Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

 21.04.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.54 Администрирование и управление безопасностью интранет- сетей

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра информационных систем

6. Составители программы:

Коваль Андрей Сергеевич, koval@cs.vsu.ru, ст.преп, факультет компьютерных наук, кафедра информационный систем

7. Рекомендована:

Научно-методическим советом ФКН, протокол НМС №5 от 10.03.2021

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

изучение методологии и технологий администрирования информационных систем (ИС). Ставятся задачи: на лекционных занятиях познакомить студентов с организацией служб поддержки и основами администрирования ИС; на лабораторных занятиях студенты должны получить навыки практического администрирования компонентов реальных ИС - оборудования IP-сетей и сетевых операционных систем.

10. Место учебной дисциплины в структуре ООП:

Входные знания: «Информационные сети», «Основы ОС UNIX», «Операционные системы».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.1 знает виды политик управления доступом и информационными потоками в компьютерных сетях	Входные знания: «Информационные сети», «Основы ОС UNIX», «Операционные системы».
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.2 умеет настраивать правила обработки пакетов в компьютерных сетях	иметь: компетенции в области составления списков доступа сетевого обоудования и конечных систем
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.3 владеет навыками управления средствами межсетевого экранирования в компьютерных сетях	владеть навыками управления средствами межсетевого экранирования аппараьных и встроенных в ОС конечных систем

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 7	Всего
Аудиторные занятия	68	68
Лекционные занятия	34	34
Практические занятия		0
Лабораторные занятия	34	34
Самостоятельная работа	40	40
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Задачи администрирования. Объекты администрирования	Задачи администрирования. Объекты администрирования. Системы сертификации специалистов ИТ, администраторов. Службы регистрации. Лабораторные темы: Методика администрирования сетевого оборудования CISCO. Виды оборудования.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2	Управление сетями.	Управление сетями. Операционная система IOS. Динамическая маршрутизация. RIP, EIGRP. Динамическая маршрутизация. OSPF, BGP. Технологии 2 уровня в корпоративных сетях. VLAN, xSTP, LACT. Проблемы безопасности на 2 уровне. Лабораторные темы: Операционная система сетевого оборудования IOS. Установка статических маршрутов и маршрутов по-умолчанию. Конфигурирование протоколов динамической маршрутизации RIP, EIGRP. Конфигурирование протоколов динамической маршрутизации OSPF, BGP. Конфигурирование NAT/PAT. Конфигурирование VTP, VLAN. Управление трафиком и списки доступа IOS. Расширенные списки доступа IOS. Администрирование лабораторной сети (индивидуальное задание).	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Службы каталогов.	Службы каталогов (пример - Active Directory). Службы управления конфигурацией. Административные шаблоны. Шаблоны безопасности. Лабораторные темы: Администрирование сетей на основе MS Windows Server 2003 и 2008. Знакомство с топологией лабораторной инфраструктуры. Планирование и размещение службы каталогов Active Directory. Уровни совместимости леса и домена для систем на основе Windows Server 2000, 2003 и 2008. Администрирование службы каталогов Active Directory. Администрирование учетных записей и ресурсов. Резервное копирование. Восстановление в случае аварии. Объекты групповой политики. Управление средой пользователя домена. Управление параметрами ОС компьютеров домена. Использование административных шаблонов. Объекты групповой политики. Установка ПО, развертывание ПО с помощью RIS, WDS.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
4	Оперативное управление и поддержка.	Оперативное управление и поддержка. Инсталляция компонентов ИС. Мониторинг системных событий и производительности. CIM. Аппаратно-программные платформы администрирования. Администрирование UNIX-подобных ОС. Лабораторные темы: Журналы производительности и оповещения. Администрирование UNIX-подобных систем: установки FreeBSD, GNU/Linux (SuSe), GNU/Linux (Gentoo), Solaris. Администрирование UNIX-подобных систем: системное администрирование и управление ПО (GNU/Linux).	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102
5	Обеспечение информационной безопасности ИС	Обеспечение ИБ - как задача управления рисками. Стратегии управления рисками, технологии внедрения управления рисками. Модели управления доступом, SELinux.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2	Управление сетями. (лаб.)	На выданном описании топологии сети представлена сеть организации, состоящая из N филиалов и центрального офиса. Необходимо сконфигурировать интранет сеть с использованием каналов поставщика услуг связи и доступ в Интернет через поставщика услуг Интернет, а также обеспечить доступ между филиалами (в т.ч. с требуемой схемой доступа) согласно описанию задания.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102
3	Службы каталогов. (лаб.)	Выполнить развертывание службы каталога AD и применить к контроллерам домена шаблоны безопасности. Показать преподавателю результат применения шаблонов и права пользователей соответствующих групп.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102
4	Оперативное управление и поддержка. (лаб.)	Развертывание сетевого экрана хоста. Конфигурирование iptables, ipfw. Развертывание SELinux . Конфигурирование политик SELinux.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2	Управление сетями. (практ.)	На выданном описании топологии сети представлена сеть организации, состоящая из N филиалов и центрального офиса. Необходимо сконфигурировать интранет сеть с использованием каналов поставщика услуг связи и доступ в Интернет через поставщика услуг Интернет, а также обеспечить доступ между филиалами (в т.ч. с требуемой схемой доступа) согласно описанию задания.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102
3	Службы каталогов. (практ.)	Выполнить развертывание службы каталога AD и применить к контроллерам домена шаблоны безопасности. Показать преподавателю результат применения шаблонов и права пользователей соответствующих групп.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102
4	Оперативное управление и поддержка. (практ.)	Развертывание сетевого экрана хоста. Конфигурирование iptables, ipfw. Развертывание SELinux . Конфигурирование политик SELinux.	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Задачи администрирования. Объекты администрирования	4			4	8
2	Управление сетями.	8	0	12	10	30
3	Службы каталогов.	8	0	8	12	28
4	Оперативное управление и поддержка.	8	0	8	8	24
5	Обеспечение информационной безопасности ИС	6	0	6	6	18
		34	0	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина требует работы с файлами-презентациями лекций и соответствующими главами рекомендованной основной литературы, а также, обязательного выполнения всех лабораторных заданий в компьютерном классе. Самостоятельная подготовка к лабораторным занятиям не требуется, т.к. необходимые рекомендации даются в аудитории, где выполняются лабораторные работы.

Самостоятельная работа проводится в компьютерных классах ФКН с использованием методических материалов расположенных на учебно-методическом сервере ФКН "\\fs.cs.vsu.ru\Library” и на сервере Moodle ВГУ moodle.vsu.ru и выполнением задач конфигурирования виртуализированной ИС. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Часть заданий может быть выполнена вне аудиторий на домашнем компьютере, после копирования методических указаний и необходимого ПО с учебно-методического сервера ФКН.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	*Сысоев, Э.В. Администрирование компьютерных сетей : учебное пособие / Э.В. Сысоев, А.В. Терехов, Е.В. Бурцева ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 80 с. : ил.— Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=499414*

№ п/п	Источник
2	*Гончарук, С.В. Администрирование ОС Linux / С.В. Гончарук. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 165 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=429014*

б) дополнительная литература:

№ п/п	Источник
1	*Курячий, Г.В. Операционная система Linux: Курс лекций. Учебное пособие / Г.В. Курячий, К.А. Маслинский. – Москва. : ДМК Пресс, 2010. – 348 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book_red&id=233108*
2	*Войтов Н.М. Администрирование ОС Red Hat Enterprise Linux. Учебный курс. – Москва : ДМК Пресс, 2011. – 192 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/1081*
3	*Вяткин, А.И. Проектирование локальных и корпоративных сетей: учебно-методический комплекс. Лабораторный практикум для студентов направления 09.03.02 «Информационные системы и технологии» профиля подготовки «Информационные системы и технологии в административном управлении» и направления 09.03.03 «Прикладная информатика» профиля подготовки «Прикладная информатика в экономике» очной формы обучения : [16+] / А.И. Вяткин ; отв. ред. И.Н. Глухих ; Тюменский государственный университет. – Тюмень : Тюменский государственный университет, 2016. – 103 с. : ил. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=574520*
4	*Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов : [16+] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 224 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=93351*

