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 магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность операционных систем

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цели и задачи изучения дисциплины определяются характеристиками области и объектов профессиональной деятельности магистра направления подготовки «Информационная безопасность».

Целями освоения дисциплины «Безопасность операционных систем» являются:

- изучение способов логической организации компьютерных сетей;
- изучение методов и технологий, используемых при развертывании, управлении и сопровождении защищенных компьютерных сетей на базе серверных операционных систем.

Задачами дисциплины являются:

- приобретение знаний и умений, необходимых для логического проектирования, конфигурирования и сопровождения защищенных компьютерных сетей на базе серверных операционных систем;
- получение навыков и умений для развертывания и управления защищенными доменными структурами компьютерных сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ОПК-5 - Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-1 - Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

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

Знать:

- принципы логической организации сети;
- средства системного администрирования;

- инструменты управления, защиты и мониторинга в сети.

Уметь:

- проектировать логическую организацию сети;
- применять административные инструменты для конфигурирования сети;
- управлять службами сетевой инфраструктуры.

Владеть:

- навыками решения задач организации сетевого взаимодействия;
- навыками управления объектами сети через централизованные службы каталогов;
- навыками защиты ресурсов сети.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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	Семестр №2
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 116 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	Конфигурирование и настройка Microsoft Windows Server Рассматриваемые вопросы: - конфигурирование и настройка сервера - настройка сетевых параметров, параметров безопасности и производительности
2	Организация сетей на базе Microsoft Windows Server Рассматриваемые вопросы: - модель логической организации сети «рабочая группа» - модель логической организации сети «домен», сравнительные характеристики
3	Логическая и физическая структура Active Directory Рассматриваемые вопросы: - структурные элементы Active Directory: объекты и их классы, домены, организационные подразделения, деревья, леса - физическая структура Active Directory: контроллер доменов, сайты
4	Центральная служба каталогов Active Directory Рассматриваемые вопросы: - создание сетевого домена - оснастки консоли администрирования для работы с доменами
5	Управление объектами в Active Directory. Учетные записи пользователей и групп Рассматриваемые вопросы: - учетные записи и политика именования - управление доменными учетными записями
6	Управление объектами Active Directory. Организационные подразделения Рассматриваемые вопросы: - управление организационными подразделениями - делегирование административных полномочий управления в подразделении
7	Администрирование сетевых служб DHCP и WINS Рассматриваемые вопросы: - служба DHCP автоматического конфигурирования TCP/IP - служба WINS разрешения символических имен узлов; конфигурирование и обслуживание службы
8	Администрирование сетевой службы DNS Рассматриваемые вопросы: - служба DNS разрешения доменных имен узлов; - схемы разрешения запросов на разрешение имен, конфигурирование службы
9	Механизмы безопасности MS Windows Server Рассматриваемые вопросы: - общая модель безопасности Windows Server, права, привилегии и разрешения доступа, встроенные и специальные группы - защита ресурсов с помощью прав доступа по сети, администрирование доступа к общим ресурсам
10	Защита ресурсов сети Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- защита ресурсов разрешениями файловой системы NTFS, администрирование доступа с помощью разрешений NTFS - совместное применение прав сетевого доступа и разрешений файловой системы
11	Многодоменные структуры сети Рассматриваемые вопросы: - многодоменная модель организации сети, доверительные отношения между доменами - транзитивная аутентификация в многодоменной сети, реализация прав доступа в многодоменной сети
12	Доменные модели Рассматриваемые вопросы: - доменные модели: модель одиночного домена, модель с одним главным доменом, модель с несколькими главными доменами, модель с полным доверием - иерархическая система доменов: деревья и леса
13	Отказоустойчивые и производительные дисковые конфигурации Рассматриваемые вопросы: - базовые конфигурации дисковых структур - технологии дисковых массивов (RAID) - характеристики RAID-технологии, уровни спецификаций
14	Программные реализации RAID на динамических дисках в MS Windows Server Рассматриваемые вопросы: - набор томов JBOD - чередующийся набор RAID0 - зеркальный набор RAID1 - чередующийся набор с четностью RAID5
15	Мониторинг событий безопасности сети Рассматриваемые вопросы: - политики аудита и управление аудитом, - настройки аудита для объектов файловой системы; анализ журнала безопасности
16	Мониторинг ресурсов и сетевого трафика Рассматриваемые вопросы: - мониторинг производительности и процессов, - мониторинг сетевого трафика, сетевой монитор и его использование

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Создание виртуальных машин В результате выполнения работы студент получает практические навыки использования средств виртуализации, установки серверных ОС
2	Создание одноранговой сети В результате выполнения работы студент получает навыки создания виртуальной одноранговой сети, настройки сетевой идентификации и проверки сетевого взаимодействия
3	Конфигурирование сервера В результате выполнения работы студент получает практические навыки установки и конфигурирования параметров сервера
4	Создание сетевого домена

