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

Кафедра   «Информационные системы цифровой экономики»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки:	<u>09.03.03 – Прикладная информатика</u>
Профиль:	<u>Прикладная информатика в бизнесе</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2018</u>

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Информационная безопасность» являются формирование теоретических основ и практических навыков в области защиты информации от несанкционированного доступа, искажения, потери. Рассматриваются тенденции развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а также с нормативными документами и методами защиты компьютерной информации. Проводится изучение современных методов защиты информации: криптография, стеганография.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Информационная безопасность" 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:

ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности
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-18	способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Лекция Лекция используется для изложения более или менее объемистого учебного материала, и поэтому она занимает почти весь урок. Естественно, что с этим связана не только определенная сложность лекции как метода обучения, но и ряд ее специфических особенностей. Важным моментом в проведении лекции является предупреждение пассивности обучающихся и обеспечение активного восприятия и осмысления ими новых знаний. Определяющее значение в решении этой задачи имеют два дидактических условия: 1) во-первых, само изложение материала учителем должно быть содержательным в научном отношении, живым и интересным по форме; 2) во-вторых, в процессе устного изложения знаний необходимо применять особые педагогические приемы, возбуждающие мыслительную активность школьников и способствующие поддержанию их внимания. Один из этих приемов – создание проблемной ситуации. Самым простым в данном случае является достаточно четкое определение темы нового материала и выделение тех основных вопросов, в которых надлежит разобраться обучающимся. Лабораторные работы Лабораторное занятие - это организационная форма обучения, регламентированная по времени (пара) и составу (учебная группа, подгруппа), цель которой - сформировать профессиональные умения и навыки в лабораторных условиях с помощью современных технических средств. Цель проведения лабораторных занятий – конкретизация теоретических знаний, полученных в процессе лекций, повышение прочности усвоения и закрепления изучаемых знаний и умений. Функциями

лабораторных занятий являются: закрепление теоретических знаний на практике; усвоение умений исследовательской работы; усвоение умений практической психологической работы; применение психологических теоретических знаний для решения практических задач; самопознание обучающихся и саморазвитие. Типичные задания: демонстрационный эксперимент, индивидуальные задания, групповые задания, эксперимент в парах, решение психол. задач, деловая игра. План занятия включает в себя: внеаудиторная самостоятельная подготовка к занятию; проверка теоретической подготовленности студентов; инструктирование студентов; выполнение практических заданий, обсуждение итогов; оформление отчета; оценка выполненных заданий и степени овладения умениями. Лабораторные работы могут носить репродуктивный характер (студенты пользуются подробными инструкциями), частично-поисковый (самостоятельный подбор материала и методик) и поисковый характер (студенты должны решить новую для них проблему, опираясь на теоретические знания). Формы организации: фронтальная, групповая и индивидуальная. Критерии эффективности: уровень самостоятельности и активности студентов; степень сформированности умений; уровень и характер поисково-исследовательской и творческой деятельности студентов; удовлетворенность студентов и преподавателей состоявшимся занятием. Проведение занятий по дисциплине (модулю) возможно с применением электронного обучения и/или 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/или дистанционных образовательных технологий применяются современные образовательные технологии, в том числе современные средства коммуникации, электронная форма обмена материалами, а также дистанционная форма групповых и индивидуальных консультаций..

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

Тема: 1. Актуальность информационной безопасности мет и метод защиты информации. Объект защиты информации. Угрозы безопасности информации в компьютерных системах.

Тема: 2. Методы и средства защиты информации. Современные методы защиты информации. Защита от несанкционированного доступа (НСД). Ограничение, разграничение, контроль доступа, идентификация, аутентификация пользователя. СОРДИ. Таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существование. Криптографические методы защиты информации. Стеганография. Концепция информационной безопасности.

Тема: 3. Защита документооборота в вычислительных системах. Угрозы и методы защиты. Комплексный метод защиты.

Тема: 4. Компьютерные вирусы и механизмы борьбы с ними. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

Тема: 5. Международные и отечественные стандарты информационной безопасности.

Стандарт ISO 15408.

Стандарты безопасности в Интернете, протоколы защиты передачи данных - SSL (TLS), SET, IP v. 6, IPSec.

Нормативные документы, регламентирующие оценку защищенности ИТ.

Тема: 6. Комплексные системы защиты информации.

Концепция создания защищенных компьютерных систем.

Этапы создания комплексной системы комплексной защиты информации

Экзамен