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

«Основы информационной безопасности »

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Вычислительные системы и сети
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Основы информационной безопасности» 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, методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

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.
• процесса сбора, передачи, накопления и обработки информации;
• установление структуры угроз защищаемой информации;

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности).

Организационно-управленческая
- контроль использования сетевых устройств и программного обеспечения
- оценка производительности сетевых устройств и программного обеспечения

Производственно-технологическая
- осуществляет разработку тестовых документов, включая план тестирования
- коррекция производительности сетевой инфокоммуникационной системы
- выполнение регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы
- восстановление параметров программного обеспечения сетевых устройств

Проектная
- планирование восстановления сетевой инфокоммуникационной системы
- планирование модернизации сетевых устройств
- проектирование компьютерных сетей

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы информационной безопасности " 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:

ОПК-3	Способен решать стандартные задачи профессиональной деятельности на

	основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-4	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил
ПКО-5	Способность разрабатывать политики информационной безопасности, регламентов и аудита, готовить отчеты о состоянии и эффективности системы безопасности на уровне БД

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Основы информационной безопасности» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 16 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными). Лабораторные работы (16 часов) проводится 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 (76 часа) студента организована с использованием традиционных видов работы. К традиционным видам работы относится 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 6 разделов, представляющих собой логически завершенный объем учебной информации. 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. 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. Контрольная работа №1

Тема: Угрозы безопасности информационной системы.

РАЗДЕЛ 3
ПОЛИТИКА БЕЗОПАСНОСТИ

Тема: Структура политики безопасности

Тема: Базовая политика безопасности.

Тема: Специализированные политики безопасности

РАЗДЕЛ 4
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Тема: Классификация криптографических алгоритмов. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы.

Тема: Симметричные криптоалгоритмы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.

Тема: Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.

РАЗДЕЛ 5
ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема: Аутентификация, авторизация и администрирование действий пользователей Контрольная работа №1

Тема: ильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.

РАЗДЕЛ 6
ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.

Тема: Защита http-трафика. Характерные угрозы. Защищенный протокол httpd

Тема: Цифровые сертификаты.. Виртуальная частная сеть.

Тема: Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec

РАЗДЕЛ 7
Итоговая аттестация