МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Выпускающая кафедра ЭЭТ	Директор ИТТСУ
Заведующий кафедрой ЭЭТ	
М.В. Шевлюгин	П.Ф. Бестемьянов
16 мая 2018 г.	25 мая 2018 г.

Кафедра «Машиноведение, проектирование, стандартизация и сертификация»

Автор Козлов Виктор Владимирович, к.т.н.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы компьютерной безопасности

Направление подготовки:	27.03.01 – Стандартизация и метрология
Профиль:	Метрология и метрологическое обеспечение
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии С.В. Володин	Протокол № 10 15 мая 2018 г. Заведующий кафедрой В.А. Карпычев

Москва 2018 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Основы компьютерной безопасности» (Б1.В.ДВ.8.2) является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение основам информационной безопасности, принципам и методам защиты информации в информационных системах.
Основные задачи можно сформулировать следующим образом:
1.изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в информационных системах;
2.изучение типовых угроз безопасности информации при её обработке в информационных системах;
3.изучение основных принципов обеспечения информационной безопасности;
4.изучение основ построения модели угроз и политики безопасности;
5.?изучение основных моделей доступа.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Основы компьютерной безопасности" 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. Алгоритмические языки программирования высокого уровня:

Знания:

Умения:

Навыки:

2.1.2. Информатика:

Знания:

Умения:

Навыки:

2.1.3. Математика:

Знания:

Умения:

Навыки:

2.1.4. Электротехника и электроника:

Знания:

Умения:

Навыки:

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	ПК-18 способностью изучать научно-техническую информацию, отечественный и зарубежный опыт в области метрологии, технического регулирования и управления качеством	Знать и понимать: основные угрозы информационной безопасности. основные методы обеспечения безопасности информационных систем; Уметь: разрабатывать базовые документы, регулирующие аспекты информационной безопасности; ?составлять модель угроз для информационной системы. Владеть: навыками разработки нормативных документов, обеспечивающих защиту данных в информационных системах.
2	ПК-19 способностью принимать участие в моделировании процессов и средств измерений, испытаний и контроля с использованием стандартных пакетов и средств автоматизированного проектирования	Знать и понимать: основные принципы построения систем автоматизированного проектирования (САПР); Уметь: назначение основных подсистем САПР (CAD, CAE, CAM, PDM); особенности пользовательского интерфейса подсистем САПР. Владеть: создавать компьютерную модель объекта исследования; • исследовать модель с применением основных подсистем САПР.
3	ПК-20 способностью проводить эксперименты по заданным методикам с обработкой и анализом результатов, составлять описания проводимых исследований и подготавливать данные для составления научных обзоров и публикаций	Знать и понимать: теоретические основы и методы проведения эксперимента; основы планирования и организации эксперимента. Уметь: на практике использовать различные технические и информационные средства для обеспечения экспериментальных исследований. Владеть: навыками работы с офисными приложениями Microsoft; навыками работы со специализированными пакетами прикладных программ.

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 6
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)	72	72
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 Введение в теорию информационной безопасности.	6		11/6		20	37/6	
2	6	Тема 1.1 Основные понятия теории информационной безопасности.	2		4/2		6	12/2	, Опрос на практическом занятии (ПРЗ)
3	6	Тема 1.2 Классификация угроз информационной безопасности.	2		4/2		7	13/2	
4	6	Тема 1.3 Основные механизмы обеспечения информационной безопасности.	2		3/2		7	12/2	
5	6	Раздел 2 Подходы к обеспечению информационной безопасности.	6		4/3		22	32/3	
6	6	Тема 2.1 Теоретический подход к обеспечению информационной безопасности.	2		1		6	9	
7	6	Тема 2.2 Нормативно-правовой подход к обеспечению информационной безопасности.	2		1/1		6	9/1	
8	6	Тема 2.3 Практический (экспериментальный) подход к обеспечению информационной безопасности.	2		2/2		10	14/2	ПК1, Опрос на ПРЗ собеседование
9	6	Раздел 3 Обеспечение и оценка эффективности системы защиты информационных систем.	6		3		30	39	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
10	6	Тема 3.1 Построение модели угроз.	2		1		10	13	
11	6	Тема 3.2 Определение и разработка политики безопасности.	2		1		10	13	
12	6	Тема 3.3 Аудит информационной безопасности.	2		1		10	13	ЗЧ, ПК2, Опрос на ПРЗ, ПК2, зачет
13		Всего:	18		18/9		72	108/9	

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	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема: Основные понятия теории информационной безопасности.	Определение субъектов и объектов безопасности в информационной системе. Определение актуальности задачи обеспечения конфиденциальности, целостности и доступности для конкретной информационной системы.	4 / 2
2	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема: Классификация угроз информационной безопасности.	Проведение классификации угроз информационной безопасности в информационной системе.	4 / 2
3	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема: Основные механизмы обеспечения информационной безопасности.	Реализация аутентификации пользователя системы на основе пары логин/пароль («секрета»).	3 / 2
4	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема: Теоретический подход к обеспечению информационной безопасности.	Построение обобщённой системы защиты информационной системы.	1
5	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема: Нормативно-правовой подход к обеспечению информационной безопасности.	Проведение классификации несанкционированного доступа и определение класса защищённости информационной системы.	1 / 1

