

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

СОГЛАСОВАНО:

Выпускающая кафедра ЭЭТ
Заведующий кафедрой ЭЭТ

16 мая 2018 г.

 М.В. Шевлюгин

УТВЕРЖДАЮ:

Директор ИТТСУ

25 мая 2018 г.

 П.Ф. Бестемьянов

Кафедра «Машиноведение, проектирование, стандартизация и сертификация»

Автор Козлов Виктор Владимирович, к.т.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Основы компьютерной безопасности»

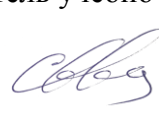
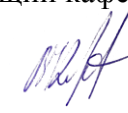
Направление подготовки: 27.03.01 – Стандартизация и метрология

Профиль: Метрология и метрологическое обеспечение

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2018

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

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.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-18	способностью изучать научно-техническую информацию, отечественный и зарубежный опыт в области метрологии, технического регулирования и управления качеством
ПК-19	способностью принимать участие в моделировании процессов и средств измерений, испытаний и контроля с использованием стандартных пакетов и средств автоматизированного проектирования
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

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

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) проводится 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 организована 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 завершённый 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. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Введение в теорию информационной безопасности.

Тема: Основные понятия теории информационной безопасности.

Опрос на практическом занятии (ПРЗ)

Тема: Классификация угроз информационной безопасности.

Тема: Основные механизмы обеспечения информационной безопасности.

РАЗДЕЛ 2

Подходы к обеспечению информационной безопасности.

Тема: Теоретический подход к обеспечению информационной безопасности.

Тема: Нормативно-правовой подход к обеспечению информационной безопасности.

Тема: Практический (экспериментальный) подход к обеспечению информационной безопасности.

Опрос на ПРЗ собеседование,

РАЗДЕЛ 3

Обеспечение и оценка эффективности системы защиты информационных систем.

Тема: Построение модели угроз.

Тема: Определение и разработка политики безопасности.

Тема: Аудит информационной безопасности.

Опрос на ПРЗ, ПК2, зачет