

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

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

06 октября 2020 г.



Кафедра «Цифровые технологии управления транспортными процессами»

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

**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	2017

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 3 05 октября 2020 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 2 02 октября 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">В.Е. Нутович</p>
--	--

Москва 2020 г.

## 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-Гамала, 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 литературы по криптографии. В результате освоения дисциплины студент будет владеть криптографическими понятиями, стандартными криптографическими алгоритмами и протоколами, реализуемыми на компьютерах, приемами 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 использование 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, биологии, 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:

ОПК-4	способностью решать стандартные задачи профессиональной
-------	---

	деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-3	способностью критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности
ПК-7	способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения

#### **4. Общая трудоемкость дисциплины составляет**

3 зачетные единицы (108 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-Гамала

## РАЗДЕЛ 3 Криптопротоколы

Тема: Понятие криптопротокола

Тема: Криптопротоколы: Диффи-Хелмана, Блюма.

Тема: Протокол аутентификации Шнорра

Тема: Эл. подпись  
устный опрос

Тема: Протоколы разделения секрета (интерактив)

Экзамен