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
6	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема: Практический (экспериментальный) подход к обеспечению информационной безопасности.	Построение системы защиты информационной системы.	2 / 2
7	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема: Построение модели угроз.	Разработка и обоснование частной модели угроз для информационной системы.	1
8	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема: Определение и разработка политики безопасности.	Разработка и обоснование политики безопасности для информационной системы.	1
9	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема: Аудит информационной безопасности.	Определение уровня защищённости информационной системы. 7.	1
			ВСЕГО:	18/ 9

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Экологический менеджмент» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 80 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 20 % с использованием формы диалоговых технологий, проблемная лекция (2 часа). Весь курс лекций (100%) построен на использовании мультимедийного оборудования

Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 18 часов. Остальная часть практического курса (18 часов) проводиться с использованием «интерактивных» (проведение семинаров) технологий, в том числе разбор и анализ конкретных ситуаций, решение проблемных задач с использованием в качестве инструмента средств современной вычислительной техники; технологий, основанных на коллективных способах обучения.

Самостоятельная работа студента организованна с использованием традиционных видов работы и с использованием возможностей современных информационных технологий. К традиционным видам работы (23 часа) относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. Применение современных информационных технологий (26 часов) предусматривает отработку отдельных тем по электронным пособиям и специальным компьютерным программам, консультации с применением специальных телекоммуникационных технологий, например, программное обеспечение «Skype», подготовка к промежуточным контролям и коллоквиумам, изучение специальных разделов с использованием интернет-ресурсов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение ситуационных задач, анализ конкретных ситуаций, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, проведение коллоквиумов.

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	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема 1: Основные понятия теории информационной безопасности.	1.Подготовка к входному контролю. 2.Подготовка к практическому занятию № 1	6
2	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема 2: Классификация угроз информационной безопасности.	1.Подготовка к практическому занятию 2.Изучение учебной литературы из источников	7
3	6	РАЗДЕЛ 1 Введение в теорию информационной безопасности. Тема 3: Основные механизмы обеспечения информационной безопасности.	1.Подготовка к практическому занятию № 3 и 4. 2.Изучение учебной литературы из источников	7
4	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема 1: Теоретический подход к обеспечению информационной безопасности.	Изучение учебной литературы из источников	6
5	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема 2: Нормативно-правовой подход к обеспечению информационной безопасности.	Изучение учебной литературы из источников:	6
6	6	РАЗДЕЛ 2 Подходы к обеспечению информационной безопасности. Тема 3: Практический (экспериментальный)	1. Подготовка к практическому занятию № 6. Изучение учебной литературы из источников	10

		подход к обеспечению информационной безопасности.		
7	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема 1: Построение модели угроз.	Изучение учебной литературы из источников:	10
8	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема 2: Определение и разработка политики безопасности.	Изучение учебной литературы из источников	10
9	6	РАЗДЕЛ 3 Обеспечение и оценка эффективности системы защиты информационных систем. Тема 3: Аудит информационной безопасности.	Изучение учебной литературы из источников	10
			ВСЕГО:	72

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	П.Н. Башлы , А. В. Бабаш, Е.. К. Баранова.	М.: РИОР, , 2013	Все разделы
2	Комплексная защита информации в корпоративныхсистемах	В.Ф. Шаньгин.	М.: ИД ФОРУМ: НИЦ , 2013	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Криптографические методы защиты информации.	А.В. Бабаш	М.: ИЦ РИОР: НИЦ ИНФРА-М, , 2014	Все разделы
4	Оценка относительного ущерба безопасности информационной системы:	Е.А. Дубинин, Ф.Б. Тебуева,, В.В. Копытов	М.: ИЦ РИОР: НИЦ ИНФРА-М, , 2014	Все разделы

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

. http://fsb.ru - сайт ФСБ России;
2. http://fstec.ru ФСТЭК России.

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

Для проведения лекционных и практических занятий используется специализированная лекционная аудитория с компьютером, интерактивной доской, проектором и экраном. Компьютеры обеспечены стандартными лицензионными программными продуктами и обязательно программным продуктом Microsoft Office не ниже Microsoft Office 2007

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

Для проведения аудиторных занятий и самостоятельной работы требуются:
1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET. Программное обеспечение для создания текстовых и графических документов, презентаций и т.п.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

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

Учебным планом на изучение дисциплины отводится один семестр. В качестве итогового контроля предусмотрен зачёт. Целесообразно осуществлять проведение зачёта в форме устного опроса по билетам.
При проведении лекционных занятий целесообразно широко применять такую форму обучения как лекция-визуализация, сопровождая изложение теоретического материала презентациями, при этом желательно заблаговременно обеспечить студентов раздаточным материалом.
Основной упор в методике проведения практических занятий должен быть сделан на отработке и закреплении учебного материала в процессе выполнения заданий с применением средств вычислительной техники в компьютерном классе. Особое внимание при этом должно быть уделено применению элементов проблемного и контекстного обучения.
Текущий контроль усвоения знаний осуществляется путем выполнения расчётных работ и ответов на вопросы на коллоквиумах в конце каждого модуля.