МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Ларина Татьяна Борисовна, доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ 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

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии  Н.А. Клычева	Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой  Б.В. Желенков

Москва 2019 г.

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.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Операционные системы:

Знания: основы организации операционных систем, принципы управления памятью, принципы управление процессами, аппаратно-программные основы операционных систем платформы x86

Умения: применять дисковые менеджеры и редакторы для решения системных задач, разрабатывать низко-уровневые системные утилиты

Навыки: средствами системного сервиса операционных систем, инструментальными средствами конфигурирования загрузки, дисковых структур и файловых подсистем

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Защита программ и данных

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-2 Способность участвовать в разработке политик безопасности, политик управления доступом и информационными потоками в компьютерных сетях.	ПКР-2.1 Знать виды политик управления доступом и информационными потоками в компьютерных сетях. ПКР-2.2 Уметь обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях. ПКР-2.3 Владеть навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

4 зачетных единиц (144 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 7
Контактная работа	96	96,15
Аудиторные занятия (всего):	96	96
В том числе:		
лекции (Л)	48	48
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	48	48
Самостоятельная работа (всего)	48	48
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

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

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	7	Раздел 1 Понятие защищенной операционной системы Методы создания защищенных информационных систем	4				4	8	
2	7	Раздел 2 Теоретические основы защиты ОС Стандарты защищенности. Формальное представление политик безопасности	4				4	8	
3	7	Раздел 3 Методы защиты операционных систем Структура безопасной операцион-ной системы	6	6			4	16	
4	7	Раздел 4 Конфигурирование безопасной загрузки Механизмы загрузки Windows NT	6	4			4	14	, Контрольный опрос
5	7	Раздел 5 Реализация механизмов защиты в операционных системах Аппаратная поддержка защиты в операционных системах платформы x86 Модель безопасности ОС Windows архитектуры NT. Структура и состав подсистем безопасности Контроль многопользовательского доступа. Механизмы ау-тентификации. Управление учет-ными записями. Контроль доступа к ресурсам. Механизмы авторизации. Права и привилегии доступа. Защита и шифрование данных в файловых системах.	6	6			4	16	, Контрольный опрос

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
6	7	Раздел 6 Администрирование локальной безопасности Управление учетными записями пользователей и групп. Политики учетных записей. Аудит и журналирование событий безопасности	6	6			4	16	ПК1, Контрольный опрос, ТК1
7	7	Раздел 7 Командный режим управления. Символические имена и маски. Перенаправление информационного потока. Базовые, сервисные и информационные команды	4	6			6	16	, Контрольный опрос
8	7	Раздел 8 Автоматизация администрирования . Язык сценариев. Командные файлы. Параметры запуска, пе-ременные и операции над ними. Реализация разветвлений и циклов в сценариях	4	6			6	16	
9	7	Раздел 9 Мониторинг производительности и процессов	4	6			6	16	ПК2, Контрольный опрос, ТК2
10	7	Раздел 10 Планирование и управление заданиями	4	8			6	18	
11	7	Раздел 11 Итоговая аттестация						0	ЗаО
12		Всего:	48	48			48	144	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 48 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	7	РАЗДЕЛ 3 Методы защиты операционных систем	Лабораторная работа №1 Использование средств виртуализации	6
2	7	РАЗДЕЛ 4 Конфигурирование безопасной загрузки	Лабораторная работа №2 Конфигурирование мультизагрузки операционных систем Windows 5.x, 6.x.	4
3	7	РАЗДЕЛ 5 Реализация механизмов защиты в операционных системах	Лабораторная работа №3 Применение разрешений NTFS.	6
4	7	РАЗДЕЛ 6 Администрирование локальной безопасности	Лабораторная работа №4. Управление учетными записями и аудит.	6
5	7	РАЗДЕЛ 7 Командный режим управления.	Лабораторная работа №5 . Интерактивный командный режим Windows.	6
6	7	РАЗДЕЛ 8 Автоматизация администрирования	Лабораторная работа №6 Разработка сценариев консольного режима	6
7	7	РАЗДЕЛ 9 Мониторинг производительности и процессов	Лабораторная работа №7 Мониторинг производительности и процессов	6
8	7	РАЗДЕЛ 10 Планирование и управление заданиями	Лабораторная работа №8. Планирование заданий.	8
			ВСЕГО:	48/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовых проектов/работ учебным планом не предусмотрено.

