

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная  
безопасность»

Автор **Голдовский Яков Михайлович, к.т.н.**

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Комплексное обеспечение защиты объекта информатизации**

Направление подготовки:	<u>10.03.01 – Информационная безопасность</u>
Профиль:	<u>Безопасность компьютерных систем</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2019</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</p>
---	--

Рабочая программа учебной дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)  
ID подписи: 4196  
Подписал: Заведующий кафедрой Желенков Борис Владимирович  
Дата: 27.09.2019

Москва 2019 г.

## 1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Комплексное обеспечение защиты объекта информатизации» являются формирование у студентов целостных представлений о всестороннем обеспечении защиты различных объектов информатизации.

Основными задачами дисциплины являются:

- изучение принципов и общих методов обеспечения информационной безопасности;
- изучение функциональных возможностей и предпосылок эффективного применения различных типов технологических систем и способов обработки и хранения конфиденциальных документов;
- изучение механизмов решения типовых задач программно-аппаратной защиты информации;
- практика выявления угроз информационной безопасности применительно к объектам защиты.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Эксплуатационная деятельность:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов

Экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств

Организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

## **2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО**

Учебная дисциплина "Комплексное обеспечение защиты объекта информатизации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

### **2.1. Наименования предшествующих дисциплин**

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

#### **2.1.1. Основы информационной безопасности :**

**Знания:** Базовый понятийный аппарат в области информационной безопасности и защиты информации; виды и состав угроз информационной безопасности; принципы и общие методы обеспечения информационной безопасности; основные положения государственной политики обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; виды носителей защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; классификацию видов, методов и средств защиты информации;

**Умения:** Выявлять угрозы информационной безопасности применительно к объектам защиты; определять состав защищаемой информации применительно к видам тайны; выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;

**Навыки:** Основные методикам проверки защищенности объектов информатизации на соответствие нормам информационной безопасности.

#### **2.1.2. Основы управления информационной безопасностью:**

**Знания:** место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

**Умения:** анализировать и оценивать угрозы информационной безопасности объекта;

**Навыки:** Владение методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; профессиональной терминологией.

#### **2.1.3. Программно-аппаратные средства защиты информации:**

**Знания:** основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак; основные принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях; сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации; средства и методы защиты от НСД хранимой информации с использованием возможностей устройств записи и чтения; принципы

функционирования основных типов вредоносных программ, способы их выявления и нейтрализации;

Умения: оценивать эффективность и надежность защиты ОС, ВС и СУБД; выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты; планировать программно-аппаратную подсистему политики безопасности организации; применять и администрировать средства программно-аппаратной защиты информации;

Навыки: навыки анализа и администрирования подсистем защиты современных ОС, ВС и СУБД; навыки использования межсетевых экранов и систем обнаружения вторжений.

## **2.2. Наименование последующих дисциплин**

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

### **2.2.1. Государственная итоговая аттестация**

### 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	ОПК-8 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-8.1 Знать меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. ОПК-8.2 Уметь формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. ОПК-8.3 Владеть навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
2	ПКО-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;	ПКО-4.1 Знать виды комплексного подхода в организации политики информационной безопасности. ПКО-4.2 Уметь формулировать, настраивать политики безопасности. ПКО-4.3 Владеть навыками формулирования и контролирования соблюдения требований политики безопасности.
3	ПКО-13 Способность осуществлять совершенствование системы управления информационной безопасностью.	ПКО-13.1 Знать тенденции развития угроз информационной безопасности. ПКО-13.2 Уметь анализировать уязвимости системы информационной безопасности. ПКО-13.3 Владеть навыками совершенствования системы управления информационной безопасностью на основе анализа угроз и текущего состояния системы информационной безопасности.