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	*Библиотека ВГУ, http://www.lib.vsu.ru*
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
2	ЭУМК «Администрирование в Информационных Системах», https://edu.vsu.ru/course/view.php?id=3102

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

1. Технологии виртуализации:

Среда виртуализации Microsoft Virtual PC

Среда виртуализации Oracle/Sun Virtual Box

2. Электронно-библиотечная система «Университетская библиотека online», http://biblioclub.ru

3. Образовательный портал Moodle (сервер Moodle ВГУ)

4. Серверные и клиентские ОС Microsoft.

5. Операционная система GNU/Linux (дистрибутив CentOS).

6. Аппаратные сетевые экраны D-Link, CISCO.

18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оснащенная видеопроектором.

2. Компьютерный класс для проведения лабораторных занятий, оснащенный программным обеспечением VirtualBox, VirtualPC, VirtualServer. Объем оперативной памяти на рабочее место не менее 2ГБ.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	1,2	ОПК-1.2	ОПК-1.2.1	Контрольная работа №1
2	3-5	ОПК-1.2	ОПК-1.2.2	Контрольная работа №2 Лабораторное задание №1,2
3	3-5	ОПК-1.2	ОПК-1.2.3	Контрольная работа №3 Лабораторное задание №3

Промежуточная аттестация

Форма контроля - Зачет с оценкой,Контрольная работа

Оценочные средства для промежуточной аттестации

Письменная итоговая контрольная работа. Выполнение всех лабораторных заданий и текущих контрольных.

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Перечень вопросов контрольных работ

№	Вопросы контрольной работы 1
1	Если правильная, то что означает команда: ip route 0.0.0.0 0.0.0.0 10.20.30.40 ? Если неправильная – поправьте и объясните.
2	На каких уровнях модели ISO/OSI можно проводить фильтрацию данных, используя списки доступа IOS?
3	В чем отличие протокола маршрутизации (routing protocol) от маршрутизируемого протокола (routed protocol)? Приведите примеры routing и routed протоколов.
4	Что означают символы O, C, R в листинге IOS таблицы маршрутизации, как возникают такие (O, C и R) записи?
5	В чем состоят задачи администрирования? Перечислите объекты администрирования?
6	К какой группе протоколов относится (и почему) RIP: к группе внешних или внутренних протоколов? А EIGRP? Какие существуют ограничения по применению EIGRP и RIP?
7	Если правильная, то что означает команда: access-list 110 permit ip any 0.0.0.0 255.255.255.255 ? Если неправильная – поправьте и объясните.
8	В чем особенности применения RIPng по сравнению с RIP?
9	В чем отличие NAT и PAT (NAT override)? В чем сложность реализации NAT для UDP пакетов по сравнению с TCP?
10	В чем отличие протокола маршрутизации «вектора состояния» (distance vector) от «состояния связи» (link state)? Какой протокол относится к классу “path vector”?
11	Если правильная, то что означает команда: access-class 123 in ? Если неправильная – поправьте и объясните.
12	Что такое IP таблица маршрутизатора, что в ней находится? Приведите пример таблицы, заполнив пару строк.
13	Почему схему адресации IPv4, основанная на классах, была заменена на CIDR? Что такое CIDR? Что такое VLSM?
14	Каковы основные особенности EIGRP? Как в IOS включается (E)IGRP маршрутизация (приведите пример последовательности команд и объясните действие каждой)?
15	Какие существуют команды IOS для проверки настройки списков доступа (просмотра списка правил и т.д.)?
16	Что такое внутренние и внешние протоколы (IGP, EGP)? Приведите примеры для каждого класса.
17	В чем преимущества, и какие есть потенциальные проблемы у динамической маршрутизации? Что такое конвергенция протокола маршрутизации?
18	Как в IOS задать IP-адрес для интерфейса? Приведите пример – серию команд (для адреса частной сети класса B).

