МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографические методы защиты информации и протоколы

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Форма обучения:	Очная

Общие сведения о дисциплине (модуле).

Основной целью изучения дисциплины «Криптографические методы защиты информации и протоколы» является формирование у обучающегося компетенций для следующих типов задач профессиональной деятельности: - научно-исследовательская; - проектная; - контрольно-аналитическая;

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач: Научно-исследовательская деятельность: - сбор, обработка, анализ и систематизация научно-технической информации, отечествен-ного и зарубежного опыта по проблемам компьютерной безопасности; Проектная деятельность: - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; -разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием. Контрольно-аналитическая деятельность: -предварительная оценка, выбор и разработка необходимых

методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при про-ведении контрольного анализа системы защиты; -подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей. Эксплуатационная деятельность: -установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения; -установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем; -проверка технического состояния и профилактические осмотры технических средств защиты информации; - проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Задачи дисциплины: - изложение основополагающих принципов защиты информации с помощью криптографических методов и изучение их практического применения. -развитие у обучаемых системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами с помощью методов криптографии; -изучение принципов синтеза и анализа криптосистем, математических методов оценки их стойкости. - получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

Общая трудоемкость дисциплины (модуля) составляет 8 з.е. (288 академических часа(ов).