**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-13** - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

**ПК-19** - Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств 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-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:

**Уметь:**

Строит математические модели для оценки безопасности компьютерных систем.

**Уметь:**

Анализирует компоненты системы безопасности с использованием современных математических методов.

**Уметь:**

Разрабатывает математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

**Владеть:**

Анализирует математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

**Уметь:**

Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

**Уметь:**

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

**Уметь:**

Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.

**Уметь:**

Проводит анализ угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта.

**Уметь:**

Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

**Знать:**

Знать основные процессы проектирования систем обеспечения информационной безопасности.

**Уметь:**

Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

**Знать:**

Знать основные методы и подходы к анализу защищенности компьютерных систем.

**Уметь:**

Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации.

**Владеть:**

Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.

**Знать:**

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

**Уметь:**

Уметь 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:**

Владеть 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 | Сем. №9 |
| Контактная работа при проведении учебных занятий (всего): | 48 | 48 |
| В том числе: | | |
| Занятия лекционного типа | 32 | 32 |
| Занятия семинарского типа | 16 | 16 |

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 96 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 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 |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | сфере, строительстве. Методы управления рисками в транспортной отрасли, на железнодорожном транспорте, в логистических системах. Методы управления рисками в экологической и социальной сфере, туризме. |
| 2 | Методы совершенствования системы управления информационной безопасностью компьютерной системы Локальная политика паролей. Управление разрешениями на файлы и папки. Использование цифровых сертификатов. Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft. Идентификация и аутентификация. Протокол Kerberos. Шифрование данных при хранении. |
| 3 | 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 |
| 4 | Современные стандарты в области информационной безопасности, использующие концепцию управления рисками 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. |
| 5 | 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. |
| 6 | Методики построения систем защиты информации 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. |
| 7 | Методики и программные продукты для оценки рисков Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов. |
| 8 | 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 | ПЗ1 |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| | 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 | ПЗ2<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 | ПЗ3<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 | ПЗ4<br>Методики и программные продукты для оценки рисков<br>Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов. |
| 5 | ПЗ5<br>Методы совершенствования системы управления информационной безопасностью компьютерной системы<br>Локальная политика паролей. Управление разрешениями на файлы и папки. Использование цифровых сертификатов. Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft. Идентификация и аутентификация. 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. |

## 4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | СР1<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 |

| № п/п | Вид самостоятельной работы |
|---|---|
| | 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 | СР2<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 | СР3<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 | СР4<br>Методики и программные продукты для оценки рисков<br>Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов. |
| 5 | СР5<br>Методы совершенствования системы управления информационной безопасностью компьютерной системы<br>Локальная политика паролей. Управление разрешениями на файлы и папки. Использование цифровых сертификатов. Центр сертификации (удостоверяющего центра) в ОС Unix и Microsoft. Идентификация и аутентификация. 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. |
| 6 | Выполнение курсового проекта. |
| 7 | Подготовка к промежуточной аттестации. |
| 8 | Подготовка к текущему контролю. |

4.4. Примерный перечень тем курсовых проектов

Примерная тематика курсовых проектов (работ)

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 | |
| 4 | Страхование и риски в туризме Загурская С.Г. МИИТ , 2009 | |
| 5 | Корпоративный менеджмент на железнодорожном транспорте (Реинжиниринг бизнес-процессов. Управление рисками предпринимательской деятельности)- VII Часть Ковальская М.И., Козырев В.А. МИИТ , 2009 | |
| 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 | |
| 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 информационной безопасности Соболев А. Н., Кириллов В.М. Гелиос АРВ , 2004 | НТБ МИИТ фб. - 3; 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 | НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2) |

| | | |
|---|---|---|
| | информации" Однотомное издание МИИТ , 2007 | |
| 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).

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://www.iso27000.ru/ http://siblec.ru/ http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru scholar.google.ru Поисковые системы: Yandex, Google, Mail.

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

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практических занятийнеобходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office не ниже Microsoft Office 2007 (2013), 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).

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. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения практических занятий:компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

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» | Сидоренко Валентина Геннадьевна |

Лист согласования

| | |
|---|---|
| Заведующий кафедрой УиЗИ | Л.А. Баранов |
| Председатель учебно-методической комиссии | С.В. Володин |