МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Системное администрирование

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 26.10.2022

1. Общие сведения о дисциплине (модуле).

Целями изучения дисциплины «Системное администрирование» являются:

- изучение основ системного управления и администрирования операционных си-стем;

- изучение методов и технологий, используемых при развертывании, управлении и сопровождении компьютерных систем.

Задачами дисциплины являются:

- получение студентами знаний о задачах, направлениях и инструментах систем-ного администрирования;

- овладение современными средствами управления ресурсами, пользователями и процессами в целях безопасности;

- получение знаний и навыков автоматизирования операций обслуживания ком-пьютерных систем, создания и поддержки безопасной информационной среды.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1.1 - Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;

ОПК 1.2 - Способен администрировать средства защиты информации в компьютерных системах и сетях ;

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ;

ПК-3 - способностью администрировать подсистемы информационной безопасности объекта защиты .

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- уровни автоматизации управления системой,

- механизмы и политики локальной безопасности и управления доступом к ресурсам,

- концепции и инструменты системного аудита,

- языковые средства разработки сценариев управления,

- средства мониторинга производительности системы, планирования и управления заданиями.

Уметь:

Уметь:

- организовать защиту данных пользователей средствами файловой системы,
- настраивать и использовать средства аудита событий безопасности,
- автоматизировать выполнение рутинных задач администрирования, создавать сценарии управления,
- планировать выполнение административных задач по времени и расписанию.

Владеть:

- навыками конфигурирования загрузки операционных систем,
- навыками использования командного интерфейса для взаимодействия с операционной системой,
- средствами настройки аудита ресурсов и пользователей и навыками планирования аудита событий в системе,
- навыками разработки сценариев для автоматизации управления системой,
- навыками планирования и управления заданиями администрирования.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №7
Контактная работа при проведении учебных занятий (всего):	96	96
В том числе:		
Занятия лекционного типа	48	48

Занятия семинарского типа	48	48

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 48 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	1 Введение в курс Рассматриваемые вопросы: - задачи и цели системного администрирования, уровни автоматизации управления; - особенности операционных систем на платформе защищенного режима процессора; - внутренняя структура операционных систем архитектуры NT 2 Конфигурирование загрузки операционных систем Рассматриваемые вопросы: - процесс загрузки системы с жесткого диска, алгоритм главного загрузчика; - конфигурирование загрузки операционных систем Windows NT, конфигурационные файлы и средства их редактирования; - менеджеры загрузки, организация мультизагрузочных конфигураций на жестком диске. 3 Управление системным реестром Рассматриваемые вопросы: - структура системного реестра; - иерархическое дерево базы данных: кусты HKLM, HKCC, HKU, HKCU, HKCR. - параметры реестра, работа с редактором реестра regedit. 4 Механизмы локальной безопасности Рассматриваемые вопросы: - механизмы регистрация, аутентификации, авторизация и аудита; - структура подсистемы безопасности NT; - структуры данных безопасности: списки управления доступом ACL, маркер доступа.

№ п/п	Тематика лекционных занятий / краткое содержание
	5 Средства безопасности файловой системы. Рассматриваемые вопросы: - разрешения файловой системы NTFS и типы разрешений; - правила применения разрешений; - влияние операций над объектами на разрешения; - шифрование объектов на логических дисках NTFS. 6 Средства администрирования локальной безопасности Рассматриваемые вопросы: - консоль управления MMC и ее оснастки; - управление учетными записями пользователей и групп; права и привилегии доступа; - встроенные и специальные учетные группы, операции с учетными записями, политики учетных записей. 7 Локальные политики Рассматриваемые вопросы: - политики аудита; - политики назначения прав пользователя; - политики параметров безопасности; - просмотр событий с помощью системных журналов. 8 Командный режим управления Рассматриваемые вопросы: - синтаксис командного интерпретатора CMD в интерактивном режиме; - символические имена и маски имен; - способы перенаправления информационного потока команды, конвейеры команд; - базовые команды работы с дисками и файловой системой; - сервисные и информационные команды, команды-фильтры. 9 Основы языка сценариев командного интерпретатора CMD Рассматриваемые вопросы: - командные файлы сценариев, язык пакетного режима, создание и редактирование командных файлов; - параметры запуска командных файлов и операции над ними; - переменные в сценарии, операции над строковыми и числовыми переменными. 10 Разветвления в сценариях Рассматриваемые вопросы: - безусловная передача управления в командных файлах, - процедурный вызов командного файла; - условные переходы по соотношению переменных, по факту существования объекта или переменной, по коду завершения предыдущей команды. 11 Организация циклов в сценариях Рассматриваемые вопросы: - цикл над элементами множества строковых значений; - циклы действий над файлами /каталогами по маске имени; - циклы над объектами в заданном дереве подкаталогов; - арифметический цикл.. 12 Обработка текстовых строк Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- способы обработка строк из текстовых файлов; - настройка параметров выделения подстрок - обработка строк информационного потока выхода команды. 13 Мониторинг производительности Рассматриваемые вопросы: - оснастка системного монитора консоли управления MMC; - настройка счетчиков производительности, создание групп сборщиков данных; - мониторинг производительности из командной строки. 14 Мониторинг процессов Рассматриваемые вопросы: - получение сведений о процессах, службах, библиотеках и их зависимостях; - фильтрация сведений по множественным условиям; - останов и удаление процессов 15 Планирование и управление заданиями Рассматриваемые вопросы: - планировщик заданий консоли MMC, создание заданий; - использование триггеров, основанных на времени и на событиях, действия и условия запуска заданий; - планирование заданий в командной строке, консольный планировщик SchTasks; - создание заданий, запускаемых по расписанию и событийно-управляемых заданий; - ручное управление заданиями.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	1 Конфигурирование загрузки. В результате выполнения работы студент получает практические навыки конфигурирования загрузки операционных систем, организация выборочной мультизагрузки нескольких операционных систем с одного жесткого диска 2 Применение разрешений файловой системы NTFS. В результате выполнения работы студент на практике закрепляет знание механизмов и правил применений разрешений файловой системы NTFS, как элементов безопасности в общей системе безопасности Windows NT 3 Политики и настройки аудита. В результате выполнения работы студент знакомится со штатными средствами администрирования локального компьютера, приобретает навыки настройки политики аудита и анализ журнала безопасности. 4 Интерактивный командный режим. В результате выполнения работы студент приобретает практические навыки и умения работы в интерактивном командном режиме операционных систем NT.