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

##### 4.1. Общая трудоемкость дисциплины составляет:

4 зачетных единиц (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 8
Контактная работа	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	24	24
практические (ПЗ) и семинарские (С)	24	24
Самостоятельная работа (всего)	42	42
Экзамен (при наличии)	54	54
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	КП (1), ПК1
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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	8	Раздел 1 Теория информационной безопасности и методология защиты информации.	5				4	9	
2	8	Тема 1.1 Информация как предмет защиты. Сущность и понятие информационной безопасности. Значение информационной безопасности и ее место в системе национальной безопасности. Современная доктрина информационной безопасности Российской Федерации. Понятие и назначение доктрины информационной безопасности.	2				4	6	
3	8	Тема 1.2 Сущность и понятие защиты информации. Цели и значение защиты информации. Теоретические и концептуальные основы защиты информации. Понятие и назначение теории защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайны.	2					2	
4	8	Тема 1.3 Понятие и назначение теории защиты информации. Критерии, условия и принципы отнесения информации к защищаемой.	1					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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Классификация конфиденциальной информации по видам тайны..							
5	8	Раздел 2 Правовое обеспечение информационной безопасности	4		6		4	14	
6	8	Тема 2.1 Назначение и структура правового обеспечения защиты информации. Правовые нормы и методы обеспечения правовой защиты информации. Основные законодательные акты, содержащие правовые нормы, направленные на защиту информации. Правовая защита открытой, общедоступной информации.	2		6		4	12	
7	8	Тема 2.2 Информация ограниченного доступа Государственная система правовой защиты государственной тайны. Особенности правовой защиты различного вида тайн. Правовое обеспечение безопасности информационных и телекоммуникационных систем.	2					2	
8	8	Раздел 3 Защита и обработка конфиденциальных документов	3		6		4	13	
9	8	Тема 3.1 Технология конфиденциального документооборота. Стадии обработки и защиты конфиденциальных документов входного потока. Стадии обработки и защиты конфиденциальных	2		6		4	12	ПК1, выполнение практических работ №1-2

№ 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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		документов выходного потока.							
10	8	Тема 3.2 Систематизация и оперативное хранение конфиденциальных документов и дел. Проверка наличия конфиденциальных документов, дел и носителей информации.	1					1	
11	8	Раздел 4 Организационное обеспечение информационной безопасности	2				4	6	, выполнение практических работ №3-4
12	8	Тема 4.1 Политика информационной безопасности предприятия. Работа с персоналом, допущенным к конфиденциальной информации. Организационная защита информации в процессе проведения совещаний и переговоров по конфиденциальным вопросам. Организация защиты информации в автоматизированных информационных системах, обрабатывающих конфиденциальную информацию.	1				4	5	
13	8	Тема 4.2 Организация защиты информации в автоматизированных информационных системах, обрабатывающих конфиденциальную информацию	1					1	
14	8	Раздел 5 Инженерно-техническая защита информации.	2		6		8	16	
15	8	Тема 5.1 Объекты	1		6		8	15	

№ 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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		информационной безопасности. Угрозы безопасности информации. Способы и средства добывания информации техническими средствами. Технические каналы утечки информации.							
16	8	Тема 5.2 Методы, способы и средства инженерно-технической охраны объекта. Способы и средства защиты информации от наблюдения. Способы и средства защиты информации от подслушивания. Основы методического обеспечения инженерно-технической защиты информации.	1					1	
17	8	Раздел 6 Криптографические методы и средства обеспечения информационной безопасности.	2		6		6	14	
18	8	Тема 6.1 Основные задачи современной криптографии. Шифры перестановки, шифры замены, шифры гаммирования. Блочные и поточные системы шифрования. Системы шифрования с открытыми ключами. Электронные цифровые подписи.	1		6		6	13	
19	8	Тема 6.2 Основные задачи современной криптографии. Шифры перестановки, шифры замены, шифры гаммирования. Блочные и поточные системы шифрования. Системы шифрования с	1					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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		открытыми ключами. Электронные цифровые подписи.							
20	8	Раздел 7 Программно-аппаратная защита информации и защита информационных процессов в компьютерных системах.	3				6	9	
21	8	Тема 7.1 Информационная безопасность Модели типовых политик безопасности компьютерных средств защиты информации. Проектирование средств реализации механизмов безопасности на аппаратном уровне. Программно-аппаратные средства идентификации и аутентификации пользователей.	1				6	7	
22	8	Тема 7.2 Программно-аппаратные средства идентификации и аутентификации пользователей.	2					2	
23	8	Раздел 8 Комплексная защита информации на предприятии.	3				6	9	
24	8	Тема 8.1 Сущность и задачи комплексной системы защиты информации (КСЗИ). Принципы организации КСЗИ. Технология организации КСЗИ. Разработка модели КСЗИ. Обеспечение функционирования КСЗИ.	2				6	8	
25	8	Тема 8.2 Назначение, структура и содержание управления КСЗИ.	1					1	

