

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 июня 2019 г.


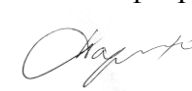
Кафедра «Управление и защита информации»

Автор Сидоренко Валентина Геннадьевна, д.т.н., профессор

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Администрирование и управление Информационной безопасности  
компьютерных систем»**

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	2019

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 25 июня 2019 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 21 24 июня 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
--	---

Москва 2019 г.

## 1. Цели освоения учебной дисциплины

Целями изучения дисциплины «Администрирование и управление Информационной безопасности компьютерных систем» являются овладение студентами теоретических и практических основ администрирования информационных систем; способов управления информационными сетями, администрирования операционных систем, приложений, сетевых и информационных сервисов, баз данных; формирование у студентов специальных знаний в области управления современными системами информационной безопасности и защиты информации.

Задачи дисциплины:

- изучение инфраструктуры вычислительной техники на железнодорожном транспорте;
- изучение функционального состава автоматизированных систем в сфере нормирования перевозочного процесса; грузовых и пассажирских перевозок; фирменного транспортного обслуживания; управления содержанием инфраструктуры;
- изучение стандартов проектирования автоматизированных систем (АС), предназначенных для эксплуатации на железнодорожном транспорте;
- изучение инструментальных средств проектирования АС ЖТ.

Основной целью изучения учебной дисциплины «Администрирование и управление Информационной безопасности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности:

- проектная;
- контрольно-аналитическая.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Проектная деятельность:

- разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;
- разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием.

Контрольно-аналитическая деятельность:

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Администрирование и управление Информационной безопасности компьютерных систем" 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-2	Способен проводить моделирование защищенных автоматизированных
-------	--

	систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой
ПКР-10	Способен проводить тестирование систем защиты информации автоматизированных систем
ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-4	Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем
УК-2	Способен управлять проектом на всех этапах его жизненного цикла

#### **4. Общая трудоемкость дисциплины составляет**

5 зачетных единиц (180 ак. ч.).

#### **5. Образовательные технологии**

Преподавание дисциплины «Администрирование и управление Информационной безопасностью компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция. Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы. В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 9 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 путём применения таких организационных форм, как индивидуальные и групповые опросы. .

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

### РАЗДЕЛ 1

Введение.

Тема: 1.1.

Основные понятия администрирования и безопасности информационных систем. История развития защиты информации и криптографии.

### РАЗДЕЛ 2

Администрирование операционных систем

Математическое обеспечение АС ЖТ. Методы и процедуры принятия решений при проектировании АС ЖТ.

Тема: 2.1.

Особенности операционных систем. Работа с командными строками.

### РАЗДЕЛ 3

Базовые средства администрирования Windows 2012 Server. Управление доменом. Active Directory

Тема: 3.1.

администрирования. Редактор реестра. Редактор локальной групповой политики. Службы Windows. Windows. ЛР № 1. Применение знаний основ администрирования ОС Windows. Управление инструментами администрирования ОС Windows. ОС Windows.

Тема: 3.2.

Управление ОС Windows. Управление дисками, основные знания видов накопителей. Диспетчер задач. Прочие инструменты Windows для администрирования ОС.

Тема: 3.3.

Управление доменом.

Контроллеры доменов.

ПЗ №2

Контролер домена.

ПЗ №3.

Четыре базовые модели организации доменов

Тема: 3.4.

Изучение Active Directory, PowerShell. ЛР №2. Основы работы с Active Directory, PowerShell.

### РАЗДЕЛ 4

Механизм групповой политики, служба DFS

Тема: 4.1.

Технический обзор политик ограниченного использования программ.

Тема: 4.2.

Технический обзор политик ограниченного использования программ.

Тема: 4.3.

Служба DFS. ЛР №3. Управление службой DFS.

## РАЗДЕЛ 5

Методы и технологии защиты информационных систем. Многоуровневая модель системы защиты

Тема: 5.1.

Виды информационных угроз. Современные виды защиты информации.

Тема: 5.2.

Устный или письменный опрос, защита лабораторных работ

Тема: 5.2.

Политики безопасности, стандарты, процедуры и метрики, подходы к анализу рисков. Lifecycle Security.

## РАЗДЕЛ 6

Основные виды угроза безопасности ИС и информации. Средства и методы защиты

Тема: 6.1.

Угрозы информационной безопасности. Источники угроз информационной безопасности.

Тема: 6.2.

Системы технического нормирования перевозочного процесса. Системы оперативного управления перевозочным процессом. Системы фирменного транспортного обслуживания. Структура, функции и алгоритмы систем технического нормирования перевозочного процесса и оперативного управления перевозочным процессом. Структура, функции и алгоритмы систем фирменного транспортного обслуживания.

## РАЗДЕЛ 7

Системы резервного копирования и восстановления данных. Эффективность информационных систем.

Тема: 7.1.

Принципы работы резервного копирования. Эффективность информационных систем. Российский и мировой рынки.

## РАЗДЕЛ 8

Основы администрирования баз данных

Тема: 8.1.

Базы данных.

Тема: 8.2.

Основы администрирования баз данных. Базовые знания в работе с SQL-сервером.

## РАЗДЕЛ 9

Межсетевой экран. Система обнаружения вторжений.

Тема: 9.1.

Межсетевой экран. Классификация. Реализация.

Тема: 9.1.

Устный или письменный опрос, защита лабораторных работ

Тема: 9.2.

СОВ. Пассивные и активные СОВ. Сравнение межсетевых экранов и СОВ.

РАЗДЕЛ 10

Зачет с оценкой