МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ


П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Сидоренко Валентина Геннадьевна, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы анализа управления рисками

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Методы анализа управления рисками" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-1 Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	ПКР-1.1 Строит математические модели для оценки безопасности компьютерных систем. ПКР-1.2 Анализирует компоненты системы безопасности с использованием современных математических методов.
2	ПКР-7 Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	ПКР-7.1 Разрабатывает математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.2 Анализирует математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.3 Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
3	ПКР-8 Способен подготовить обоснование необходимости защиты информации в автоматизированной системе	ПКР-8.1 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта. ПКР-8.2 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.
4	ПКР-9 Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой	ПКР-9.1 Проводит анализ угроз безопасности информации, обрабатываемой автоматизированными системами высокоскоростного транспорта. ПКР-9.2 Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.
5	ПКС-2 Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	ПКС-2.1 Знать основные процессы проектирования систем обеспечения информационной безопасности. ПКС-2.2 Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.
6	ПКС-3 Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	ПКС-3.1 Знать основные методы и подходы к анализу защищенности компьютерных систем. ПКС-3.2 Уметь применять инструментальные средства анализа защищенности компьютерных систем на объектах информатизации. ПКС-3.3 Владеть навыками разработки документации по сопровождению систем обеспечения информационной безопасности на объектах информатизации.
7	ПКС-5 Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите	ПКС-5.1 Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации. ПКС-5.2 Уметь разрабатывать нормативно правовые

№ п/п	Код и название компетенции	Ожидаемые результаты
	информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации	акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования. ПКС-5.3 Владеть навыками разработки нормативной правовой документации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 9
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	90	90
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КП (1), ПК1, ПК2	КП (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	9	Раздел 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 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	8		2		16	26	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		безопасности с пол-ным перекрытием. Программные риски.							
2	9	Раздел 2 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. 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	6		4		16	26	ПК1

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		информационной безопасности.							
3	9	Раздел 3 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.	4		4		16	24	
4	9	Раздел 4 Методики и программные продукты для оценки рисков Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов.	8		4		18	30	КП, ПК2
5	9	Раздел 5 Методы совершенствования системы управления	10		4		24	38	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		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. 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	9	Раздел 6 Зачет с оценкой						0	ЗаО
7		Всего:	36		18		90	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	9		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 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
2	9		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. 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.	4

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
3	9		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.	4
4	9		Методики и программные продукты для оценки рисков Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов.	4
5	9		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. 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
			ВСЕГО:	18 / 0

4.5. Примерная тематика курсовых проектов (работ)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Методы анализа управления рисками» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 70 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 30 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.

Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) . Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы.

В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося.

Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	9		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 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.	16
2	9		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. 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.	16
3	9		Методики построения систем защиты информации Вопросы политики безопасности. Стандарты, процедуры, метрики и анализ рисков. Методики стратегического планирования построения системы защиты. Модель	16

			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	9		Методики и программные продукты для оценки рисков Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методика Microsoft. Анализ существующих подходов.	18
5	9		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. Межсетевые экраны Встроенный межсетевой экран (firewall). Настройка протокола IPSec. Автоматическое обновление операционной системы с использованием службы WSUS. Установка сервера обновлений. Управление обновлениями. Распространение обновлений.	24
			ВСЕГО:	90

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Информационная безопасность и защита информации	Мельников В. П., Клейменов С. А., Петраков А.М.	Академия, 2009 НТБ МИИТ фб. - 3; чз.2 - 2; уч.4 - 15	Все разделы
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	Все разделы
3	Риск-менеджмент	Левицкая Л.П., Федорова Н.О.	МИИТ, 2013 http://library.miit.ru/ №3568	Все разделы
4	Страхование и риски в туризме	Загурская С.Г.	МИИТ, 2009 http://library.miit.ru/ №2998	Все разделы
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/	Все разделы
6	Методы оценки и управления рисками при строительстве и реконструкции железных дорог	Спиридонов Э.С., Беляев А.С., Гулак В.И.	МИИТ, 2010 http://library.miit.ru/	Все разделы
7	Задача о минимизации рисков	Брушлинская Н.Н.	МИИТ, 2007 http://library.miit.ru/ №2672	Все разделы
8	Финансовая среда предпринима-тельства и предпринима-тельские риски	Резер А.В., Шиповская Н.И.	МИИТ, 2006 http://library.miit.ru/	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
9	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	Все разделы
10	Управление рисками при реализации инвестиционных про-ектов	Москвин В.А.	Финансы и статистика , 2004 НТБ МИИТ фб. - 3; чз.2 - 2; уч.2 - 15	Все разделы
11	Риск-анализ инвестиционного проекта	Грачева М.В., Бабаскин С.Я.; Волков И.М.	ЮНИТИ, 2001 НТБ МИИТ фб. - 3; чз.2 - 3; уч.6 - 22; уч.2 - 22	Все разделы
12	Методы анализа и управления эколого-экономическими	Тихомиров Н. П., Потравный И.М.,	ЮНИТИ-ДАНА , 2003	Все разделы

	рисками	Тихомирова Т.М.	НТБ МИИТ фб. - 3; чз.1 - 1; чз.4 - 1; уч.1 - 20	
13	Физические основы технических средств обеспечения информационной безопасности	Соболев А. Н., Кириллов В.М.	Гелиос АРВ , 2004 НТБ МИИТ фб. - 3; чз.2 - 2; уч.3 - 21	Все разделы
14	Методы предотвращения и обнаружения вторжений	Соловьев В. П., Павленко Н.В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы
15	Безопасность операционных систем и приложений	Соловьев В. П., Павленко Н.В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы
16	Безопасность систем баз данных	Соловьев В. П., Гуренко В..В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы
17	Безопасность операционных систем	Соловьев В. П., Павленко Н.В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы
18	Защита от вирусов, межсетевые экраны и другие механизмы обеспечения безопасности информационных систем	Соловьев В. П., Павленко Н.В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы
19	Защищенные беспроводные и мобильные коммуникации	Соловьев В. П., Иванов Д.В., Пуцко Н.Н.	МИИТ, 2007 НТБ МИИТ фб. - 3; чз.2 - 2	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ 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.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
Для проведения практических занятий необходимы 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.

10. 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 INTRANET
4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.
Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.
Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.
Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.
При подготовке специалиста важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний,

полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что- то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств являются составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.