

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

25 мая 2018 г.



Кафедра «Управление и защита информации»

Автор Привалов Александр Андреевич, к.т.н.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2018</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии</p> <p style="text-align: center;"> С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 15 мая 2018 г. Заведующий кафедрой</p> <p style="text-align: center;"> Л.А. Баранов</p>
--	--

Москва 2018 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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 видами 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 объектах защиты руководящих и нормативных документов, а так же внутренних документов организации, и о каналах утечки защищаемой информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Аппаратные средства вычислительной техники:

Знания: современные аппаратные средства вычислительной техники их параметры, характеристики.

Умения: изменять, дополнять, адаптировать, использовать аппаратно-программные средства вычислительной техники для решения поставленных задач защита информации.

Навыки: прогнозировать, предполагать, моделировать развитие событий, ситуаций при изменении конфигураций аппаратных средств вычислительной техники.

2.1.2. Организационное и правовое обеспечение информационной безопасности:

Знания: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности;- методологию создания систем защиты информации;- современные подходы к построению систем защиты информации;- компьютерную систему как объект информационного воздействия и методы обеспечения ее информационной безопасности; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.

Умения: - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам оценки защищенности информации в компьютерных системах; - анализировать и оценивать угрозы информационной безопасности объекта, выбирать методы и средства защиты.

Навыки: - профессиональной терминологией в области информационной безопасности; - методами анализа и контроля показателей технической защиты информации в компьютерных системах и объектах информатизации.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Государственная итоговая аттестация

2.2.2. Научно-исследовательская работа

2.2.3. преддипломная практика

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	ПК-16 способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	<p>Знать и понимать: действующих нормативных правовых актов по информационной безопасности на территории РФ, а также знания основных зарубежных стандартов</p> <p>Уметь: применять полученные знания для разработки проектов нормативных правовых актов и другой документации, регламентирующих работу по обеспечению информационной безопасности компьютерных систем</p> <p>Владеть: навыками использования современных программных и технических сред для проектирования</p>
2	ПК-6 способностью участвовать в разработке проектной и технической документации	<p>Знать и понимать: основные организационные и правовые методы обеспечения безопасности информационных систем, современные технические методы и средства защиты информации компьютерных систем и сетей, формальные модели политик безопасности, политик управления доступом и информационными потоками в информационных системах, методы анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области информационной безопасности.</p> <p>Уметь: исследовать существующие и разрабатывать новые методы защиты информации, исследовать существующие и разрабатывать новые защищенные протоколы обмена информацией, разрабатывать предложения по совершенствованию управления безопасностью информационных систем и сетей, проводить анализ проектных решений по обеспечению защищенности компьютерных систем, разрабатывать проектную и техническую документацию, проводить обоснование и выбор рационального решения по уровню защищенности информационной системы с учетом заданных требований.</p> <p>Владеть: современными методами и средствами защиты информации при ее передаче и хранении, современными методами исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ, навыками проведения инструментального мониторинга технической защиты информации и инструментального мониторинга защиты от атак в компьютерных системах и сетях, методами анализа безопасности информационных систем с использованием отечественных и зарубежных стандартов в области</p>