19	Что такое административное расстояние. Для каких протоколов оно имеет большие значения и почему?
20	Если правильная, то что означает команда: ip access-group 123 in ? Если неправильная – поправьте и объясните.
21	Если правильная, то что означает команда: access-list 123 permit tcp any 0.0.0.0 255.255.255.255 eq 443 ? Если неправильная – поправьте и объясните.
22	Что такое списки доступа IOS, каких типов они бывают и для чего используются? Какие команды IOS нужно выполнить, чтобы воспользоваться списками доступа?
23	Если правильная, то что означает команда: ip route 163.4.0.0 255.255.0.0 10.1.1.1 ? Если неправильная – поправьте и объясните.
24	Что такое VLAN и как реализовано? Как назывался и чем отличался прототип этой технологии, разработанный CISCO?
25	Особенности протокола IS-IS, для чего он используется и каковы требования к сети при его использовании.
26	Если правильная, то что означает команда: access-list 11 permit tcp ip any any eq 80 ? Если неправильная – поправьте и объясните.
27	Какая команда (команды) IOS покажет маршрутную таблицу маршрутизатора?
28	Что такое агрегирование адресов, для чего используется? Что такое IP-подсеть и IP-суперсеть? Примеры.
29	Каковы основные особенности RIP? Как в IOS включается RIP (приведите пример последовательности команд и объясните действие каждой)?
30	В чем особенность области с номером 0 (Area 0) и какой протокол маршрутизации использует области?
31	В чем отличия RIP и EIGRP маршрутизаций, в каких случаях используют одну, а в каких - другую? Какие масштабные ограничения есть у RIP? Почему RIP иногда называют «маршрутизацией по слухам».
32	Если правильная, то что означает команда: ip route 15.15.0.0 255.255.0.0 151.150.150.150? Если неправильная – поправьте и объясните.
33	На каком оборудовании обычно необходимо выполнять конфигурирование VLAN? В чем состоит это конфигурирование (что нужно сделать, «по шагам»)?
34	Каковы основные отличия EIGRP от OSPF? К сетях какого масштаба используется OSPF и почему? В чем главное ограничение использования EIGRP? Какой из протоколов использует области (area) и для чего они нужны?
35	Назовите и опишите методы борьбы с петлями маршрутизации. Почему они возникают и как их избежать (способы)?
№	Вопросы контрольной работы 2
1	В чем сходство Directory Service с более ранними решениями: NYS+NFS. Опишите эти решения.
2	Как конфигурируются iptables? Как делаются изменения в текущей работе iptables и каким образом эти изменения можно сохранить, чтобы они остались и после перезагрузки ОС?
3	Как создать Active Directory? Что такое схема Active Directory, возможно ли ее изменение? Что такое и для чего используется динамический DNS (DDNS) в службе каталога AD.

