**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 специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором 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

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 видов деятельности: эксплуатационная; специализация №8. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами 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-17** - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;

**ПК-20** - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

**ПК-21** - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

**ПК-22** - Способен проводить тестирование систем защиты информации автоматизированных систем;

**ПК-23** - Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем;

**ПК-25** - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

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

**ПК-28** - 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.

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 №9 |
| 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<br>Рассматриваемые вопросы:<br>- Предмет курса и его связь со смежными дисциплинами.<br>- Библиография. |
| 2 | Теория рисков.<br>Рассматриваемые вопросы:<br>- Риск и неопределенность.<br>- Функция полезности.<br>- Классификация рисков.<br>- Природа рисков.<br>- Методы управления рисками в финансовой сфере, банковском деле, страховании.<br>- Методы управления рисками в производственной сфере, строительстве.<br>- Методы управления рисками в транспортной отрасли, на железнодорожном транспорте, в логистических системах.<br>- Методы управления рисками в экологической и социальной сфере, туризме. |
| 3 | Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности.<br>Рассматриваемые вопросы:<br>- Модель безопасности с полным перекрытием. информационной безопасностью, анализ средства обеспечения безопасности.<br>- Модель безопасности с пол-ным перекрытием.<br>- Программные риски. |
| 4 | Стандартыв области информационной безопасности, использующие<br>Рассматриваемые вопросы:<br>- Современные стандарты в области информационной безопасности, использующие концепцию управления рисками<br>- Вопросы стандартизации в области информационной безопасности. |
| 5 | Проблематика управления информационной безопасностью<br>Рассматриваемые вопросы:<br>- Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности. |
| 6 | Стандарты ISO/IEC<br>Рассматриваемые вопросы:<br>- ISO/IEC 15408.<br>- Критерии оценки безопасности информационных технологий.<br>- Стандарты ISO/IEC 17799/27002 и 27001.<br>- ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология.<br>- Практические правила управления информационной безопасностью". |
| 7 | ГОСТ Р ИСО/МЭК<br>Рассматриваемые вопросы:<br>- ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".<br>- Системы менеджмента информационной безопасности. |
| 8 | Методики построения систем защиты информации<br>Рассматриваемые вопросы:<br>- Вопросы политики безопасности.<br>- Стандарты, процедуры, метрики и анализ рисков.<br>- Методики стратегического планирования построения системы защиты.<br>- Модель многоуровневой защиты. |
| 9 | Данные об информационной системе |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | Рассматриваемые вопросы:<br>- Сбор данных об информационной системе с помощью средств администрирования.<br>- Сбор данных о топологии сети с помощью средства администрирования сетей.<br>- Использование сканеров безопасности для получения информации о сети.<br>- Выявление уязвимостей. |
| 10 | Методики и программные продукты для оценки рисков<br>Рассматриваемые вопросы:<br>- Методика CRAMM.<br>- Методика FRAP.<br>- Методика OCTAVE.<br>- Методика RiskWatch.<br>- Методика Microsoft.<br>- Анализ существующих подходов. |
| 11 | Методы совершенствования системы управления информационной безопасностью компьютерной системы<br>Рассматриваемые вопросы:<br>- Локальная политика паролей.<br>- Управление разрешениями на файлы и папки.<br>- Использование цифровых сертификатов.<br>- Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft. |
| 12 | Идентификация и аутентификация.<br>Рассматриваемые вопросы:<br>- Протокол Kerberos.<br>- Шифрование данных при хранении.<br>- Межсетевые экраны<br>- Встроенный межсетевой экран (firewall).<br>- Настройка протокола IPSec.<br>- Автоматическое обновление операционной системы с использованием службы WSUS.<br>- Установка сервера обновлений.<br>- Управление обновлениями.<br>- Распространение обновлений. |

## 4.2. Занятия семинарского типа.

## Лабораторные работы

| № п/п | Наименование лабораторных работ / краткое содержание |
|---|---|
| 1 | Введение<br>В результате выполнения лабораторной работы студент рассматривает основные понятия, классификацию рисков, модели безопасности. |
| 2 | Стандарты информационной безопасности<br>В результате выполнения работы студент изучает основные стандарты и ГОСТы в области информационной безопасности. |
| 3 | Построение систем защиты информации<br>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 |

