МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

08 сентября 2017 г.

Кафедра «Управление и защита информации»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 1 06 сентября 2017 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 2 04 сентября 2017 г. Заведующий кафедрой  Л.А. Баранов

Москва

1. Цели освоения учебной дисциплины

В курсе «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 её прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.
Компетенции, приобретаемые студентами, применяются для научно-исследовательской и проектной деятельности:
- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
- разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов.
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:

ОПК-4	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
ПК-5	способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «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 22 часов. Остальная часть практического курса (10 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 работ).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, выполнение курсовой работы..

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

РАЗДЕЛ 1
История и основные понятия криптографии
Контрольная работа

Тема: История криптографии

Тема: Основные понятия криптографии

Тема: Виды шифров. Результаты К. Шеннона.

Тема: Понятие криптоанализа.

Тема: Криптостойкость шифров.

Тема: Атаки на шифры.

Тема: Статистический анализ шифр-текстов.

Тема: Псевдослучайные последовательности и шифрование.

РАЗДЕЛ 2
Математические принципы шифрования
Контрольная работа

Тема: Алгоритмы быстрого возведения в степень по модулю.

Тема: Алгоритм нахождения НОД.

Тема: Алгоритм нахождения обратного элемента по модулю.

Тема: Китайская теорема об остатках.

Тема: Генерирование случайных подстановок, шифры перестановок.

Тема: Простые числа, их распределение, псевдопростые числа.

Тема: Тесты на простоту. Тест Рабина-Миллера.

Тема: Построение больших простых чисел.

РАЗДЕЛ 3
Криптосистемы и понятие протокола
Проверка и защита курсовой работы.

Тема: Блочное шифрование. Поточные шифры.

Тема: Алгоритм шифрования RSA.

Тема: Алгоритм шифрования Эль-Гамаля.

Тема: Алгоритм шифрования Рабина.

Тема: Криптографические хэш-функции.

Тема: Понятие эллиптической кривой.

Тема: Структура группы на эллиптической кривой.

Тема: Понятие криптопротокола.

Экзамен