4	Что такое служба каталога? Дайте определение и на этом определении покажите как именно реализованы в Microsoft Active Directory те элементы, которые упомянуты в Вашем определении службы каталога. Что такое DN и RDN?
5	В чем проблемы дискреционной политики безопасности (управления доступом)? Почему несмотря на эти проблемы DAC широко используется (практически во всех ОС)? Можно ли решить эти проблемы в рамках DAC и как?
6	Что такое GID, UID в классических UNIX ОС и как они используются для управления доступом? Какие возможности добавляют SUID, SGID?
7	Что такое лес и какие еще существуют структурные уровни в Active Directory? Для чего нужны эти уровни? Что такое сайты применительно к Active Directory и в каких случаях и как их создают? Для чего создают сайты?
8	Какие изменения в управлении доступом классического UNIX возможны с использованием SUDO? Решаются ли этой технологией проблемы подхода DAC и в какой степени?
9	Что такое SELinux, какие задачи решает и кем разработан и поддерживается? Опишите последовательность действий по включению и настройке его на CentOS. Какие помните распространенные утилиты SELinux, для чего используются?
10	Что такое репликация в Active Directory, разделы и контексты AD? В какой области (ях) выполняется репликация? Что такое схема, где хранится и как модифицируется?
11	Что такое домены, контексты, пользователи SELinux, помеченные и непомеченные пользователи и процессы? Как ограничения SELinux работают вместе с традиционным управлением доступом на основе GID/UID?
12	Что такое субъекты и объекты в контексте управления доступом. Как работает мандатная (MAC) политика управления доступом? В чем ее отличие от DAC (приведите примеры доступа к файлу в DAC и MAC? Почему MAC мало распространена в существующих ОС?
№	Вопросы контрольной работы 3
1	Как работает X-Window, что такое X-сервер и X-клиент? С помощью каких транспортных механизмов они могут взаимодействовать, когда X-сервер и X-клиент находятся на одном компьютере и когда на разных? В чем особенности графического решения X-Window, по сравнению с другими известными Вам графическими системам?
2	Каким образом администратор определяет как и в каком порядке останавливаются сервисы/демоны при завершении ОС UNIX и как определяется последовательность завершения различных сервисов/демонов?.
3	Почему сначала в серверных, затем в пользовательских компьютерах стали использовать EFI? Какие возможности по сравнению со стандартной схемой дает EFI, можно ли обойтись без EFI и в каких случаях? Какие есть проблемы у MBR-метода?
4	Что такое MBR? В каких случаях необходимо использовать вместо него GPT и какие возможности это дает?
5	Опишите последовательность загрузки ОС ПК (IBM-совместимом) с момента включения питания до загрузки ядра. Что такое “стандартный код” MBR, как он работает?
6	Как и для чего используют администраторы уровни загрузки (run levels), существующие в некоторых ОС UNIX? Перечислите утилиты UNIX для архивирования, перечислите утилиты для компрессии файлов.

7	Каким образом администратор определяет как и в каком порядке останавливаются сервисы/демоны при завершении ОС UNIX и как определяется последовательность завершения различных сервисов/демонов?
8	Для чего нужны программы-менеджеры пакетов ПО в ОС UNIX? Опишите их функции.
9	Какие уязвимости существуют у классической системы syslog? В чем смысл использования параметров facility, priority, как именно используются они при журналировании? Какие существуют варианты записи/передачи сообщений в syslog? Предположим необходимо собрать сообщения с 5 коммутаторов с помощью SYSLOG, какова последовательность действий администратора?
10	Где и в каком виде может находиться информация о пользователях, группах в ОС UNIX? Где обычно находится эта информация в случае отдельной рабочей станции? Каким образом можно управлять (создавать/удалять/модифицировать) пользователями в ОС UNIX? Приведите последовательности действий по созданию, удалению и блокированию (входа в систему) пользователя в ОС UNIX.
11	В чем отличие первичного (primary) и расширенного (extended) разделов диска? Какие существуют ограничения на кол-во разделов этих типов? Можно ли загрузить ОС, находящуюся на логическом диске расширенного раздел, в чем отличия/как осуществить загрузку (если возможно) в сравнении с расположением ОС на первичном разделе?
12	Опишите последовательность загрузки ОС UNIX с момента загрузки ядра до запуска пользователем первого приложения (рассмотрите два варианта загрузки: до 3 и до 5 уровней). В чем особенность SystemV загрузки?

Перечень лабораторных заданий

1	На выданном описании топологии сети представлена сеть организации, состоящая из N филиалов и центрального офиса. Необходимо сконфигурировать интранет сеть с использованием каналов поставщика услуг связи и доступ в Интернет через поставщика услуг Интернет, а также обеспечить доступ между филиалами (в т.ч. с требуемой схемой доступа) согласно описанию задания.
2	Выполнить развертывание службы каталога AD и применить к контроллерам домена шаблоны безопасности. Показать преподавателю результат применения шаблонов и права пользователей соответствующих групп.
3	Развертывание SELinux . Конфигурирование политик SELinux

20.2 Промежуточная аттестация

Перечень вопросов итоговой контрольной работы

1. Вариант:
    a. Можно ли использовать DNS не MS (например, DNS под ОС UNIX) для работы AD и

каким образом? Что такое SRV RR?

