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

«Компьютерная безопасность»

Направление подготовки:	01.03.02 – Прикладная математика и информатика
Профиль:	Математические модели в экономике и технике
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2019

1. Цели освоения учебной дисциплины

В курсе Б1.В.ОД.16 «Компьютерная безопасность» изучаются основные математические методы криптографии. 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: алгебраические и теоретико-числовые основы криптографии, криптосистемы RSA, Эль-Гамаля, Рабина, а также криптопротоколы Диффи-Хелмана, Шнорра, Блюма и некоторые другие. использование частотных характеристик открытых текстов для анализа простейших шифров замены и перестановки, применение стандартов в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных систем, изучение современной литературе по криптографии. В результате освоения дисциплины студент будет владеть криптографическими понятиями, стандартными криптографическими алгоритмами и протоколами, реализуемыми на компьютерах, приёмами математического моделирования в шифровании. владеть знаниями и опытом, связанным с теорией алгебраических чисел (символ Лежандра, символ Якоби, закон взаимности Гаусса).
Компетенции, приобретаемые студентами, применяются для проектной и производственно-технологической, а также научно-исследовательской деятельности.
Дисциплина предназначена для получения знаний в следующих видах деятельности: проектная и производственно-технологическая, научно-исследовательская.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
проектная и производственно-технологическая:
- исследование математических методов моделирования информационных и имитационных моделей по тематике выполняемых научно-исследовательских прикладных задач или опытно-конструкторских работ;
- исследование автоматизированных систем и средств обработки информации, средств администрирования и методов управления безопасностью компьютерных сетей;
- развитие и сипользование инструментальных средств, автоматизированных систем в научной и практической деятельности;
научно-исследовательская:
- изучение новых научных результатов, научной литературы или научно-исследовательских проектов в соответствии с профилем объекта профессиональной деятельности;
- применение наукоемких технологий и пакетов программ для решения прикладных задач в области физики, химии, билогии, экономики, медицины, экологии.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Компьютерная безопасность" 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:

ПКС-1	Уметь ставить цели создания системы, разрабатывать концепцию

	системы и требования к ней, выполнять декомпозицию требований к системе

4. Общая трудоемкость дисциплины составляет

2 зачетные единицы (72 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Компьютерная безопасность» осуществляется в форме лекций и лабораторных работ. Лекции (30 часов) проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 80 % являются традиционными классически-лекционными (объяснительно-иллюстративные). Часть лекций (6 часов) проводится в интерактивной форме. Это – круглые столы, разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач. Лабораторные работы проводятся в компьютерных (дисплейных) залах-лабораториях. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. 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 компьютеров. Проведение занятий по дисциплине возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):- использование современных средств коммуникации;- электронная форма обмена материалами;- дистанционная форма групповых и индивидуальных консультаций;- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д..

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

РАЗДЕЛ 1
Алгебраические и теоретико-числовые основы криптографии.

Тема: Кольца вычетов

Тема: Прямое произведение колец

Тема: Конечные поля

Тема: Символ Лежандра (интерактив)

Тема: Базовые алгоритмы
устный опрос

РАЗДЕЛ 2
Криптосистемы

Тема: Свойства криптосистем

Тема: Тест Рабина-Миллера

Тема: Построение больших простых чисел

Тема: Система RSA

Тема: Система Эль-Гамаля

РАЗДЕЛ 3
Криптопротоколы

Тема: Понятие криптопротокола

Тема: Криптопротоколы: Диффи-Хелмана, Блюма.

Тема: Протокол аутентификации Шнорра

Тема: Эл. подпись
устный опрос

РАЗДЕЛ 4
Дифференцированный зачет.