МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Математическое моделирование и системный анализ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

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

1. Цели освоения учебной дисциплины

В курсе Б1.Б.24 «Криптографические методы защиты информации» изучаются основные математические методы криптографии. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются в дисциплинах профессионального цикла, связанных с защитой информации. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической криптографии и ее прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.
Компетенции, приобретаемые студентами, применяются для научно-исследовательской деятельности.
Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: основные задачи и понятия криптографии, понятие шифрования, примение принципов шифрования, построение криптографических систем и алгоритмов, применеие алгоритмов при защите информации.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Криптографические методы защиты информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины Б1.Б.24 «Криптографические методы защиты информации» осуществляется в форме лекций, практических занятий и курсовой работы. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративные). Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 28 часов. Остальная часть практического курса (6 часов) проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, дискуссии (решение

проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения (возможны видеоконференции при подготовке курсовых проектов).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. Предполагаются консультации студентов по курсовой работе.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 для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных лабораторных заданий с использованием. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
История и основные понятия криптографии

Тема: История и основы криптографии

Тема: Основные понятия криптографии

Тема: Виды шифров. Результаты К. Шеннона

Тема: Криптостойкость шифров. Атаки

Тема: Статистический анализ шифр-текстов

Тема: Псевдослучайные последовательности и шифрование

РАЗДЕЛ 2
Матем. принципы шифрования

Тема: Стандартные вспомогательные алгоритмы

Тема: Генерирование случайных подстановок, шифры перестановок

Тема: Простые числа, из распр-ние, псевдопростые числа

Тема: Тесты на простоту. Тест Рабина-Миллера

Тема: Построение больших простых чисел

РАЗДЕЛ 3
Криптосистемы и понятие протокола

Тема: Блочное шифрование.Поточные шифры

Тема: Алгоритм шифрования RSA

Тема: Алгоритм шифрования Эль-Гамаля

Тема: Алгоритм шифрования Рабина

Тема: Криптографические хэш-функции

Тема: Понятие криптопротокола