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

«Администрирование средств защиты информации в компьютерных системах»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2019

1. Цели освоения учебной дисциплины

Цели и задачи изучения дисциплины «Администрирование средств защиты информации в компьютерных системах» определяются характеристикой области и объектов профессиональной деятельности бакалавра профиля «Безопасность компьютерных систем» направления подготовки «Информационная безопасность».
В результате изучения дисциплины студент должен владеть современными средствами защиты ресурсов вычислительной системы, управления пользователями и процессами в интересах безопасности, уметь автоматизировать операции информационного обслуживания системы, создавать и поддерживать безопасную операционную среду.
Дисциплина формирует знания и умения для решения задач в соответствии с видами профессиональной деятельности: эксплуатационная деятельность, проектно-технологическая деятельность, экспериментально-исследовательская деятельность, организационно-управленческая.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Администрирование средств защиты информации в компьютерных системах" 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	Способность участвовать в разработке политик безопасности, политик управления доступом и информационными потоками в компьютерных сетях

4. Общая трудоемкость дисциплины составляет

4 зачетных единиц (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины«Администрирование средств защиты информации в компьютерных системах» осуществляется в форме лекций и лабораторных занятий. Лекции проводятся в традиционной классно-урочной форме. По дисциплине предусмотрены лабораторные занятия, содержащие интерактивные упражнения и задания, в ходе выполнения которых студент изучает и закрепляет материал. Занятия носят характер семинара-диалога и семинара-тренинга.. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Курс разбит на несколько разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера для оценки знаний и задания практического характера для оценки умений и навыков. Теоретические знания проверяются путем индивидуальных и групповых опросов..

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

РАЗДЕЛ 1
Понятие защищенной операционной системы
Методы создания защищенных информационных систем

РАЗДЕЛ 2
Теоретические основы защиты ОС
Стандарты защищенности. Формальное представление политик безопасности

РАЗДЕЛ 3
Методы защиты операционных систем
Структура безопасной операцион-ной системы

РАЗДЕЛ 4
Конфигурирование безопасной загрузки
Механизмы загрузки Windows NT

РАЗДЕЛ 4
Конфигурирование безопасной загрузки
Контрольный опрос

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Контрольный опрос

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Аппаратная поддержка защиты в операционных системах платформы x86

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Модель безопасности ОС Windows архитектуры NT. Структура и состав подсистем безопасности

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Контроль многопользовательского доступа. Механизмы ау-тентификации. Управление учет-ными записями.

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Контроль доступа к ресурсам. Механизмы авторизации. Права и привилегии доступа.

РАЗДЕЛ 5
Реализация механизмов защиты в операционных системах
Защита и шифрование данных в файловых системах.

РАЗДЕЛ 6
Администрирование локальной безопасности
Контрольный опрос, ТК1

РАЗДЕЛ 6
Администрирование локальной безопасности
Управление учетными записями пользователей и групп. Политики учетных записей.

РАЗДЕЛ 6
Администрирование локальной безопасности
Аудит и журналирование событий безопасности

РАЗДЕЛ 7
Командный режим управления.
Символические имена и маски. Перенаправление информационного потока. Базовые, сервисные и информационные команды

РАЗДЕЛ 7
Командный режим управления.
Контрольный опрос

РАЗДЕЛ 8
Автоматизация администрирования
. Язык сценариев. Командные файлы. Параметры запуска, пе-ременные и операции над ними.

РАЗДЕЛ 8
Автоматизация администрирования
Реализация разветвлений и циклов в сценариях

РАЗДЕЛ 9
Мониторинг производительности и процессов
Контрольный опрос, ТК2

РАЗДЕЛ 10
Планирование и управление заданиями

РАЗДЕЛ 11
Итоговая аттестация