

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

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: 19.10.2022

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 | Сем. №2 |
| Контактная работа при проведении учебных занятий (всего): | 48 | 48 |
| В том числе: | | |
| Занятия лекционного типа | 16 | 16 |
| 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 132 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 | <p>1 Организация сетей на базе Microsoft Windows Server Рассматриваемые вопросы: - конфигурирование и настройка сервера; - удаленное администрирование; - настройка сетевых параметров; - модели логической организации сети: «рабочая группа» и «домен», сравнительные характеристики.</p> <p>2 Центральная служба каталогов Active Directory. Рассматриваемые вопросы: - структурные элементы Active Directory: объекты и их классы, домены, организационные подразделения, деревья, леса; - физическая структура Active Directory: контроллер доменов, сайты; - создание сетевого домена; - оснастки консоли администрирования для работы с доменами.</p> <p>3 Управление объектами службы каталогов Active Directory Рассматриваемые вопросы: - учетные записи и политика именования; - управление доменными учетными записями; - настройки профилей и сценариев входа; - управление организационными подразделениями; - делегирование административных полномочий управления в подразделении.</p> <p>4 Администрирование сетевых протоколов и служб разрешения символических имен. Рассматриваемые вопросы: - сетевые протоколы и конфигурирование TCP/IP. Служба DHCP автоматического конфигурирования TCP/IP; - служба WINS разрешения символических имен узлов; конфигурирование и обслуживание службы. - служба DNS разрешения доменных имен узлов; схемы разрешения запросов на разрешение имен, конфигурирование службы.</p> <p>5 Защита ресурсов сети 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. - защита ресурсов разрешениями файловой системы NTFS, администрирование доступа с помощью</p> |

| № п/п | Тематика лекционных занятий / краткое содержание |
|----------|--|
| | <p>разрешений NTFS, совместное применение прав сетевого доступа и разрешений файловой системы.</p> <p>6 Многодоменные структуры сети Рассматриваемые вопросы: - многодоменная модель организации сети, доверительные отношения между доменами, транзитивная аутентификация в многодоменной сети, реализация прав доступа в многодоменной сети. - 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.</p> <p>7 Отказоустойчивые и производительные дисковые конфигурации Рассматриваемые вопросы: - технологии дисковых массивов (RAID, характеристики RAID-технологии, уровни спецификаций; - программные реализации RAID на динамических дисках в MS Windows Server: набор томов, чередующийся набор RAID0, зеркальный набор RAID1, чередующийся набор с четностью RAID5.</p> <p>8 Мониторинг ресурсов и событий сети Рассматриваемые вопросы: - политики аудита, управление аудитом, настройки аудита для объектов файловой системы; - мониторинг производительности и процессов, анализ данных производительности, - мониторинг сетевого трафика, сетевой монитор и его использование для анализа сетевого трафика.</p> |

4.2. Занятия семинарского типа.

Лабораторные работы

| № п/п | Наименование лабораторных работ / краткое содержание |
|----------|---|
| 1 | <p>1 Создание виртуальной компьютерной сети. В результате выполнения работы студент получает практические навыки использования средств виртуализации, создания одноранговой сети из виртуальных узлов, настройки сетевой идентификации и проверки сетевого взаимодействия.</p> <p>2 Доменная логическая организация сети. В результате выполнения работы студент получает практические навыки установки и конфигурирования параметров безопасности сервера, создания сетевого домена, установки и настройки основных служб сетевой доменной инфраструктуры.</p> <p>3 Управление объектами службы каталогов Active Directory. В результате выполнения работы студент получает практические навыки создания и настройки доменных учетных записей пользователей и групп, структурирования учетных записей в организационные подразделения с делегированием административных полномочий.</p> <p>4 Защита ресурсов сети с помощью разрешений общего доступа по сети и разрешений NTFS. В результате выполнения работы студент получает практические навыки настройки избирательного доступа пользователей домена к общему сетевому ресурсу, реализации аудита доступа к общим ресурсам для обнаружения попыток несанкционированного доступа.</p> <p>5 Многодоменные структуры сети. В результате выполнения работы студент закрепляет полученные знания о многодоменных структурах сети, настройке доверительных отношений между доменами, проверке действия доверительных</p> |

| № п/п | Наименование лабораторных работ / краткое содержание |
|-------|---|
| | отношений |
| | 6 Отказоустойчивые и производительные дисковые конфигурации. В результате выполнения работы студент закрепляет знания о RAID-технологиях, получает опыт организации различных видов программных RAID-массивов жестких дисков и проверки на практике отказоустойчивости и возможности восстановления информации на поврежденных дисках. |
| | 7 Мониторинг ресурсов и событий сети. В результате выполнения работы студент на практике получает опыт установки и настройки программного сетевого монитора, приобретает умения и навыки анализа сетевого трафика. |

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 серверной операционной системы |
| 4 | Подготовка к выполнению заданий по лабораторным работам |
| 5 | Подготовка отчетов о выполнении лабораторных работ |
| 6 | Выполнение курсовой работы. |
| 7 | Подготовка к промежуточной аттестации. |
| 8 | 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 Kerberos
- Биометрическая аутентификация (Windows Biometric Framework)
- Служба шифрования данных - Encrypting 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. – 96 с. | http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/DC-1512.pdf (дата доступа: 25.01.2022). - Текст : непосредственный. |
| 2 | 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 |
| 3 | Ларина Т.Б. Администрирование сетей. Логическая организация и конфигурирование: Учебное пособие. -М.: РУТ (МИИТ), 2017. – 170 с | http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/DC-410.pdf (дата обращения: 25.01.2022). - 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://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/DC-900.pdf (дата обращения: 25.01.2022). - Текст : непосредственный;каф.ВССиИБ, ауд.1332. - 50 экз |
| 5 | Власов Ю.В., Рицкова | https://www.studmed.ru/rickova-t-i-vlasov-yu-v-administrirovanie- |

| | | |
|---|--|--|
| | Т.И. Администрирование сетей на платформе MS Windows Server. БИНОМ М.:2012 г. - 384с. | setey-na-platfome-ms-windows-server_a7591b6b89c.html (дата обращения 25.01.2022). - 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-principyu-tehnologii-protokoly-4-e-izd_a3dbdb7967a.html (дата обращения 25.01.2022). - 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. Подписка МИИТ.

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, Zoom, 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»

Ларина Татьяна
Борисовна

Лист согласования

Заведующий кафедрой ВССиИБ
Председатель учебно-методической
комиссии

Б.В. Желенков

Н.А. Клычева