

**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

«Методы и средства обеспечения 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

Дисциплина «Методы и средства обеспечения информационной безопасности» 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 "Методы и средства обеспечения информационной безопасности" 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 «Методы и средства обеспечения информационной безопасности» 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 заверченный 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.

Управление информационными рисками

Международные стандартизирующие организации и стандарты в области управления информационной безопасностью.

РАЗДЕЛ 2

Основные функции систем управления информационной безопасностью

Тема: Понятие систем управления информационной безопасностью (СУИБ) выполнение и защита лабораторных работ №1-3

Тема: Понятие систем управления информационной безопасностью (СУИБ)

Функции систем управления информационной безопасностью.

Выявление и анализ рисков информационной безопасности; планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ; контролирование этих процессов; внесение в процессы минимизации информационных рисков необходимых корректировок.

РАЗДЕЛ 3

Принципы качественного управления информационной безопасностью

Тема: Качественное управление информационной безопасностью.

Комплексный подход; рискообразующие факторы; согласованность с бизнес-задачами и стратегией предприятия; уровень управляемости; адекватность используемой и генерируемой информации; эффективность СУИБ как баланс между возможностями, производительностью и издержками; непрерывность управления; процессный подход.

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 криптоалгоритмы. 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 firewall. 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

Иерархическая организация процессов управления информационной безопасностью

Тема: Иерархия процессов управления информационной безопасностью. Замкнутый жизненный цикл системы управления информационной безопасностью. Системный подход к созданию системы управления информационной безопасностью.

РАЗДЕЛ 7

Итоговая аттестация