций. Система нормативно- методических и организационно-

№ п/п	Тематика лекционных занятий / краткое содержание
	распорядительных документов организации по обеспечению безопасности информационных технологий.
3	Утечка информации по техническим каналам Технические каналы утечки информации. Технические средства минимизации ущерба от инцидентов.
4	Информационные технологии. 1. Угрозы безопасности информационных технологий. Виды мер и основные принципы обеспечения безопасности информационных технологий. 2. Правовые основы обеспечения безопасности информационных технологий. Государственная система защиты информации.
5	Аппаратно-программные средства защиты информации от несанкционированного доступа. Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.
6	Безопасность в компьютерных системах и сетях 1. Проблемы обеспечения безопасности в компьютерных системах и сетях. Назначение, возможности, и основные защитные механизмы межсетевых экранов. 2. Виртуальные частные сети. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности. Анализ содержимого почтового и WEB-трафика (CONTENT SECURITY).
7	Аудит информационной безопасности 1. События безопасности, аудит. Мониторинг событий безопасности. 2. Стандартны и критерии проведения аудита информационной безопасности. 3. Методология аудита информационной безопасности. Организация процесса аудита.
8	Техническая защита информации 1. Основные приборы и оборудование, применяемое для выявления технических каналов утечки информации. 2. Основы организации и обеспечения работ по технической защите информации. 3. Технические средства защиты информации и организация работ по защите информации.
9	Компьютерные инциденты 1. Понятие о компьютерных инцидентах. Минимизация ущерба, наносимого инцидентом. Юридические предпосылки для расследования инцидентов и минимизации ущерба. Расследование инцидентов в Российской Федерации и за рубежом. 2. Некоторые средства контроля коммуникаций и средств ЭВТ. Действия в случае возникновения инцидента. Изъятие и исследование компьютерной техники и носителей информации.
10	Методы аудирования. 1. Основные понятия в области безопасности информационных технологий. Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях. Ответственность за нарушения. 2. Порядок работы с носителями ключевой информации. Инструкции по организации паролей и антивирусной защиты. Аудит информационной безопасности компаний: общие понятия и определения.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Практическое занятие №1 Вводное занятие. Техника безопасности в компьютерном классе.
2	Практическое занятие №2 Доклады студентов по теме «Технические каналы утечки информации», «Технические средства минимизации ущерба от инцидентов».
3	Практическое занятие №3 Доклады студентов по теме «Угрозы безопасности информационных технологий», «Виды мер и основные принципы обеспечения безопасности информационных технологий», «Правовые основы обеспечения безопасности информационных технологий».
4	Практическое занятие №4 Доклады студентов по теме «Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты», Аппаратно-программные средства защиты информации от несанкционированного доступа», «Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа».
5	Практическое занятие №5 Доклады студентов по теме «Проблемы обеспечения безопасности в компьютерных системах и сетях», «Назначение, возможности, и основные защитные механизмы межсетевых экранов», «Виртуальные частные сети», «Возможности сканеров безопасности».
6	Практическое занятие №6 Доклады студентов по теме «Мониторинг событий безопасности», «Стандартны и критерии проведения аудита информационной безопасности», «Методология аудита информационной безопасности», «Организация процесса аудита».
7	Практическое занятие №7 Доклады студентов по теме «Основные приборы и оборудование, применяемое для выявления технических каналов утечки информации», «Основы организации и обеспечения работ по технической защите информации», «Технические средства защиты информации и организация работ по защите информации».
8	Практическое занятие №8 Доклады студентов по теме «Понятие о компьютерных инцидентах», «Расследование инцидентов в российской федерации и за рубежом», Средства контроля коммуникаций и средств ЭВТ».
9	Практическое занятие №9 Доклады студентов по теме «Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях», «Порядок работы с носителями ключевой информации».

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительного материала.
2	Выполнение курсовой работы.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

- Особенности обеспечения информационной безопасности микропроцессорных систем управления;

- Сертификация средств защиты информации по требованиям ФСБ;

- Особенности обеспечения информационной безопасности защищенных помещений;

- Особенности утечки информации по ПЭМИН;

- Особенности обеспечения информационной безопасности объектов вычислительной техники;

- Особенности утечки информации по закрытому каналу связи (Intranet);

- Сертификация средств защиты информации по требованиям ФСТЭК;

- Утечки информации по виброакустическому каналу;

- Особенности утечки информации по открытому каналу Ethernet;

- Особенности обеспечения информационной безопасности на транспортных средствах;

- Особенности утечки информации по акустоэлектрическому каналу;

- Классификация объектов информатизации по требованиям информационной безопасности;

- Особенности обеспечения информационной безопасности диспетчерских систем управления.

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации Прохорова О.В. Учебник 7-е изд., стер. — Санкт-Петербург: Лань, - 122 с. — ISBN 978-5-507-57304-2. , 2026	https://reader.lanbook.com/book/525917
2	Организационное и правовое обеспечение информационной безопасности Донгак Ш.М., Хади Н.М. Практикум Москва : РТУ МИРЭА, 74 с. — ISBN 978-5-7339-2307-9. , 2024	https://reader.lanbook.com/book/448901#1

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).

Для проведения лекционных занятий

необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Для проведения практических занятий необходимы

необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:Microsoft Office 2003, MathCAD 14.0 или другая система моделирования.

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

Для проведения лекционных и практических занятий требуется комплекс программно-технических средств в составе:

-ноутбук; -источник бесперебойного питания; -интерактивная доска; -проектор с разрешением не менее 1280x1024

9. Форма промежуточной аттестации:

Зачет в 10 семестре.

Курсовая работа в 10 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, доцент, к.н. кафедры «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта А.А. Привалов

Согласовано:

Заведующий кафедрой ИУиИБ Л.А. Баранов

Председатель учебно-методической комиссии Н.А. Андриянова