| № п/п | Наименование лабораторных работ / краткое содержание |
|---|---|
| | 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<br>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.<br>Введение<br>Предмет курса и его связь со смежными дисциплинами. Библиография. Теория рисков. 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. Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности. Модель безопасности с полным перекрытием. информационной безопасностью, анализ средства обеспечения безопасности. Модель безопасности с пол-ным перекрытием. Программные риски. |
| 2 | Подготовка к лабораторным работам.<br>Современные стандарты в области информационной безопасности, использующие концепцию управления рисками<br>Вопросы стандартизации в области информационной безопасности. Проблематика управления информационной безопасностью, анализ средства обеспечения безопасности. 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". ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Системы менеджмента информационной безопасности. |
| 3 | Выполнение курсовой работы.<br>Методики построения систем защиты информации<br>Вопросы политики безопасности. Стандарты, процедуры, метрики и анализ рисков. Методики стратегического планирования построения системы защиты. Модель многоуровневой защиты. 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 |
| 4 | Выполнение курсового проекта. |
| 5 | Подготовка к промежуточной аттестации. |
| 6 | Подготовка к текущему контролю. |

4.4. Примерный перечень тем курсовых проектов

Построение множества эффективных решений и эффективной границы

для задачи инвестирования с безрисковым активом.

Построение множества эффективных решений и эффективной границы для общей задачи инвестирования на примере задачи с n=3 активами.

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2009 | ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ) |
| 2 | Надежность технических систем и техногенный риск Ч.1 Надеж-ность технических систем Воскобоев В. Ф. Альянс, , 2008 | НТБ МИИТ фб. - 3; чз.2 - 2; чз.4 - 2 |
| 3 | Риск-менеджмент Левицкая Л.П., Федорова Н.О. МИИТ, , 2013 | http://library.miit.ru/ №3568 |
| 4 | Страхование и риски в туризме Загурская С.Г. МИИТ , 2009 | http://library.miit.ru/ №2998 |
| 5 | Корпоративный менеджмент на железнодорожном транспорте (Реинжиниринг бизнес-процессов. Управление рисками предпринимательской деятельности)- VII Часть Ковальская М.И., Козырев В.А. МИИТ , 2009 | http://library.miit.ru/ |
| 6 | Методы оценки и управления рисками при строительстве и реконструкции железных дорог Э.С. Спиридонов, Александр Сергеевич Беляев, Владимир Игоревич Гулак Книга 2010 | |
| 7 | Задача о минимизации рисков Н.Н. Брушлинская; МИИТ. Каф. "Вычислительная математика" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (уч.1) |
| 8 | Финансовая среда предпринима-тельства и предпринима-тельские риски Резер А.В., Шиповская Н.И. МИИТ , 2006 | http://library.miit.ru/ |
| 1 | Информационная безопас-ность и защита информации в корпоративных сетях железнодорожного транспорта. Учебник для студ. вузов ж.-д. трансп. Яковлев В.В.; Корниенко А.А. УМК МПС России , 2002 | НТБ МИИТ уч.4 - 252; чз.1 - 1; фб. - 3 |
| 2 | Управление рисками при реализации инвестиционных про-ектов Москвин В.А. Финансы и статистика , 2004 | НТБ МИИТ фб. - 3; чз.2 - 2; уч.2 - 15 |
| 3 | Риск-анализ инвестиционного проекта М.В. Грачева, С.Я. Бабаскин, И.М. Волков и др.; Под ред. М.В. Грачевой Однотомное издание ЮНИТИ , 2001 | НТБ (уч.6); НТБ (фб.); НТБ (чз.2) |
| 4 | Методы анализа и управления эколого-экономическими рисками Тихомиров Н. П., Потравный И.М.,Тихомирова Т.М. ЮНИТИ-ДАНА , 2003 | НТБ МИИТ фб. - 3; чз.1 - 1; чз.4 - 1; уч.1 - 20 |
| 5 | Физические основы техниче-ских средств обеспечения | НТБ МИИТ фб. - 3; |

| | | |
|---|---|---|
| | информационной безопасности Соболев А. Н., Кириллов В.М. Гелиос АРВ , 2004 | чз.2 - 2; уч.3 - 21 |
| 6 | Методы предотвращения и обнаружения вторжений В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2) |
| 7 | Безопасность операционных систем и приложений В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2) |
| 8 | Безопасность систем баз данных В.П. Соловьев, В.В. Гуренко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2) |
| 9 | Безопасность операционных систем В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2) |
| 10 | Защита от вирусов, межсе-тевые экраны и другие механизмы обеспечения безопасности ин-формационных систем В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ , 2007 | НТБ МИИТ фб. - 3; чз.2 - 2 |
| 11 | Защищенные беспроводные и мобильные коммуникации В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.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/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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:

Зачет в 9 семестре.
Курсовой проект в 9 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
«Управление и защита информации» В.Г. Сидоренко

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин