

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Цифровые технологии управления транспортными процессами»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Методы и средства криптографической защиты информации»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2019

1. Цели освоения учебной дисциплины

В курсе «Методы и средства криптографической 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 экспериментально-исследовательской деятельности.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: основные задачи и понятия криптографии, понятие шифрования, применение принципов шифрования, построение криптографических систем и алгоритмов, применение алгоритмов при защите информации.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Методы и средства криптографической 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-2	Способен использовать совокупность необходимых математических методов для решения задач обеспечения защиты информации
ПКО-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Методы и средства криптографической защиты информации» осуществляется в форме лекций и практических занятий. 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. Проведение практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объеме 16 часов. Возможен 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. К интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к текущему и промежуточному контролю, интерактивные консультации в режиме

реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. 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 заданий с использованием компьютеров или на бумажных носителях..

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

РАЗДЕЛ 1

Квадратичные вычеты и основы теории эллиптических кривых

Контр. работа №1

[1], [2], доп. [2]. Подготовка дом. заданий, курсовой работы

Тема: Квадраты в конечных полях

Тема: Символ Лежандра

Тема: Свойства символа Лежандра

Тема: Символ Якоби

Тема: Понятие эллиптической кривой

РАЗДЕЛ 2

История и основные понятия криптографии

Контр. работа №2

[1], [2], доп. [2]. Подготовка дом. заданий, курсовой работы

Тема: История и основы криптографии.

Тема: Виды шифров. Результаты К. Шеннона. Криптостойкость шифров. Атаки

Тема: Статистический анализ шифр-текстов

Тема: Генерирование случайных подстановок. Базовые алгоритмы криптографии

Тема: Простые числа, тесты на простоту. Тест Рабина-Миллера

Тема: Построение больших простых чисел

РАЗДЕЛ 3

Системы шифрования

[1], [2], доп. [2]. Подготовка дом. заданий, курсовой работы

Тема: Блочное шифрование.

Тема: Алгоритм шифрования Эль-Гамала

Тема: Алгоритм шифрования Рабина

РАЗДЕЛ 5

Итоговая аттестация