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

«Числовые методы криптографии»

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

Цели освоения учебной дисциплины Б1.В.ОД.9 Числовые методы криптографии: Курс «Числовые методы криптографии» является математической дисциплиной, продолжающей теоретико-числовую и алгебраическую подготовку студентов. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются и в других дисциплинах, связанных с защитой информации. Цель преподавания дисциплины – обеспечить студентам знания в области теории чисел и алгебры, 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: задачи теории чисел, алгебры и теории групп, работа в мультипликативной группе колец вычетов, применение свойств символов Лежандра и Якоби, тестов на простоту для натуральных чисел; использование методов разложения чисел и многочленов на множители.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Числовые методы криптографии" 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:

ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации
ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПСК 1.2);

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины Б1.В.ОД.9 «Числовые методы криптографии» 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. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 12 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.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, основаным 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
Алгебраические основы крипт-фии

Тема: Идеалы в кольцах. Прямое произведение колец

Тема: группы подстановок

Тема: Факторкольца. Теоремы о гомоморфизмах колец

Тема: цикловая з-апись подстановки.Ее порядок.

Тема: подгруппы.теорема Лагрнжа.

Тема: группы

РАЗДЕЛ 2
Теоретико-групповые основы крипт-фии

Тема: циклические группы

Тема: Сопряженные элементы и нормальные подгруппы

Тема: Факторгруппы. Теоремы о гомоморфизмах групп

Тема: Мультипликативная группа поля вычетов. Малая теорема Ферма

Тема: Мультипликативная группа кольца вычетов. Теорема Эйлера. Функция Эйлера

Тема: Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю

РАЗДЕЛ 3
Квадратичные сравнения

Тема: Квадраты в конечных полях

Тема: Символ Лежандра и его выч-ние

РАЗДЕЛ 4
Нестандартные числовые системы

РАЗДЕЛ 5
Геометрические модели Zp и Qp

Тема: p-адическая топология в Z

Тема: Кольцо целых p-адических чисел Zp

Тема: Поле p-адических чисел Qp

Тема: Геометрические модели Zp и Qp.

РАЗДЕЛ 5
Итоговая аттестация