№ п/п	Наименование лабораторных работ / краткое содержание
	В результате выполнения работы студент получает навыки логической конфигурации сетевого домена, установка и настройки основных служб сетевой доменной инфраструктуры
5	Управление объектами Active Directory. Учетные записи В результате выполнения работы студент получает практические навыки создания и настройки доменных учетных записей пользователей и групп
6	Управление объектами Active Directory. Парольная политика, профили и сценарии В результате выполнения работы студент получает практические навыки настройки в домене парольной политики, перемещаемых профилей и сценариев входа пользователей в домен
7	Управление организационными подразделениями В результате выполнения работы студент получает практические навыки структурирования объектов домена в организационные подразделения, делегирования административных полномочий и проверки их работоспособности
8	Защита ресурсов сети с помощью разрешений общего доступа по сети В результате выполнения работы студент получает практические навыки настройки избирательного доступа пользователей домена к общему сетевому ресурсу, проверки эффективных разрешений в комбинации личных и групповых сетевых разрешений
9	Защита ресурсов сети с помощью разрешений NTFS. В результате выполнения работы студент получает практические навыки использования разрешений файловой системы для защиты доступа к файлам и каталогам
10	Совместное использование разрешений сетевого доступа и разрешений файловой системы В результате выполнения работы студент закрепляет на практике понимание механизмов совместного действия разрешений разного типа для защиты общего ресурса сети
11	Многодоменные структуры сети В результате выполнения работы студент получает опыт создания многодоменной сети виртуальных узлов, настройки доверительных отношений между доменами, проверки действия доверительных отношений
12	Защита ресурсов в многодоменной сети В результате выполнения работы студент закрепляет знания о механизмах действия разрешений общего доступа и разрешений файловой сиситемы в многодоменной сети
13	Дисковые массивы Raid5 и Raid0 В результате выполнения работы студент получает навыки конфигурации сервера с несколькими дисковыми накопителями, создания программного RAID-массива типа Raid5 и Raid0, проверки характеристик отказоустойчивости
14	Дисковые массивы Raid1 и Jbod В результате выполнения работы студент получает навыки создания программных массивов дисков типа Raid1 и Jbod и проверки их характеристики отказоустойчивости
15	Мониторинг событий сети В результате выполнения работы студент получает опыт использования средств аудита для наблюдения собитий безопасности в сети
16	Мониторинг ресурсов сети В результате выполнения работы студент приобретает умения и навыки анализа сетевого трафика, использования штатных средств мониторинга производительности сети

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Анализ и проработка лекционного материала
2	Изучение рекомендуемой учебной литературы
3	Подготовка к выполнению заданий по лабораторным работам
4	Подготовка отчетов о выполнении лабораторных работ
5	Выполнение курсовой работы.
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

В рамках курсовой работы требуется выполнить анализ организации и функционирования заданной службы серверной операционной системы или технологии, ориентированной на обеспечение безопасности.

Примерный перечень тем:

- ICS. Служба общего доступа к подключению Интернет
- Служба агента политик безопасности IPSec
- NAP. Технология защита доступа сети
- Службы сертификации Windows
- Технологии шифрования дисков – BitLocker
- Центр обеспечения безопасности (Windows Security Center)
- Технологии VPN в организации безопасных сетей
- Межсетевые экраны. Брандмауэр Windows
- NPS - сервер сетевых политик
- Службы SRP(Software Restriction Policy) и AP Locker
- Служба Kerberous
- Биометрическая аутентификация (Windows Biometric Framework)
- Служба шифрования данных - Encripting File System
- Служба управления правами -RMS (Rights Management Services)
- Защитник Windows(Microsoft Defender)

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

№ п/п	Библиографическое описание	Место доступа
1	Ларина Т.Б.Сетевые операционные системы. Учебное пособие. М.:РУТ(МИИТ), 2021. – 106 с.	http://library.miit.ru/bookscatalog/upos/DC-1512.pdf (дата доступа: 16.03.2024). - Текст : непосредственный.
2	Ларина Т.Б. Виртуализация операционных систем. Учебное пособие. - М.: РУТ (МИИТ), 2020. - 65 с.	http://library.miit.ru/bookscatalog/metod/DC-1368.pdf (дата обращения: 16.03.2024). - Текст : непосредственный;каф.ВССиИБ, ауд.1332. - 30 экз
3	Ларина Т.Б. Администрирование сетей. Логическая организация и конфигурирование: Учебное пособие. -М.: РУТ (МИИТ), 2017. – 170 с	http://library.miit.ru/bookscatalog/metod/DC-410.pdf (дата обращения: 16.03.2024).Текст : непосредственный.каф.ВССиИБ, ауд.1332. - 50 экз
4	Ларина Т.Б. Администрирование сетей. Защита ресурсов и мониторинг: Учебное пособие. - М.: РУТ (МИИТ), 2018. – 91 с.	http://library.miit.ru/bookscatalog/metod/DC-900.pdf (дата обращения: 16.03.2024). - Текст : непосредственный.каф.ВССиИБ, ауд.1332. - 50 экз
5	Рицкова Т.И., Власов Ю.В. Администрирование сетей на платформе MS Windows Server. -М.: Национальный открытый университет «ИНТ УИТ», 2016, - 622 с. - ISBN 978-5-94774-858-1	https://www.studmed.ru/olifer-vg-olifer-na-kompyuternye-seti-principy-tehnologii-protokoly-4-e-izd_a3dbdb7967a.html (дата обращения 16.03.2024). - Текст : непосредственный.
6	Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебное пособие для вузов СПб:, Питер, 4-е изд., 2010, -916 с.	https://www.studmed.ru/olifer-vg-olifer-na-kompyuternye-seti-principy-tehnologii-protokoly-4-e-izd_a3dbdb7967a.html (дата обращения 16.03.2024). - Текст : непосредственный.

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

Национальный открытый университет «ИНТУИТ» https://intuit.ru/

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

- Microsoft Windows
- Microsoft Office
- Программные средства виртуализации операционных систем: Microsoft VirtualPC, VMWare WS, Oracle VirtualBox

- При проведении занятий с применением дистанционных образовательных технологий могут применяться средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, WhatsApp.

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:

Курсовая работа во 2 семестре.
Экзамен во 2 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» Т.Б. Ларина

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова