МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.ДВ.03.01 Администрирование и безопасность компьютерных систем и сетей

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 7 от 26.05.2023г.
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024

8. Учебный год: 2026/2027 **Семестр(ы):** 8

9. Цели и задачи учебной дисциплины

В рамках дисциплины изучаются принципы и методы обеспечения безопасности и анализа современных сетевых технологий с построением виртуальных каналов и туннелей их научных основ. Современные технологии построения безопасных сетей с использованием межсетевых экранов, передача данных через интернет с использованием шифрования, обеспечение конфиденциальности передаваемых данных через открытый канал.

Формирование у студентов основ теоретических знаний и практических навыков по созданию (настройке) доменной среды для реализации бизнес-процессов в корпоративных сетях (интрасетях) предприятий с точки зрения системного администратора. Получение практических навыков сетевого администрирования информационной системы организации.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к вариативной части блока Б1 дисциплин учебного плана.

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

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	ПК-1.4	проводит оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам;	Знает: требования нормативных документов оценки соответствия механизмов безопасности компьютерной системы. Умеет: проводить оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам.
ПК-2	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.4	разрабатывает модели угроз безопасности информации и нарушителей	Знает: модели угроз безопасности информации и нарушителей. Умеет: разрабатывать модели угроз безопасности информации и нарушителей.
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных ,	ПК-3.2	знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов	Знает: методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов. Умеет: проводить анализ и формализацию

	исследовательских и прикладных задач	ПК-3.4	способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей	поставленных задач в области безопасности компьютерных систем и сетей.

12. Объем дисциплины в зачетных единицах/час - 3/108.
Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			8			
Аудиторные занятия	48		48			
в том числе: лекции	16		16			
Практические	0		0			
Лабораторные	32		32			
Самостоятельная работа	60		60			
Контроль	0		0			
Итого:	108		108			
Форма промежуточной аттестации	зачет с оценкой		зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Администрирование информационных систем.	Цели и задачи администрирования информационных систем. Требования к специалистам служб администрирования ИС. Стандарты работы ИС и стандартизирующие. Объекты администрирования и модели управления. Средства администрирования операционных систем. Администрирование сетевых систем.	Б1.В.ДВ.03.01 Администрирование и безопасность компьютерных систем и сетей (10.05.01)
1.2	Служба каталогов Active Directory ADDS.	Эволюция службы каталогов. Понятие ADDS. Служба ADDS. Структура службы ADDS. Объекты каталога и их наименования. Компоненты ADDS. Иерархия доменов. Доверительные отношения между доменами. Определение организационных единиц домена. Планирование и управление ADDS. Планирование пространства имен ADDS. Учетные записи пользователей. Группы пользователей и групповые политики. Безопасность ADDS. Протоколы Kerberos и IPSecurity.	
1.3	Производительные сети.	Администрирование процесса конфигурации. Администрирование процесса поиска и диагностики ошибок. Брандмауэры. Средства виртуализации. Удаленный доступ в информационных системах. Virtual Private Network (VPN). Администрирование с помощью протоколов TELNET и SSH. Методы мониторинга в локальных сетях.	
2. Лабораторные работы			

