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:	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

Дисциплина "Информационная безопасность и защита информации" предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческой
- разработка политики информационной безопасности на уровне БД
- разработка регламентов и аудит системы безопасности данных на уровне БД
- подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД
-контроль использования сетевых устройств и программного обеспечения
-администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Производственно-технологической
- разработка технических спецификаций на программные компоненты и их взаимодействие
- осуществляет разработку тестовых документов, включая план тестирования
- разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным
- разработка архитектуры ИС
- разработка прототипов ИС
- восстановление параметров программного обеспечения сетевых устройств
- размещение и соединение элементов электрических схем стандартных ячеек библиотеки

Проектной
- определение первоначальных требований заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ;
- разработка тестовых программ или генераторов тестовых программ для модели ИС на языках программирования целевой системы.

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:

ПКР-3	Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Информационная безопасность и защита информации» осуществляется в форме лекций, практических занятий и выполнения курсовой работы.Лекции проводятся в традиционной классно-урочной организационной

форме в объеме 32 часа, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).Практические занятия (32 часа) организованы с использованием технологий развивающего обучения. Самостоятельная работа студента (72 часа) 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 управление информационной безопасностью

Тема: Основные понятия.
Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные.
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.
Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности.

РАЗДЕЛ 2
Угрозы информационной безопасности

Тема: Природа возникновения угроз
выполнение и защита лабораторных работ №1-3

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.
Угрозы безопасности информационной системы.
Сетевая разведка: Sniffing; Ping-sweep, сканирование портов. Несанкционированный доступ: IP-spoofing; Man-in-the-middle; Подмена стороны. DOS-атака. DDOS-атака. Уязвимость программных приложений. Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.
Компьютерные вирусы. Троянские программы. Сетевые черви. Пути распространения вредоносного программного кода. Программы удаления вредоносного программного кода. Обновления безопасности. Антивирусные программы.

РАЗДЕЛ 3
Политика безопасности

Тема: Структура политики безопасности.
Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Уровни решений политики безопасности: верхний, средний и нижний. Область применения политики безопасности. Выработка позиции организации. Роль руководителей подразделений. Роль администраторов сетей. Роль администраторов сервисов. Роль пользователя информационной системы. Санкции.

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. Симметричные криптоалгорит-мы.Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. Асимметричные криптоалгоритмы.Алгоритм RSA. Алгоритм ДиффиХэлмана. 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.
Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.
Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Технология Zone-based farewall. Основные схемы применения межсетевых экранов. Методы анализа сетевой информации. Сигнатуры. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).

Тема: Аутентификация, авторизация и администрирование действий пользователей.
выполнение и защита практических работ № 4-6, выполнение курсовой работы

РАЗДЕЛ 6
Защита информации в глобальной сети.

Тема: Защита http-трафика
Характерные угрозы. Защищенный протокол httpd. Цифровые сертификаты.Виртуальная частная сеть.
Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.

РАЗДЕЛ 7
Итоговая аттестация