№ п/п	Наименование лабораторных работ / краткое содержание
	5 Параметры и переменные командных файлов. В результате выполнения работы студент закрепляет знания синтаксиса пакетного командного режима, навыки использования операций над параметрами и переменнами сценариев. 6 Разработка разветвленных сценариев управления. В результате выполнения индивидуального задания студент приобретает опыт разработки нелинейных сценариев администрирования, навыки создания командных файлов с использованием разветвлений и циклов. 7 Мониторинг производительности. В результате выполнения работы студент приобретает навыки и умения использования средств системного монитора для мониторинга объектов производительности системы в графическом и консольном режиме. 8 Планирование заданий. В результате выполнения индивидуального задания студент знакомится с инструментами планирования административных заданий и приобретает навыки разработки сценариев автоматического запуска задач в графическом и консольном режиме.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Анализ и проработка лекционного материала
2	Изучение рекомендуемой учебной литературы
3	Освоение инструментов администрирования в консольном и графическом режимах опеарционной системы
4	Подготовка выполнения заданий по лабораторным работам
5	Подготовка отчетов о выполнении лабораторных работ
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Ларина Т.Б. Командная строка и сценарии Windows. Учебное пособие. М.:МИИТ, 2014. – 96 с.	каф.ВССиИБ, ауд.1332. - 150 экз.
2	Ларина Т.Б. Дисковые структуры операционных систем.	http://195.245.205.171:8087/jirbis2/books/scanbooks_new/13-138.pdf (дата обращения: 25.01.2022). - Текст : непосредственный.;каф.ВССиИБ, ауд.1332. - 100 экз.

	Учебное пособие. М: МИИТ, 2011. - 173 с.	
3	Ларина Т.Б. Администрирование операционных систем. Мониторинг и планирование заданий: Учебное пособие. М.:МИИТ, 2018. – 75 с.	http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/DC-901.pdf (дата обращения: 25.01.2022). - Текст : непосредственный.;каф.ВССиИБ, ауд.1332. - 100 экз.
4	Ларина Т.Б. Виртуализация операционных систем. Учебное пособие. - М.: РУТ (МИИТ), 2020. - 65 с.	http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/DC-1368.pdf (дата обращения: 25.01.2022). - Текст : непосредственный ;каф.ВССиИБ, ауд.1332. - 30 экз
5	Ларина Т.Б. Администрирование операционных систем. Управление системой. Учебное пособие. - М.: РУТ (МИИТ), 2020. - 71 с.	http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/DC-1384.pdf (дата обращения: 25.01.2022). - Текст : непосредственный.;каф.ВССиИБ, ауд.1332. - 30 экз.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) http://miit.ru

Научно-техническая библиотека РУТ (МИИТ): http://library.miit.ru

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Оерационная система Microsoft Windows, Microsoft Office.

Программные средства виртуализации операционных систем MS Virtul PC, Oracle VirtualBox или VMWare WS.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Лекционная аудитория, оснащенная компьютером и проектором. Персональные компьютеры в учебной лаборатории с необходимым программным обеспечением. В случае проведения дистанционных занятий

необходимо наличие средств для организации удаленных коммуникаций.

9. Форма промежуточной аттестации:

Зачет в 7 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы

Доцент, доцент кафедры «Вычислительные системы, сети и информационная безопасность»	Ларина Татьяна Борисовна

Лист согласования

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А. Клычева