№ 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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Технология управления КСЗИ. правление КСЗИ в условиях чрезвычайных ситуаций. Сущность и содержание контроля функционирования КСЗИ.							
26	8	Экзамен						54	КП, ЭК
27		Всего:	24		24		42	144	

#### 4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 24 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	8	РАЗДЕЛ 2 Правовое обеспечение информационной безопасности Тема: Назначение и структура правового обеспечения защиты информации.	Практическое занятие №1.  Информационный характер процесса управления машиностроительным производством	6
2	8	РАЗДЕЛ 3 Защита и обработка конфиденциальных документов Тема: Технология конфиденциального документооборота.	Практическое занятие №2.  Тест-опрос по сущности комплексной защиты информации	6
3	8	РАЗДЕЛ 5 Инженерно-техническая защита информации. Тема: Объекты информационной безопасности.	Практическое занятие №3.  Определение оценки вероятности реализации угроз	6
4	8	РАЗДЕЛ 6 Криптографические методы и средства обеспечения информационной безопасности. Тема: Основные задачи современной криптографии.	Практическое занятие №4.  Обеспечение безопасности информационного объекта	6
ВСЕГО:				24/0

#### 4.5. Примерная тематика курсовых проектов (работ)

Тема курсового проекта: Комплексная система защиты информации на предприятии. Объектом исследования настоящего курсового проекта является вымышленная, в учебных целях организация. Например, общество с ограниченной ответственностью «Кредит Коллектор».

Исходными данными для курсового проектирования служит некоторый вариант задания, отражающий в себе характеристики исследуемого объекта (выдает преподаватель).

Цели курсового проекта:

1. Спроектировать комплексную систему защиты информации на конкретном предприятии, отвечающую требованиям надзирающих органов и обладающую свойствами комплексности, системности и достаточности;
2. Оценить эффективность спроектированной системы.

Для достижения целей проекта необходимо выполнить следующие задачи:

1. Провести анализ объекта информатизации, т.е. определить входные данные для построения комплексной системы защиты информации;

Основными категориями входных данных для построения КСЗИ являются:

- правовая информация об объекте;
- организационное устройство объекта, включая систему менеджмента и внутренних процессов;
- информация о местонахождении объекта, его физических особенностях;
- информация о человеческих ресурсах на предприятии;
- информация об исходной защищённости объекта.

2. На базе проведённого анализа разработать следующую документацию:

- перечень сведений конфиденциального характера;
- политика информационной безопасности;
- положение о коммерческой тайне;
- инструкция по организации охраны и пропускного режима;
- частная модель угроз информационной безопасности;
- неформальная модель нарушителя.

3. Спроектировать следующие подсистемы технической защиты информации:

- подсистему контроля и управления доступом;
- подсистему видеонаблюдения;
- подсистему охранной и пожарной сигнализаций;
- подсистему противодействия утечки по техническим каналам;
- подсистему защиты корпоративной сети;

4. Провести анализ эффективности спроектированной системы и сделать выводы по необходимости её внедрения.

Для выполнения изложенных выше задач будет использован комплексный подход.

Разработка каждой подсистемы, технической и организационной систем будут

согласованы в области организационной, методической и технической совместимости

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Комплексное обеспечение защиты объекта информатизации» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 24 часа, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).

Практические занятия (24 часа) проводятся с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения.

Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (38 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 8 раздела, представляющих собой логически завершённый объем 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 путем 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	8	РАЗДЕЛ 1 Теория информационной безопасности и методология защиты информации. Тема 1: Информация как предмет защиты.	- проработка учебного материала; подготовка к практическим занятиям.[1 стр. 3-60], [3 стр. 19-40]	4
2	8	РАЗДЕЛ 2 Правовое обеспечение информационной безопасности Тема 1: Назначение и структура правового обеспечения защиты информации.	- проработка учебного материала; подготовка к практическим занятиям.[2 стр. 3-20] , [3 стр. 55-62]	4
3	8	РАЗДЕЛ 3 Защита и обработка конфиденциальных документов Тема 1: Технология конфиденциального документооборота.	- проработка учебного материала; подготовка к практическим занятиям. [1 стр. 71-80] , [4 стр. 4-12]	4
4	8	РАЗДЕЛ 4 Организационное обеспечение информационной безопасности Тема 1: Политика информационной безопасности предприятия.	- проработка учебного материала; подготовка к практическим занятиям.[2 стр.24-30] , [5 стр. 3-16]	4
5	8	РАЗДЕЛ 5 Инженерно-техническая защита информации. Тема 1: Объекты информационной безопасности.	- проработка учебного материала; подготовка к практическим занятиям.[1 стр. 100-110] , [3 стр. 70-86]	8
6	8	РАЗДЕЛ 6 Криптографические методы и средства обеспечения информационной безопасности. Тема 1: Основные задачи современной криптографии.	- проработка учебного материала; подготовка к практическим занятиям.[2 стр. 40-57] , [3 стр. 90-98]	6
7	8	РАЗДЕЛ 7 Программно-аппаратная защита информации и защита	- проработка учебного материала; подготовка к практическим занятиям.[1 стр.110-115] , [4 стр. 18-30]	6

		информационных процессов в компьютерных системах. Тема 1: Информационная безопасность		
8	8	РАЗДЕЛ 8 Комплексная защита информации на предприятии. Тема 1: Сущность и задачи комплексной системы защиты информации (КСЗИ).	- проработка учебного материала; подготовка к практическим занятиям.[2 стр.70-76] , [5 стр. 24-48]	6
ВСЕГО:				42

## 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	Защита от вирусов, межсетевые экраны и другие механизмы обеспечения безопасности информационных систем [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех."	Соловьев Владимир Павлович	М. : МИИТ, 2007 НТБ МИИТ	Все разделы
2	Методы предотвращения и обнаружения вторжений [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех."	Соловьев Владимир Павлович	М. : МИИТ, 2007 НТБ МИИТ	Все разделы
3	Безопасность операционных систем [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех."	Соловьев Владимир Павлович	М. : МИИТ, 2007 НТБ МИИТ	Все разделы

### 7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Защищенные беспроводные и мобильные коммуникации [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех."	Соловьев Владимир Павлович	М. : МИИТ, 2007 НТБ МИИТ	Все разделы
5	Безопасность коммуникационных сетей [Текст] : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита инф-ции" напр. "Информатика и выч. тех."	Соловьев Владимир Павлович	М. : МИИТ, 2007 НТБ МИИТ	Все разделы

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

- Форум специалистов по информационным технологиям <http://citforum.ru/>
- Интернет-университет информационных технологий <http://www.intuit.ru/>
- Тематический форум по информационным технологиям <http://habrahabr.ru/>

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

Microsoft Windows  
 Microsoft Office  
 Microsoft Windows  
 Microsoft Office

## **10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

№1329

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

№1327

10 персональных компьютера, 10 монитора, проектор, маркерная доска.

## **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:

- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- 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, знание основ надежности подвижного состава, 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 семестровый план 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 работы. 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 зачету и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является 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.