2.1	Настройка виртуальных машин в VirtualBox.	Цель работы: установить и настроить три виртуальные машины в программном продукте VirtualBox.	Б1.В.ДВ.03.01 Администрирование и безопасность компьютерных систем и сетей (10.05.01)
2.2	Настройка DNS и DHCP серверов в ОС Windows.	Цель работы: настроить DNS-сервер и DHCP-сервер.	
2.3	Ввод клиентов в домен ADDS.	Цель работы: научиться добавлять новых пользователей в домен AD	
2.4	Настройка DNS и DHCP в ОС Linux.	Цель работы: научиться работать со службами DNS и DHCP в Ubuntu	
2.5	Настройка Zabbix.	Цель работы: научиться настраивать систему мониторинга Zabbix в Ubuntu	
2.6	Общие ресурсы на сервере Linux.	Цель работы: научиться открывать общий доступ до папки на Ubuntu-сервере.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Администрирование информационных систем.	4		4	20	0	28
1.2	Служба каталогов Active Directory ADDS.	4		12	20	0	36
1.3	Производительные сети.	8		16	20	0	44
	Итого:	16		32	60	0	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. – Санкт-Петербург : , 2020 – Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях – 2020. – 357 с. – ISBN 978-5-6044429-8-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/329378. – Режим доступа: для авториз. пользователей.
2	Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова ; под редакцией О. И. Шелухина. – Москва : Горячая линия-Телеком, 2018. – 220 с. – ISBN 978-5-9912-0323-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111119. – Режим доступа: для авториз. пользователей.
3	Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. – Москва : МИСИС, 2018. – 31 с. – ISBN 978-5-906953-53-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/116743. – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
4	Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М. А. Иванов, И. В. Чугунков. – Москва : НИЯУ МИФИ, 2012. – 400 с. – ISBN 978-5-7262-1676-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/75810. – Режим доступа: для авториз. пользователей.
5	Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд. – Москва : ИНТУИТ, 2016. – 368 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100522. – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

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

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.ДВ.03.01 Администрирование и безопасность компьютерных систем и сетей (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Администрирование информационных систем.	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.4	
2	Служба каталогов Active Directory ADDS.	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
3	Производительные сети.	ПК-2	ПК-2.4	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.2	
			ПК-3.4	
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- лабораторные работы.

Перечень лабораторных работ

1	Настройка виртуальных машин в VirtualBox.	Цель работы: установить и настроить три виртуальные машины в программном продукте VirtualBox. Задачи: 1. Установить Windows Server 2016. 2. Установить Windows 10. 3. Установить Ubuntu 16.04 LTS. 4. Настроить между ними сеть со статическими IP-адресами. 5. Настроить на всех машинах выход в интернет Windows Server 2016. 6. Провести первичную настройку серверных компонентов на Windows Server 2016. 7. Сделать экспорт конфигурации виртуальных машин.
2	Настройка DNS и DHCP серверов в ОС Windows.	Цель работы: настроить DNS-сервер и DHCP-сервер. Задачи: 1. Настроить в Windows Server 2016 домен. 2. Настроить DNS-сервер. 3. Настроить DHCP-сервер.
3	Ввод клиентов в домен ADDS.	Цель работы: научиться добавлять новых пользователей в домен AD Задача: ввести две рабочие станции (Windows и Ubuntu) в домен.
	Настройка DNS и DHCP в ОС Linux.	Цель работы: научиться работать со службами DNS и DHCP в Ubuntu Задачи: 1. Создать три виртуальные машины: Ubuntu-сервер, Ubuntu-клиент и Windows-клиент. 2. Настроить на Ubuntu-сервере службу DHCP. 3. Настроить на Ubuntu-сервере службу DNS, где именем для сервера будет ваша фамилия, для клиентов можно те, что были в предыдущих лабораторных. 4. Настроить прокси-сервер.
	Настройка Zabbix.	Цель работы: научиться настраивать систему мониторинга Zabbix в Ubuntu Задачи: 1. Настроить на Ubuntu-сервере веб-сервер, MySQL и PHP для дальнейшей настройки Zabbix. 2. Настроить на Ubuntu-сервере систему мониторинга Zabbix. 3. Настроить на Ubuntu-клиенте и на Windows-клиенте Zabbix-агентов.
	Общие ресурсы на сервере Linux.	Цель работы: научиться открывать общий доступ до папки на Ubuntu-сервере. Задачи: 1. Добавить все три рабочие станции в одну рабочую группу с названием своей фамилии. 2. Настроить Samba на допуск к папке под логином и паролем для обоих клиентов.