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. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	7	РАЗДЕЛ 1 Понятие защищенной операционной системы	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам. Изучение учебной литературы из приведенных источников: [7,8,10,11]	4
2	7	РАЗДЕЛ 2 Теоретические основы защиты ОС	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам. Изучение учебной литературы из приведенных источников: [7,8,10,11]	4
3	7	РАЗДЕЛ 3 Методы защиты операционных систем	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам 2. Изучение учебной литературы из приведенных источников: [8,10,11] 3. Подготовка к выполнению лабораторной ра-боты №1	4
4	7	РАЗДЕЛ 4 Конфигурирование безопасной загрузки	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам 2. Изучение учебной литературы из приведенных источников: [2] 3. Подготовка к выполнению лабораторной ра-боты №2	4
5	7	РАЗДЕЛ 5 Реализация механизмов защиты в операционных системах	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам. 2. Изучение учебной литературы из приведенных источников: [4,5,6] 3. Подготовка к выполнению лабораторной ра-боты №3	4
6	7	РАЗДЕЛ 6 Администрирование локальной безопасности	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам Изучение учебной литературы из приведенных источников: [4,5] 3. Подготовка к выполнению лабораторной ра-боты №4	4
7	7	РАЗДЕЛ 7 Командный режим управления.	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам. 2. Изучение учебной литературы из приведенных источников: [1] 3. Подготовка к выполнению лабораторной ра-боты №5	6
8	7	РАЗДЕЛ 8 Автоматизация	Изучение, анализ и дополнительная проработка лекционного материала по	6

		администрирования	соответствующимй темам 2. Изучение учебной литературы из приведенных источников: [1] 3. Подготовка к выполнению лабораторных ра-бот №6	
9	7	РАЗДЕЛ 9 Мониторинг производительности и процессов	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам 2. Изучение учебной литературы из приведенных источников: [3] 3. Подготовка к выполнению лабораторной работы №7	6
10	7	РАЗДЕЛ 10 Планирование и управление заданиями	Изучение, анализ и дополнительная проработка лекционного материала по соответствующимй темам. . Изучение учебной литературы из приведенных источников: [3] 3. Подготовка к выполнению лабораторной ра-боты №8	6
			ВСЕГО:	48

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Командная строка и сценарии Windows. Учебное пособие	Ларина Т.Б	М.: МИИТ, 2014 НТБ, ауд.1332 (140), 2014 НТБ МИИТ	Разделы 7-8
2	Дисковые структуры операцион-ных систем. Учебное пособие	Ларина Т.Б.	М.:МИИТ, 2011 НТБ 5 - фб.(3), чз.1(2) 1332 (50), 2011 НТБ МИИТ	Раздел 4
3	Администрирование операцион-ных систем. Мониторинг и пла-нирование заданий: Учебное по-собие.	Ларина Т.Б.	- М.: РУТ (МИИТ),2018. – 75 с. , 2018 НТБ МИИТ	Разделы 9,10
4	Администрирование локальных сетей Windows NT. Учебное по-собие для вузов.	Назаров С.В	Финансы и статистика М.: 2011 335с. , 2011 НТБ МИИТ	Разделы 1-6
5	Администрирование сетей на платформе MS Windows Server	Власов Ю.В., Риц-кова Т.И.	БИНОМ М.: 2012 г. 384 стр. НТБ, 2012 НТБ МИИТ	Разделы 1, 6
6	Аппаратно-программные основы операционных систем платформы x86	Т.Б.Ларина	М.:МИИТ, 2009 НТБ 5 - фб.(3), чз.1(2) 1332 (60), 2009 НТБ МИИТ	Раздел 5
7	Комплексная защита информа-ции в корпоративных системах. Учеб. пособие для вузов	В.Ф. Шаньгин	М. : Форум, ИНФРА-М, 2017. - 592 с. : Фб – 3 экз, 2017 НТБ МИИТ	Раздел 1-3

