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 Цыганова Наталия Алексеевна

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Комплексное обеспечение защиты объекта информатизации

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии  Н.А. Клычева	Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой  Б.В. Желенков

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 бе¬зопасности;
? изучение функциональных возможностей и предпосылкок эффективного применения различных типов технологических систем и спо¬собов обработки и хранения конфиденциальных документов;
? изучение механизмов решения типовых задач программно-аппаратной защиты информации;
? практика выявления угроз информационной безопасности применитель¬но к объектам защиты.

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

Эксплуатационная:
- 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

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-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать и понимать: понятийный аппарат информационной безопасности основные направления обеспечения информационной безопасности основные угрозы информационной безопасности основные источники информационной безопасности основные методы обеспечения информационной безопасности основные средства защиты информации Уметь: обосновывать выбор технических средств обеспечения информационной безопасности обосновывать меры обеспечения информационной безопасности в соответствии с законодательством РФ определять виды информации подверженные атакам потенциального злоумышленника выявлять потенциальные каналы утечки информации применять программные и аппаратные средства защиты информации Владеть: методологией выбора информационных ресурсов, подлежащий защите
2	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать и понимать: научно-техническую литературу, нормативные и методические материалы Уметь: решать задачи, связанные с подбором, изучением и обобщением полученной информации Владеть: навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

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

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 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 8
Контактная работа	36	36,15
Аудиторные занятия (всего):	36	36
В том числе:		
лекции (Л)	18	18
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	36	36
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1	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 промежу-точной 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.	3		3/2		4	10/2	
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.	1		1		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		2/2			4/2	
4	8	Раздел 2 Правовое обеспечение информационной безопасности	3		3/2		4	10/2	
5	8	Тема 2.1 Назначение и структура правового обеспечения	1		1		4	6	

№ 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
		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.							
6	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		2/2			4/2	
7	8	Раздел 3 Защита и обработка конфиденциальных документов	3		3/2		6	12/2	
8	8	Тема 3.1 Технология конфиденциального документооборота. Стадии обработки и защиты конфиденциальных документов входного потока. Стадии обработки и защиты конфиденциальных документов выходного потока.	1		1		6	8	ПК1, выполнение практических рарот №1-4
9	8	Тема 3.2 Систематизация и оперативное хранение конфиденциальных документов и дел. Проверка наличия конфиденциальных документов, дел и носителей информации.	2		2/2			4/2	

№ 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
10	8	Раздел 4 Организационное обеспечение информационной безопасности	1		1		4	6	
11	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		1		4	6	
12	8	Раздел 5 Инженерно-техническая защита информации.	3		3/2		4	10/2	
13	8	Тема 5.1 Объекты информационной безопасности. Угрозы безопасности информации. Способы и средства добывания информации техническими средствами. Технические каналы утечки информации.	1		1/2		4	6/2	
14	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.	2		2			4	

№ 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
		Основы методического обеспечения инженерно-технической защиты информации.							
15	8	Раздел 6 Криптографические методы и средства обеспечения информационной безопасности.	1		1/2		4	6/2	
16	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		1/2		4	6/2	
17	8	Раздел 7 Программно-аппаратная зашита информации и защита информационных процессов в компьютерных системах.	1		1		4	6	
18	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		1		4	6	
19	8	Раздел 8 Комплексная зашита информации на предприятии.	3		3/3		6	12/3	
20	8	Тема 8.1	1		2/2		6	9/2	

№ 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
		Сущность и задачи комплексной системы защиты информации (КСЗИ). Принципы организации КСЗИ. Технология организации КСЗИ. Разработка модели КСЗИ. Обеспечение функционирования КСЗИ.							
21	8	Тема 8.2 Назначение, структура и содержание управления КСЗИ. Технология управления КСЗИ. правление КСЗИ в условиях чрезвычайных ситуаций. Сущность и содержание контроля функционирования КСЗИ.	2		1/1			3/1	
22	8	Экзамен						36	ЭК
23		Всего:	18		18/13		36	108/13	