№ п/п	Код и название компетенции	Ожидаемые результаты
		информационной безопасности;
3	ПК-8 способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	<p>Знать и понимать: Проектирование информационной системы (ИС). Понятия и структура проекта ИС. Требования к эффективности и надежности проектных решений. Основные компоненты технологии проектирования ИС. Методы и средства проектирования ИС. Краткая характеристика применяемых технологий проектирования. Требования, предъявляемые к технологии проектирования ИС. Выбор технологии проектирования ИС. Каноническое проектирование ИС. Стадии и этапы процесса проектирования ИС. Состав работ на предпроектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС, эксплуатации и сопровождения. Состав проектной документации. Состав, содержание и принципы организации информационного обеспечения ИС.</p> <p>Уметь: с позиций системного подхода ставить задачу построения ИС на объекте автоматизации; управлять процессом проектирования ИС; применять полученные знания для построения систем управления информационными потоками; осуществлять обоснованный выбор профессионально-ориентированных ИС в предметной области; способы проведения анализа предметной области и решения задачи способы построения ИС с использованием различных методов; 4 канонического и типового проектирования ИС способы проектирования документальных и фактографических баз данных;</p> <p>Владеть: понятийным аппаратом курса, навыками программирования в современных средах, навыками анализа информации, методами проектирования, методами синтеза информационных систем, современными методами защиты информации, навыками составления чертежей и смет, навыками выбора оборудования для ЗИ</p>
4	ПСК-8.4 способностью участвовать в создании системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении	<p>Знать и понимать: проектирование документальных БД: анализ предметной области, разработка состава и структуры БД, проектирование логико-семантического комплекса. Проектирование фактографических БД: методы проектирования; концептуальное, логическое и физическое проектирование. Принципы и особенности проектирования интегрированных ИС. Система управления информационными потоками как средство интеграции приложений ИС. Методы и средства организации метаинформации проекта ИС. Типовое проектирование ИС. Понятие типового элемента. Технологии параметрически-ориентированного и модельно-ориентированного проектирования. Автоматизированное проектирование ИС с использованием CASE-технологии. Функционально-ориентированный и объектно-ориентированный подходы. Содержание RAD- технологии прототипного создания</p>

№ п/п	Код и название компетенции	Ожидаемые результаты
		<p>приложений. Межсистемные интерфейсы и драйверы; интерфейсы в распределенных системах. Стандартные методы совместного доступа к базам и программам в сложных информационных системах</p> <p>Уметь: использовать стандартные методы совместного доступа к базам данных и программам в сложных ИС, разрабатывать и отлаживать эффективные алгоритмы и программы с использованием современных технологий программирования.</p> <p>Владеть: навыками выбора специального ПО, специальными средствами проектирования объектов информатизации на базе компьютерных систем в защищенном исполнении</p>

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

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 10
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)	41	41
Экзамен (при наличии)	45	45
ОБЩАЯ трудоемкость дисциплины, часы:	140	140
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.89	3.89
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

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 промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	10	Раздел 1 Введение Правовые основы обеспечения защиты информации.	2		2/2		2	6/2	
2	10	Раздел 2 Утечка информации по техническим каналам Технические каналы утечки информации. Технические средства минимизации ущерба от инцидентов.	2		2/1	1	4	9/1	
3	10	Раздел 3 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.	4		2/1		6	12/1	
4	10	Раздел 4 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-	4		2/1		7	13/1	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		методических и организационно-распорядительных документов организации по обеспечению безопасности информационных технологий. 2. Аппаратно-программные средства защиты информации от несанкционированного доступа. Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.							
5	10	Раздел 5 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).	4		2/1	1	6	13/1	ПК1, Устные опросы, доклады, % выполнения курсовой работы
6	10	Раздел 6 Аудит информационной безопасности 1. События безопасности, аудит. Мониторинг событий безопасности. 2. Стандартны и	6		2/1		4	12/1	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		критерии проведения аудита информационной безопасности. 3. Методология аудита информационной безопасности. Организация процесса аудита.							
7	10	Раздел 7 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.	6		2/1	1	4	13/1	
8	10	Раздел 8 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	4		2/1	1	4	11/1	ПК2, Устные опросы, доклады, % выполнения курсовой работы

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		компьютерной техники и носителей информации.							
9	10	Раздел 9 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		2/1		4	10/1	
10	10	Раздел 10 Курсовая работа						0	КР, Выполнение и защита курсовой работы
11	10	Экзамен						45	ЭК
12		Всего:	36		18/10	4	41	144/10	

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	10	РАЗДЕЛ 1 Введение	Практическое занятие №1 Вводное занятие. Техника безопасности в компьютерном классе.	2 / 2
2	10	РАЗДЕЛ 2 Утечка информации по техническим каналам	Практическое занятие №2 Доклады студентов по теме «Технические каналы утечки информации», «Технические средства минимизации ущерба от инцидентов».	2 / 1
3	10	РАЗДЕЛ 3 Информационные технологии.	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».	2 / 1
4	10	РАЗДЕЛ 4 Меры и средства защиты информации.	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».	2 / 1
5	10	РАЗДЕЛ 5 Безопасность в компьютерных системах и сетях	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».	2 / 1
6	10	РАЗДЕЛ 6 Аудит информационной безопасности	Практическое занятие №6 Доклады студентов по теме «Мониторинг событий безопасности», «Стандарты и критерии проведения аудита информационной безопасности», «Методология аудита информационной безопасности», «Организация процесса аудита».	2 / 1
7	10	РАЗДЕЛ 7 Техническая защита информации	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».	2 / 1

