МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Выпускающая кафедра УТБиИС	Первый проректор
Заведующий кафедрой УТБиИС	
С.П. Вакуленко	В.С. Тимонин
28 июня 2019 г.	18 апреля 2022 г.

Кафедра «Вычислительные системы и сети»

Автор Шамров Михаил Иванович, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Компьютерная безопасность

Направление подготовки:	38.03.02 – Менеджмент
Профиль:	Транспортный бизнес и логистика
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 1 25 июня 2019 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 12 24 июня 2019 г. И.о. заведующего кафедрой Б.В. Желенков

Москва 2022 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Компьютерная безопасность» являются изучение студентами основных понятий информационной безопасности, изучение основных видов угроз информационной безопасности; получение представления об организации и принципах обеспечения информационной безопасности; знакомство с основами методов криптографического закрытия данных; получение навыков разработки политики безопасности предприятия.
Основными задачами дисциплины являются:
• освоение методов оценки степени угрозы информационной безопасности;
• изучение использования соответствующих методов защиты.;
• рассмотрение методов организации комплексной системы защиты информации;
• изучение студентами основных угроз информационной безопасности и методов защиты от них.

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

Организационно-управленческая деятельность:
• оценки степени угрозы информационной безопасности;
• участие в разработке организационно-технической документации (графиков работ, инструкций, планов, смет) и установленной отчетности по утвержденным формам.

Предпринимательская деятельность:
• безопасное использование глобальных компьютерных сетей;
• применение защищенной электронной коммерции;
• безопасное использование электронной почты;

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Компьютерная безопасность" 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. Информатика:

Знания: основные методы, способы и средства получения, хранения и переработки информации

Умения: работать с ин-формацией в глобаль-ных компьютерных сетях

Навыки: навыками работы с компьютером как средством управления информацией

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Информационные технологии в транспортных системах

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-4 способностью осуществлять деловое общение и публичные выступления, вести переговоры, совещания, осуществлять деловую переписку и поддерживать электронные коммуникации;	Знать и понимать: Принципы защиты данных, при осуществлении коммуникации с применением информационных технологий Уметь: применять известные методы и средства поддержки информационной безопасности в компьютерных системах, используемых при осуществлении деловой переписки и обмене данными Владеть: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
2	ОПК-7 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Знать и понимать: принципы работы с информацией, организацию поисковых систем. Уметь: использовать информационные системы для поиска необходимой информации, анализировать полученные данные. Владеть: основными методами получения обработки и хранения информации.
3	ПК-6 способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений.	Знать и понимать: разновидности алгоритмов шифровки информации Уметь: обосновать целесообразность внедрения конкретного алгоритма защиты информации в существующий бизнесс-процесс Владеть: базовыми нывыками симметричного шифрования информации и навыками шифрования открытым ключом

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

4.1. Общая трудоемкость дисциплины составляет:

2 зачетные единицы (72 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 3
Контактная работа	28	28,15
Аудиторные занятия (всего):	28	28
В том числе:		
лекции (Л)	14	14
практические (ПЗ) и семинарские (С)	14	14
Самостоятельная работа (всего)	44	44
ОБЩАЯ трудоемкость дисциплины, часы:	72	72
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	2.0	2.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗЧ	ЗЧ

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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	3	Раздел 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Работа с основной и дополнительной литературой [1],[2],[3], а также с периодическими изданиями на сайте http://elibrary.ru/	6/2		3		4	13/2	
2	3	Тема 1.1 Классификация криптографических алгоритмов. Классификация криптографических алгоритмов. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы.	2		1		1	4	
3	3	Тема 1.2 Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.	2/2		1		2	5/2	
4	3	Тема 1.3 Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и	2		1		1	4	ПК1, Контрольная работа

№ 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
		недостатки асимметричного шифрования и область его применения. Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.							
5	3	Раздел 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Работа с основной и дополнительной литературой [1],[2],[3], а также с периодическими изданиями на сайте http://elibrary.ru/	6/2		4/1		14	24/3	
6	3	Тема 2.1 Аутентификация, авторизация и администрирование действий пользователей. Аутентификация, авторизация и администрирование действий пользователей.	2/2		1/1		1	4/3	
7	3	Тема 2.2 Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.	4		3		13	20	
8	3	Тема 2.2.3 Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	2		2		7	11	
9	3	Раздел 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Работа с основной и дополнительной литературой [1],[2],[3], а также с	2/2		7/7		26	35/9	

№ 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
		периодическими изданиями на сайте http://elibrary.ru/							
10	3	Тема 3.1 Защита http-трафика. Характерные угрозы. Защищенный протокол httpd. Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.					19	19	
11	3	Тема 3.2 Цифровые сертификаты.. Виртуальная частная сеть. Цифровые сертификаты.. Виртуальная частная сеть.	2/2		2/2		4	8/4	ПК2, Контрольная работа
12	3	Тема 3.3 Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec. Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.			5/5		3	8/5	
13	3	Зачет						0	ЗЧ
14		Всего:	14/6		14/8		44	72/14	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 14 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	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема: Классификация криптографических алгоритмов.	ПЗ 1 Шифрование и дешифровка	1
2	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема: Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.	ПЗ 2 Шифрование и дешифровка	1
3	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема: Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.	ПЗ 3 Шифрование и дешифровка	1
4	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема: Аутентификация, авторизация и администрирование действий пользователей.	ПЗ 1 Защита от несанкционированного доступа	1 / 1
5	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема: Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.	ПЗ 2 Защита от несанкционированного доступа	1

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
6	3	РАЗДЕЛ 2 Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА. Тема: Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	ПЗ 3 Защита от несанкционированного доступа	2
7	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема: Цифровые сертификаты.. Виртуальная частная сеть.	ПЗ 2 Защита информации в глобальной сети.	2 / 2
8	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема: Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.	ПЗ 3 Защита информации в глобальной сети.	5 / 5
			ВСЕГО:	14/8

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Проведение занятий по дисциплине «Компьютерная безопасностьг» осуществляется в форме лекций и практических занятий.
Лекции являются традиционными классически-лекционными с использованием презентаций.
Практические занятия организованы с использованием технологий развивающего обучения.
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 для оценки умений и навыков.

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	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема 1: Классификация криптографических алгоритмов.	СР 1 1. Шифрование и дешифровка сообщений. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.19-24], [2 стр. 25-32], [3, стр. 1-3].	1
2	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема 2: Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.	СР 2 1. Шифрование и дешифровка сообщений. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.19-24], [2 стр. 25-32], [3, стр. 1-3].	2
3	3	РАЗДЕЛ 1 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА Тема 3: Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.	СР 3 1. Шифрование и дешифровка сообщений. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.19-24], [2 стр. 25-32], [3, стр. 1-3].	1
4	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.	Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.	5
5	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема 1: Аутентификация, авторизация и администрирование действий пользователей.	СР 1 1. Шифрование и дешифровка сообщений. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из	1

			приведенных источников: [1, стр.19-24], [2 стр. 25-32], [3, стр. 1-3].	
6	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема 2: Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА.	СР 2 1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	1
7	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема 2: Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА.	Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	4
8	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема 2: Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА.	СР 2 1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	1
9	3	РАЗДЕЛ 2 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. Тема 2: Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА.	Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	4
10	3	РАЗДЕЛ 2 Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА. Тема 3: Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	СР 3 1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	3
11	3	РАЗДЕЛ 2 Основные принципы системы ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА. Тема 3: Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	СР 3 1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	3

12	3	РАЗДЕЛ 2 Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA. Тема 3: Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.	СР 3 1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	3
13	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.	Защита http-трафика. Характерные угрозы. Защищенный протокол httpd. Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.	15
14	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 1: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.	СР 1 1. Обзор стандартов рамочного протокола IPSec. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3].	1
15	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 1: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.	ПЗ 1 Защита информации в глобальной сети.	3
16	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 1: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.	СР 1 1. Обзор стандартов рамочного протокола IPSec. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3].	1
17	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 1: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.	ПЗ 1 Защита информации в глобальной сети.	3
18	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 2: Цифровые сертификаты.. Виртуальная частная сеть.	СР 2 1. Обзор стандартов рамочного протокола IPSec. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3].	4

19	3	РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. Тема 3: Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.	СР 3 1. Обзор стандартов рамочного протокола IPSec. 2. Анализ и дополнительная проработка материала. 3. Подготовка к практическим занятиям. 4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3].	3
			ВСЕГО:	59

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	Криптографическая защита компьютерной информации	Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова	М.:МИИТ, Электронная библиотека МИИТ 36 с, 2013 НТБ МИИТ	Разделы 1-3
2	Канальный уровень модели OSI	Б.В. Желенков	М.:МИИТ,49 с, Электронная библиотека МИИТ, 2011 НТБ МИИТ	Разделы 1-3

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Защита информации в вычислительных системах	В.И. Морозова, К.Э. Врублевский	М.:МИИТ,122 с,Электронная библиотека МИИТ, 2008 НТБ МИИТ	Разделы 1-3

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

1. http://library.miit.ru/
2. http://www.edu.ru/
3. http://elibrary.ru/
4. http://www.fgosvpo.ru/
5. http://www.rzd.ru/

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

Для подготовки материалов лекционных и практических занятий требуется использование пакета программ Microsoft Office.
Для демонстрации презентационных материалов на лекционных и практических занятиях на компьютере (ноутбуке) в аудитории должен быть установлен стандартный лицензионный пакет программ Microsoft Office.

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

1. Лекционные аудитории, должны быть оснащены мультимедийным оборудованием: проектором или интерактивной доской для демонстрации презентаций, компьютером или ноутбуком.
2. Аудитория для лабораторных работ (вместимостью не менее 20 посадочных мест) должны быть оборудованы маркерной или меловой доской, а при наличии технической возможности - мультимедийным оборудованием: проектором или интерактивной доской для демонстрации презентаций, компьютером или ноутбуком.
3. Научно-техническая библиотека РУТ (МИИТ) и/или аудитории для самостоятельной работы студентов. Аудитория для самостоятельной работы студентов должна быть оборудована рабочими местами (столы и стулья), не менее чем 2 компьютерами или ноутбука с подключением к сети Интернет. На компьютерах (ноутбуках) в аудитории должен быть установлен стандартный лицензионный пакет программ Microsoft Office.

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 бакалаврами 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 выпускников.
При подготовке студентов важны не только серьезная теоретическая подготовка, знание основ изучаемого предмета, 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.
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.