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	8	РАЗДЕЛ 1 Теория информационной безопасности и методология защиты информации. Тема: Информация как предмет защиты.	Сущность информационной безопасности. Объекты информационной безопасности.	1
2	8	РАЗДЕЛ 1 Теория информационной безопасности и методология защиты информации. Тема: Сущность и понятие защиты информации.	Понятие целей защиты, информации, их отличие от задач защиты информации. Увязка целей защиты информации с защищаемой информацией и субъектами информационных отношений.	2 / 2
3	8	РАЗДЕЛ 2 Правовое обеспечение информационной безопасности Тема: Назначение и структура правового обеспечения защиты информации.	Правовое определение информации. Правовые последствия документирования информации. Доктрина информационной безопасности.2	1
4	8	РАЗДЕЛ 2 Правовое обеспечение информационной безопасности Тема: Информация ограниченного доступа	Особенности организации правовой защиты различного вида тайн. Основные нормативно-правовые документы по защите различных видов информации ограниченного доступа.	2 / 2
5	8	РАЗДЕЛ 3 Защита и обработка конфиденциальных документов Тема: Технология конфиденциального документооборота.	Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены в документопотоках.	1
6	8	РАЗДЕЛ 3 Защита и обработка конфиденциальных документов Тема: Систематизация и оперативное хранение конфиденциальных документов и дел.	Назначение и задачи стадии формирования и оперативного хранения дел.	2 / 2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
7	8	РАЗДЕЛ 4 Организационное обеспечение информационной безопасности Тема: Политика информационной безопасности предприятия.	Концепция информационной безопасности предприятия. Структура и требования по информационной безопасности предприятия.	1
8	8	РАЗДЕЛ 5 Инженерно-техническая защита информации. Тема: Объекты информационной безопасности.	Понятие объекта защиты и его структурное представление. Демаскирующие признаки объектов защиты и их классификация.	1 / 2
9	8	РАЗДЕЛ 5 Инженерно-техническая защита информации. Тема: Методы, способы и средства инженерно-технической охраны объекта.	Концепция инженерно-технической защиты информации. Способы и средства технической охраны.	2
10	8	РАЗДЕЛ 6 Криптографические методы и средства обеспечения информационной безопасности. Тема: Основные задачи современной криптографии.	Конфиденциальность. Целостность. Аутентификация. Неотслеживаемость. Цифровая подпись. Управление ключами. Общие требования к криптосистемам.	1 / 2
11	8	РАЗДЕЛ 7 Программно-аппаратная зашита информации и защита информационных процессов в компьютерных системах. Тема: Информационная безопасность	Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в КС.	1
12	8	РАЗДЕЛ 8 Комплексная зашита информации на предприятии. Тема: Сущность и задачи комплексной системы защиты информации (КСЗИ).	Назначение и общее содержание КСЗИ. Основные задачи КСЗИ. Факторы, влияющие на организацию КСЗИ.	2 / 2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
13	8	РАЗДЕЛ 8 Комплексная зашита информации на предприятии. Тема: Назначение, структура и содержание управления КСЗИ.	Понятие и цели управления КСЗИ. Сущность процессов управления. Принципы управления службой защиты информации.	1 / 1
			ВСЕГО:	18/13

4.5. Примерная тематика курсовых проектов (работ)

Учебным планом не предусмотрено.

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, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративные).
Практические занятия организованы с использованием технологий развивающего обучения. Проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, (решение проблемных поставленных задач с помощью современной вычислительной техники и анализа статистических данных).
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 относится отработка отдельных тем по пособиям, подготовка к текущему и промежуточному контролю, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 8 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (анализ конкретных ситуаций, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения ситуационных задач, решение тестов с использованием компьютеров или на бумажных носителях.

Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.
В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):
- использование современных средств коммуникации;
- электронная форма обмена материалами;
- дистанционная форма групповых и индивидуальных консультаций;
- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д.

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]	6
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]	4
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]	4
7	8	РАЗДЕЛ 7 Программно-аппаратная зашита информации и защита	- проработка учебного материала; подготовка к практическим занятиям.[1 стр.110-115] , [4 стр. 18-30]	4

		информационных процессов в компьютерных системах. Тема 1: Информационная безопасность		
8	8	РАЗДЕЛ 8 Комплексная зашита 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:	36

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	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	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	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	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	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
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014
Microsoft Windows
Microsoft Office
Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

Putty
Бесплатноеиспользование (MIT)

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».
В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.
В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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.
В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.
Допускается замена оборудования его виртуальными аналогами.

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.