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»

Специальность:	38.05.01 – Экономическая безопасность
Специализация:	Финансово-экономическое обеспечение федеральных государственных органов, обеспечивающих безопасность Российской Федерации
Квалификация выпускника:	Экономист
Форма обучения:	очная
Год начала подготовки	2018

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Информационная безопасность» являются формирование у студентов целостного представления предусматривается изучение вопросов защиты информации в сетях ЭВМ, идентификации и аутентификации пользователя, криптографического закрытия информации различными методами с применением вычислительной техники и прикладного программного обеспечения. В результате изучения дисциплины студенты должны уметь: применять методы и приемы защиты от несанкционированного доступа, получить навыки шифрации и дешифрации информации методами криптографического преобразования данных.

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:

ПСК-4	способностью грамотно применять законодательство об информатизации и защите информации и инструментальные средства обработки информации в профессиональной деятельности в целях обеспечения информационной безопасности хозяйствующих субъектов

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

В обучении студентов по данной дисциплине используются:1. при проведении лекционных занятий:- вводная;- лекция-информация; - проблемная лекция;- лекция визуализация;2. для проведения лабораторных и практических занятий:- проектная технология;- технология учебного исследования;- техника «круглый стол»,- техника «публичная защита»;- технология обучения в сотрудничестве и в малых группах;- технология проблемного обучения;- технологии дистанционного обучения;- разбор конкретных ситуаций..

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

РАЗДЕЛ 1
Основные понятия и определения, эволюция подходов к обеспечению ИБ

Тема: Информация. Информационная сфера

Содержание понятия «Информация». Формы информации. Свойства ин-формации в форме сведений и в фор-ме сообщений. Информация как объект исследования. Понятия информа-ционного воздействия и информаци-онного взаимодействия. Составляю-щие информационной сферы.

Тема: Национальные интересы и без-опасность России

Принципы соблюдения информацион-ной безопасности. Две классификации национальных интересов. Основные составляющие национальных интере-сов в информационной сфере. Общие методы обеспечения информационной безопасности. Понятие информацион-ных ресурсов. Основные классы ин-формационных ресурсов

Тема: Введение

РАЗДЕЛ 2
Информационные, программно-математические, физические и организационные угрозы

Тема: Информационная война. Ин-формационное оружие

Интересы и угрозы в области инфор-мационной безопасности. Составляю-щие национальной безопасности. Про-блемы информационной войны. Клас-сификация информационного оружия. Основные объекты воздействия в ин-формационной войне. Цели информа-ционной войны. Понятия начала и окончания войны.

Тема: Угрозы безопасности России. Угрозы безопасности АСОД

Виды угроз безопасности России. Классификация угроз. Понятие «Инте-гральная информационная безопас-ность». Схема основных элементов и объектов защиты в АСОД. Угрозы безопасности в АСОД. Мировые стан-дарты в области информационной без-опасности. Основные компоненты критериев безопасности ITSEC. Про-цесс управления рисками. Общая схема анализа безопасности.

РАЗДЕЛ 3
Защита от несанкционированного доступа, модели и основные принципы защиты информации

Тема: Показатели защищенности СВТ

Функции и задачи защиты информа-ции. Функции непосредственной за-щиты. Механизмы защиты. Управле-ние механизмами защиты. Основные группы факторов, влияющие на ин-формационную безопасность техниче-ской системы. Класс и показатели за-щищенности СВТ (АС).

Тема: 6 Защита информации в АСОД

Понятие защиты информации. Поня-тие защиты информации в АСОД. Ос-новные методы защиты информации в вычислительных сетях. Методы, при-меняемые для установления подлин-ности различных объектов

Тема: Виды доступа. Уровни доступа. Контроль доступа

Виды доступа к информации. Обяза-тельное доведение. Свободный доступ. Ограничения и запреты. Виды информации с ограниченным доступом. Методы защиты информации от

преднамеренного до-ступа (при применении простых средств хранения и обработки информации). Идентификация и аутентификация пользователя.

РАЗДЕЛ 4
Компьютерные вирусы и антивирусные программы

Тема: Проблема вирусного заражения

Компьютерный вирус(закладка): поня-тие, пути распространения, проявле-ние действия вируса. проникновения Структура современных вирусов: мо-дели поведения вирусов; деструктив-ные действия вируса; разрушение про-грамм защиты, схем контроля или из-менение состояния программной сре-ды. Воздействия на программно-аппаратные средства защиты инфор-мации. Последствия от вирусных вторжений и катастроф.

Тема: Перспективные методы антивирусной защиты

Перспективные методы антивирусной защиты. Антивирусные проверки на ПК, на файловых серверах и серверах приложений, на прокси-серверах, на межсетевых экранах. Борьба со спамом. Базовые однолинейные мето-ды. Спамоборона. Многоплатформен-ные антивирусные и антиспамовые решения компании Sophos.

Тема: Основные классы антивирусных программ

Программы-детекторы, программы-доктора, программы - ревизоры, про-граммы-фильтры. Интегрированные антиспамовые и антивирусные реше-ния от компании Sybari. Антивирусные программы семейства Dr.Web? для рабочих станций. Структура Dr.Web?. Ядро Dr.Web?. Программы – антивирусы: Aidstest, Adinf, Norton Antivirus, AVP. Профилактика зараже-ния вирусом.

РАЗДЕЛ 5
Защита от утечки информации по техническим каналам

Тема: Криптографические методы защиты информации

Периоды развития криптологии. Пер-вые шифры. Два направления в крип-тологии. Цели криптографии и крип-тоанализа. Разделы криптографии. Стеганография. Закрывать информа-цию методами зимены,(моно-алфавитной и поли-алфавитной под-становки), перестановки, с помощью аналитических преобразований, мето-дом гаммирования. Система с откры-тым ключем. Электронно-цифровая подпись. Приемы хеширования. Рабо-та с криптоцениром MS OutLook.

Тема: Проблемы защиты информации в сетях ЭВМ

Защита информации в ПК. Сервисы безопасности. Архитектура механиз-мов защиты в сетях. Международные стандарты. Межсетевые экраны. Прок-си серверы.

РАЗДЕЛ 6
Организационно-правовое обеспечение ИБ

Тема: Организационная защита информации. Комплексное обеспечение безопасности

Сущность ОЗИ и ее место в комплекс-ной системе защиты информации. Ви-ды ОЗИ. Лицензирование деятельно-сти предприятия по проведению работ, связанных с использование сведений составляющих гостайну. Организация физической охраны предприятия. Источники. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.

Тема: Правовые основы защиты информации

Опыт законодательного регулирования информатизации в России и за рубе-жом. Концепция правового обеспече-ния информационной безопасности РФ. Стандарты и нормативно-методические документы в области обеспечения информационной без-опасности. Государственная система обеспечения информационной без-опасности. Международные правовые акты по защите информации.

Зачет