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)

Методы анализа управления рисками

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).

Целями изучения дисциплины «Методы анализа управления рисками» являются теоретическая и практическая подготовка специалистов к деятельности, связанной управления рисками, связанными с безопасностью информационных и компьютерных систем.

Задачи дисциплины: изучение принципов принятия решений в условиях риска и неопределенности; изучение характеристик полезности; получение навыков решения задач принятия решений в условиях риска; получение навыков анализа источников риска и их описания; получение навыков разработки математических моделей рисковых ситуаций; получение навыков использования методов решения задач оптимального управления риском. Основной целью изучения учебной дисциплины «Методы анализа управления рисками» является формирование у обучающегося компетенций для следующих типов задач профессиональной деятельности: эксплуатационная; специализация №8. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): Эксплуатационная деятельность: проверка технического состояния и профилактические осмотры технических средств защиты информации. Специализация №8: разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла.

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

Знать:

- основные процессы проектирования систем обеспечения информационной безопасности
- основные методы и подходы к анализу защищенности компьютерных систем.
- основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.
- программно-аппаратные средства защиты информации

Уметь:

- разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
- применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.
- разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования.

Владеть:

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.
- навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.
- навыками разработки нормативной правовой документации.

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 №10
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	Введение Рассматриваемые вопросы: - Предмет курса и его связь со смежными дисциплинами. - Библиография.
2	Теория рисков. Рассматриваемые вопросы: - Риск и неопределенность. - Функция полезности. - Классификация рисков. - Природа рисков. - Методы управления рисками в финансовой сфере, банковском деле, страховании. - Методы управления рисками в производственной сфере, строительстве. - Методы управления рисками в транспортной отрасли, на железнодорожном транспорте, в логистических системах. - Методы управления рисками в экологической и социальной сфере, туризме.

№ п/п	Тематика лекционных занятий / краткое содержание
3	Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности. Рассматриваемые вопросы: - Модель безопасности с полным перекрытием. информационной безопасностью, анализ средства обеспечения безопасности. - Модель безопасности с пол-ным перекрытием. - Программные риски.
4	Стандартыв области информационной безопасности, использующие Рассматриваемые вопросы: - Современные стандарты в области информационной безопасности, использующие концепцию управления рисками - Вопросы стандартизации в области информационной безопасности.
5	Проблематика управления информационной безопасностью Рассматриваемые вопросы: - Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности.
6	Стандарты ISO/IEC Рассматриваемые вопросы: - ISO/IEC 15408. - Критерии оценки безопасности информационных технологий. - Стандарты ISO/IEC 17799/27002 и 27001. - ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. - Практические правила управления информационной безопасностью".
7	ГОСТ Р ИСО/МЭК Рассматриваемые вопросы: - ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". - Системы менеджмента информационной безопасности.
8	Методики построения систем защиты информации Рассматриваемые вопросы: - Вопросы политики безопасности. - Стандарты, процедуры, метрики и анализ рисков. - Методики стратегического планирования построения системы защиты. - Модель многоуровневой защиты.
9	Данные об информационной системе Рассматриваемые вопросы: - Сбор данных об информационной системе с помощью средств администрирования. - Сбор данных о топологии сети с помощью средства администрирования сетей. - Использование сканеров безопасности для получения информации о сети. - Выявление уязвимостей.
10	Методики и программные продукты для оценки рисков Рассматриваемые вопросы: - Методика CRAMM. - Методика FRAP. - Методика OCTAVE. - Методика RiskWatch. - Методика Microsoft. - Анализ существующих подходов.
11	Методы совершенствования системы управления информационной безопасностью компьютерной системы

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - Локальная политика паролей. - Управление разрешениями на файлы и папки. - Использование цифровых сертификатов. - Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft.
12	Идентификация и аутентификация. Рассматриваемые вопросы: - Протокол Kerberos. - Шифрование данных при хранении. - Межсетевые экраны - Встроенный межсетевой экран (firewall). - Настройка протокола IPSec. - Автоматическое обновление операционной системы с использованием службы WSUS. - Установка сервера обновлений. - Управление обновлениями. - Распространение обновлений.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Введение В результате выполнения работы студент рассматривает основные понятия, классификацию рисков, модели безопасности.
2	Стандарты информационной безопасности В результате выполнения работы студент изучает основные стандарты и ГОСТы в области информационной безопасности.
3	Построение систем защиты информации В результате выполнения работы студент рассматривает особенности построения систем защиты информации, отрабатывает навык анализа и сбора данных об информационной системе и топологии сети с помощью средств администрировния и использование сканеров безопасности для получения информации о сети.
4	Методики и программные продукты для оценки рисков В результате выполнения лабораторной работы студент рассматривает особенности методики CRAMM, методики FRAP, методики OCTAVE, методики RiskWatch, методики Microsoft и анализирует существующие подходы.
5	Совершенствование системы управления информационной безопасностью компьютерной системы В результате выполнения работы студент рассматривает локальную политику паролей, управление разрешениями на файлы и папки, умение использовать цифровых сертификатов, изучает центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft, идентификацию и аутентификацию, протоколы Kerberos и шифрование данных при хранении.

4.3. Самостоятельная работа обучающихся.

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

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

№ п/п	Библиографическое описание	Место доступа
1	Оценкка рисков Шеверева Е.А. Учебное пособие М.: МИРЭА - Российский технологический университет, 162 с. , 2022	https://reader.lanbook.com/book/310883#2
2	Инвестиционная деятельность режимных объектов Пронина Ю.Ю. Учебное пособие Пенза: Изд-во ПГУ, - 116 с. - ISBN 978-5-907364-44-8 , 2020	https://reader.lanbook.com/book/322748#2

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

Пакет прикладных программ MATLAB

Пакет прикладных программ MATCad

Пакет прикладных программ LABView

Среда визуального программирования MicroSoft Visual Studio 2013.

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:

Экзамен в 10 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта В.Г. Сидоренко

Согласовано:

Заведующий кафедрой ИУиИБ Л.А. Баранов

Председатель учебно-методической комиссии Н.А. Андриянова