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
8	Операционные системы. Концепции построения и обеспечения безопасности.	Ю.Ф. Мартемьянов, Ал.В. Яковлев,	-М.: Горячая линия - Телеком, 2011. -332 с. , 2011 НТБ МИИТ	Раздел 2 - 3
9	Самоучитель системного адми-нистратора	Кенин А.М.	Кенин А.М.СПб: БХВ-Петербург, 2008 , 2008	Разделы 3-8

			НТБ МИИТ	
10	Защита в операционных системах.	В.Г.Проскурин	М.: Горячая линия – Телеком, 2016, -192 , 2016 НТБ МИИТ	Раздел 2 - 4

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- https://drive.google.com/drive/my-drive - авторские методические материалы на файловом сервере в общем доступе для использования студентами
- http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ
- http://elibrary.ru/ - научно-электронная библиотека.
- http://www.intuit.ru - сайт Интернет-университета информационных технологий
- поисковые системы: Yandex, Google

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекций используется специализированная аудитория, оснащенная мультимедийным проекционным оборудованием и персональным компьютером. Для проведения лабораторных занятий используется учебный класс с персональными компьютерами. Требования к компьютерам: процессор не ниже Pentium4, операционная система от Windows XP и старше, доступ в Интернет
Используемое программное обеспечение:
- Microsoft Office 2010 или старше для создания рисунков, презентаций и мультимедийных компонентов лекций;
- система виртуализации операционных систем Microsoft Virtual PC 2007 (в свободном доступе)
- авторская программная система тестирования знаний
Электронные версии методических материалов, дистрибутивы программных средств размещены на файл-сервере ауд.1332 и доступны для доступа со студенческих компьютеров в локальной сети по ссылке: \1332srv\Учебные материалы \Администрирование

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Требования к аудиториям для проведения занятий
Перечень технических средств обучения, используемых в учебном процессе для освоения дисциплины:
- мультимедийное оборудование лекционной аудитории 1329: компьютер, проектор, лазерная указка
- персональные компьютеры учебного вычислительного класса с необходимым программным обеспечением
Требования к программному обеспечению при прохождении учебной дисциплины
- Microsoft Office 2010 или старше, система виртуализации операционных систем

Microsoft Virtual PC 2007 (свободно распространяемая), дисковый редактор HxD Hex Editor (в свободном доступе), дисковый менеджер Minitools Partition Wizard Free (в свободном доступе)
- авторская программная система тестирования знаний

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для эффективного освоения курса важна последовательность и непрерывность работы студенты в семестре для получения и закрепления основных знаний и навыков.
Студент должен четко представлять правила и последовательность работы, на это надо обратить особенное внимание на вводной лекции. Обратить внимание студентов на то, что успешное завершение курса возможно только при последовательной и непрерывной работе в семестре.
Лекции и практические занятия представляют собой содержательно единые занятия.
Текущая работа на практических занятиях требует активной работы. Пропуск занятий недопустим.
Студент должен быть подготовлен к выполнению очередной лабораторной работы в результате самостоятельной домашней работы и индивидуальных консультаций преподавателя.
Текущая оценка успеваемости. Критериями оценки являются работа на занятиях, ответы на контрольные вопросы. выполнение индивидуальных заданий. Студент получает оценки текущего контроля на 8-й неделе и 12-й неделе семестра (РИТМ), оценку промежуточного контроля - на зачете. При суммарной оценке РИТМ менее 3, студент не получает допуск на зачет. Отмечается «невыполнение учебной программы курса».