

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

Кафедра «Вычислительные системы, сети и информационная  
безопасность»

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Информационная безопасность и защита информации»**

Направление подготовки:	<u>38.03.02 – Менеджмент</u>
Профиль:	<u>Логистика и управление цепями поставок</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очно-заочная</u>
Год начала подготовки	<u>2017</u>

## 1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Информационная безопасность и защита информации» являются изучение студентами основных понятий информационной безопасности, изучение основных видов угроз информационной безопасности; получение представления об организации и принципах обеспечения информационной безопасности; знакомство с основами методов криптографического закрытия данных; получение навыков разработки политики безопасности предприятия.

Основными задачами дисциплины являются:

- освоение методов оценки степени угрозы информационной безопасности;
- изучение использования соответствующих методов защиты.;
- рассмотрение методов организации комплексной системы защиты информации;
- изучение студентами основных угроз информационной безопасности и методов защиты от них.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческая деятельность:

- организация работы малых групп исполнителей;
- участие в разработке организационно-технической документации (графиков работ, инструкций, планов, смет) и установленной отчетности по утвержденным формам.

Предпринимательская деятельность:

- безопасное использование корпоративной сети, использование глобальных компьютерных сетей;
- применение защищенной электронной коммерции;
- безопасное использование электронной почты;

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Информационная безопасность и защита информации" 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 осуществлять деловое общение и публичные выступления, вести переговоры, совещания, осуществлять деловую переписку и поддерживать электронные коммуникации
ОПК-7	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-6	способностью участвовать в управлении проектом, программой внедрения технологических и продуктовых инноваций или программой организационных изменений

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

2 зачетных единиц (72 ак. ч.).

#### **5. Образовательные технологии**

Преподавание дисциплины «Информационная безопасность и защита информации» осуществляется в форме лекций и практических занятий. Практические занятия проводятся с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения. 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. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы. .

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

##### **РАЗДЕЛ 1**

##### **ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ**

Тема: Основные понятия.

Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные.

Тема: Государственные структуры, отвечающие за защиту данных.

опрос

Определение служебной тайны. Законодательство РФ в области информационной безопасности. Информационная безопасность коммерческой структуры. Типовой набор должностей, связанных с защитой данных на предприятии.;

Тема: Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности..

##### **РАЗДЕЛ 2**

##### **УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Тема: Природа возникновения угроз.

Классификация угроз по преднамеренности проявления. Классификация по источнику угрозы. Классификация по степени воздействия на информационную систему. По

способам доступа к ресурсам информационной системы.

Тема: Угрозы безопасности информационной системы.

Тема: Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.

### РАЗДЕЛ 3 ПОЛИТИКА БЕЗОПАСНОСТИ

Тема: Структура политики безопасности.

Тема: Базовая политика безопасности.

опрос

Тема: Специализированные политики безопасности.