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
8	10	РАЗДЕЛ 8 Компьютерные инциденты	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».	2 / 1
9	10	РАЗДЕЛ 9 Методы аудирования.	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».	2 / 1
ВСЕГО:				18 / 10

4.5. Примерная тематика курсовых проектов (работ)

Примерные темы курсовой работы:

- 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.

Цель курсовой работы – закрепление знаний по курсу и развитие у обучающихся навыков самостоятельной творческой работы.

Курсовая работа должна иметь следующую структуру: титульный лист, содержание, введение, 3-4 тематических главы, заключение, список использованных источников. При необходимости добавления объемного иллюстративного материала (листинг программ, блок-схемы, объемные расчеты и т.п.) допускается одно или несколько приложений в конце. Объем работы должен составлять 15-45 страниц А4 при использовании шрифта Times New Roman 14 и полуторного междустрочного интервала.

Защита курсовой работы происходит в установленные преподавателем сроки в виде доклада с презентацией на 5-10 слайдов.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % 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. Часть практических работ, выполняемых с использованием ПЭВМ, подразумевает оформление соответствующего отчёта.

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 относятся 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. 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.

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	10	РАЗДЕЛ 1 Введение	<ol style="list-style-type: none"> 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 	2
2	10	РАЗДЕЛ 2 Утечка информации по техническим каналам	<ol style="list-style-type: none"> 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 	4
3	10	РАЗДЕЛ 3 Информационные технологии.	<ol style="list-style-type: none"> 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 	6
4	10	РАЗДЕЛ 4 Меры и средства защиты информации.	<ol style="list-style-type: none"> 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 	7
5	10	РАЗДЕЛ 5 Безопасность в компьютерных системах и сетях	<ol style="list-style-type: none"> 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети 	6

			«ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 6. Подготовка к первому текущему контролю (РИТМ МИИТ).	
6	10	РАЗДЕЛ 6 Аудит информационной безопасности	1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям.	4
7	10	РАЗДЕЛ 7 Техническая защита информации	1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям.	4
8	10	РАЗДЕЛ 8 Компьютерные инциденты	1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 6. Подготовка ко второму текущему контролю (РИТМ МИИТ).	4
9	10	РАЗДЕЛ 9 Методы аудирования.	1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [1], [2]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала. 5. Подготовка к практическим занятиям. 6. Подготовка к защите курсовой работы.	4
ВСЕГО:				41

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	В.П. Мельников, С.А. Клейменов, А.М. Петраков	Издательский центр "Академия", 2012 ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)	Все разделы
2	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта	В.В. Яковлев, А.А. Корниенко	УМК МПС России, 2002 НТБ (уч.4); НТБ (фб.); НТБ (чз.1)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства)	А.А. Корниенко, М.А. Еремеев, С.Е. Ададулов; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко	Маршрут, 2006 НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Википедия <http://ru.wikipedia.org/>

- Всё для студента twirpx.com

- ЭБС МИИТ library.miit.ru

<http://elibrary.ru/> - научно-электронная библиотека.

Поисковые системы: Yandex, Google, Mail.

Internet, сайты и порталы государственных структур (ФСТЭК России, ФСБ России) и компаний, деятельность которых направлена на проблемы информационной безопасности. Компьютерные презентации, актуальных для данной дисциплины, дипломных проектов выпускников кафедры по компьютерной безопасности.

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 2003, MathCAD 14.0 или другая система моделирования.

10. 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

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.

Организирующая; 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.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература. Обучающимся рекомендуется после каждой лекции изучать рекомендованную литературу по изучаемой тематике. Перед выполнением каждой практической работы необходимо прорабатывать теоретический материал и практическую часть. Курсовую работу рекомендуется выполнять поэтапно, регулярно демонстрируя процесс выполнения преподавателю. Рекомендуется защищать курсовую работу досрочно.