b. Опишите последовательность загрузки ОС ПК (IBM-совместимом) с момента включения питания до загрузки ядра. Что такое стандартный код MBR, как он работает (по шагам)?
c. В чем отличие NAT и PAT (NAT override)? В чем сложность реализации NAT для UDP пакетов по сравнению с TCP?
d. Что означают символы O, C, R в листинге таблицы маршрутизации IOS, как возникают такие (O, C и R) маршруты ?
e. Что такое репликация в Active Directory, разделы и контексты AD? В какой области (ях) выполняется репликация? Что такое схема, где хранится и как модифицируется?
f. В чем преимущества, и какие есть потенциальные проблемы у динамической маршрутизации? Что такое конвергенция протокола маршрутизации?

2. Вариант:
    a. Что такое лес и какие еще существуют структурные уровни в Active Directory? Для чего нужны эти уровни? Что такое сайты применительно к Active Directory и в каких случаях и как их создают? Для чего создают сайты (примеры)?
    b. Почему сначала в серверных, затем в пользовательских компьютерах стали использовать EFI? Какие возможности по сравнению со стандартной схемой дает EFI, можно ли обойтись без EFI и в каких случаях ?
    c. Что такое SELinux, какие задачи решает и кем разработан и поддерживается? Опишите последовательность действий по включению и настройке его на CentOS. Какие помните распространенные утилиты SELinux, для чего используется каждая?
    d. Какие варианты хранения записей (RR) поддерживает DNS компании MS? На что повлияет выбор места хранения?
    e. Что такое субъекты и объекты в контексте управления доступом. Как работает мандатная (MAC) политика управления доступом? В чем ее отличие от DAC (приведите примеры доступа к файлу в DAC и MAC? Почему MAC мало распространена в существующих ОС
    f. Какие способы используются (как они работает) для решения проблем образования циклов броадкаст-домена (домена широковещания)?

3. Вариант:
    a. Что такое GID, UID в классических UNIX ОС и как они используются для управления доступом? Какие возможности добавляют SUID, SGID?
    b. Где и в каком виде может находиться информация о пользователях, группах в ОС UNIX? Где обычно находится эта информация в случае отдельной рабочей станции? Каким образом можно управлять (создавать/удалять/модифицировать) пользователями в ОС UNIX? Приведите последовательности действий по созданию, удалению и блокированию (входа в систему) пользователя в ОС UNIX с использованием обычного редактора (например, vi).
    c. Где размещены параметры ОС и пользователя, ***после*** применения групповых политик? Какие существуют инструменты отладки механизма групповых политик? Консоль групповой политики недоступна, как исправить параметры GPO?
    d. Что такое DACL, SACL, ACE?
    e. Что такое «сертификационная программа», что входит в это понятие, кто разрабатывает. Что такое VUE и Prometric?

f. Что такое административное расстояние. Для каких протоколов оно имеет большие значения и почему?

4. Вариант:
    a. В чем проблемы дискреционной политики безопасности (управления доступом)? Почему несмотря на эти проблемы DAC широко используется (практически во всех ОС)? Можно ли решить эти проблемы в рамках DAC и как?
    b. Что такое GID, UID в классических UNIX ОС и как они используются для управления доступом? Какие возможности добавляют SUID, SGID?
    c. Компетенции и профессии, имеющие отношение к администрированию ИС. Многоуровневая поддержка.
    d. В чем отличие первичного (primary) и расширенного (extended) разделов диска? Какие существуют ограничения на кол-во разделов этих типов? Можно ли загрузить ОС, находящуюся на логическом диске расширенного раздел, в чем отличия/как осуществить загрузку (если возможно) в сравнении с расположением ОС на первичном разделе?
    e. Опишите последовательность загрузки ОС UNIX с момента загрузки ядра до запуска пользователем первого приложения (рассмотрите два варианта загрузки: до 3 и до 5 уровней). В чем особенность SystemV загрузки?
    f. Назовите и опишите методы борьбы с петлями маршрутизации. Почему они возникают и как их избежать (способы)?