МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Груздева Людмила Михайловна, к.т.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Основы информационной безопасности »

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины (модуля) «Основы информационной безопасности» являются:
– обучить студентов принципам обеспечения информационной безопасности, подходам к анализу информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;
– содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.
Задачи изучения дисциплины:
- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах;
- изучение типовых угроз безопасности информации при её обработке в компью-терных системах;
- изучение основных принципов обеспечения информационной безопасности;
- изучение основ построения модели угроз и политики безопасности;
- изучение основных моделей управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

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-1	Способен представлять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-9	Способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ОПК-19	Способен в процессе функционирования компьютерных систем и сетей и организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПКО-1	Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Технология обучения как учебного исследования Технология педагогических мастерскихТехнология коллективной мыследеятельности (КМД)Технология эвристического обучения.

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

РАЗДЕЛ 1
Информационная безопасность в системе национальной безопасности Российской Федерации

Тема: 1.1.
Понятие национальной безопасности. Сущность и содержание национальной безопасности. Основные задачи в области обеспечения национальной безопасности. Объект и субъект безопасности. Виды безопасности. Виды защищаемой информации. Основные понятия и общеметодологические принципы информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.

Тема: 1.2.
Национальные интересы России в информационной сфере. Место и роль России в глобальном информационном пространстве. Национальные интересы России в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

Тема: 1.3.
Виды угроз информационной безопасности Российской Федерации. Проблемы обеспечения информационной безопасности. Угрозы конституционным правам и свободам человека и гражданина. Угрозы информационному обеспечению государственной политики РФ. Угрозы развитию отечественной индустрии информации, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Классификация угроз безопасности информационных и телекоммуникационных средств и систем. Модель действий нарушителя.

Тема: 1.4.
Источники угроз информационной безопасности РФ. Внешние источники угроз. Внутренние источники угроз. Классификация источников угроз и уязвимостей информационной безопасности.

РАЗДЕЛ 2
Информационная война, методы и средства её ведения

Тема: 2.1.
Информационная безопасность и информационное противоборство. Понятие информационной войны. Проблемы информационных войн. Субъекты информационного противоборства. Цель информационного противоборства. Составные части и методы информационного противоборства.

Тема: 2.2.
Приемы информационного воздействия в информационной войне. Информационная война как целенаправленное информационное воздействие информационных систем. Способы перепрограммирования информационных систем. Проблема начала информационной войны.

Тема: 2.3.
Типовая стратегия информационной войны. Обобщенный алгоритм информационной войны. Основные аспекты информационной войны. Последствия информационной войны.

РАЗДЕЛ 3

Защита от несанкционированного доступа (НСД) к информации

Тема: 3.1.
Классификация автоматизированных систем и требования по защите информации. Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации.

Тема: 3.2.
Структура системы защиты информации от НСД. Назначение и функции элементов. Направления защиты от НСД. Основные способы НСД. Принципы защиты информации от НСД. Структура системы защиты информации от НСД, назначение и функции элементов.

Тема: 3.3.
Тестирование

Тема: 3.3.
Модели управления доступом. Правила разграничения доступа. Мандатная и дискреционная модели управления доступом. Ролевая и атрибутные модели.

РАЗДЕЛ 4
Основные методы обеспечения информационной безопасности

Тема: 4.1.
Основные понятия криптографической защиты информации. Определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.

Тема: 4.2.
Идентификация и аутентификация. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и цифровые подписи. Методы аутентификации.

Тема: 4.3.
Разграничение и контроль доступа к информации. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации; по способам ее обработки: считать, записать, внести изменения, выполнить команду; по условному номеру терминала; по времени обработки и др. Разделение привилегий на доступ к информации.

Тема: 4.4.
Технологии межсетевых экранов. Технология межсетевых экранов (МЭ) - защита корпоративных сетей от внешних угроз. Функции МЭ. МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты.

Тема: 4.5.
Виртуальные частные сети. Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.

Тема: 4.6.
Методы обнаружения вторжений (атак). Краткая история вторжений (атак) на интрасети. Основные понятия. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений.

Тема: 4.7.
Компьютерные вирусы и средства антивирусной защиты. Вирусы как угроза информационной безопасности. Средства антивирусной защиты.

РАЗДЕЛ 5
Стандарты защищенности информации в компьютерных системах

Тема: 5.1.
Характеристика систем стандартизации в области защиты информации. Информационная безопасность распределенных систем. Европейские критерии безопасности информационных технологий.

Тема: 5.1.
Тестирование

Экзамен