Технология проведения

Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все

задания, и они правильные, даны пояснения);
оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к зачету с оценкой (КИМ №1)

1. Функции администрирования информационных систем.
2. Процедуры администрирования. Объекты администрирования.
3. Программная структура.
4. Методы администрирования информационных систем Основные понятия и определения.
5. Пользовательские учетные записи.
6. Стандартные группы.
7. Служба каталогов.
8. Управление учетными записями пользователей и групп.
9. Групповые политики.
10. Профили пользователей: структура, управление.
11. Функциональные возможности пользовательской MMC.
12. Модели сетей.
13. Создание совместно используемых папок.
13. Управление доступом.
14. Разрешения общих папок и разрешения NTFS.
15. Распределенная файловая система DFS.
16. Контроль доступа к файлам и папкам.
17. Аудит обращений и использования ресурсов.
18. Создание и назначение служебного профиля пользователя.
19. Средства управления общего пользования и их возможности.
20. Управление объектами службы каталогов.
21. Поиск объектов в каталогах.
22. Репликация каталогов.
23. Управление службами и приложениями в сетях под управлением ОС Windows.
24. Управление дисками в сетях под управлением ОС Windows.
25. Репликация данных.
26. Администрирование ИС для доступа из Интернет.
27. Многотерминальные системы.
28. Распределённая обработка данных в ИС.
29. Планирование операций печати.
30. Подключение физических принтеров (устройств печати).
31. Создание принтеров на сервере.
32. Настройка параметров (свойств) принтера.
33. Настройка параметров (свойств) сервера печати.
34. Командные файлы и сценарии регистрации.
35. Управление личным каталогом.
36. Административные сетевые команды.
37. Средства контроля и оптимизации сети.
38. Оснастка «Производительность».
39. Сетевой монитор.
40. Системный монитор.
41. Диспетчер задач.
42. Мониторинг сети с помощью просмотра событий.
43. Обновление аппаратных и программных средств.
44. Обеспечение безопасности системы.

45. Обеспечение бесперебойной подачи питания.
46. Выполнение резервного копирования.
47. Инсталляция информационной системы.
48. Эксплуатация и сопровождение информационной системы.
49. Оперативное управление и регламентные работы.
50. Управление и обслуживание технических средств.
51. Аппаратно-программные платформы администрирования.
52. Информационные системы администрирования.
53. Организация баз данных администрирования.
54. Работа с параметрами командной строки сценария.
55. Подключение внешних файлов.
56. Шифрование сценариев.
57. Цифровая подпись для сценариев WSH.
58. Политика безопасности для сценариев WSH.
59. Выполнение основных операций с файловой системой.
60. Отчет об использовании дискового пространства.
61. Удаление временных файлов с жесткого диска.

Критерии оценки ответов на вопросы зачете с оценкой

Для оценивания результатов обучения на зачете с оценкой используется - 4-балльная шала:
«отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации;

1) закрытые задания (тестовые, средний уровень сложности):

1. Укажите ip-адрес, используемый для проверки работоспособности стека TCP/IP на локальном компьютере, с помощью утилиты ping.
a. 127.0.0.1
b. 192.168.0.1
c. 255.255.255.255
d. 0.0.0.0
Ответ - a 2.
Для какого метода рассылки пакетов в локальных сетях используется ip-адрес назначения 255.255.255.255?
a. Одноадресатная рассылка
b. Групповая рассылка
c. Широковещательная рассылка
d. Рассылка ближайшему из группы получателей
Ответ - c
3. Какое утверждение точно описывает технологию статического NAT?
a. Для статического преобразования NAT необходимо число публичных адресов, равное количеству компьютеров в локальной сети.
b. Для преобразования необходим только один публичный адрес.
c. Для работы статического преобразования необходимо знать порт назначения для передаваемых данных.
d. Преобразование не может использоваться для доступа пользователей в Интернет.
Ответ - a
4. В чем заключается основная уязвимость протокола DHCP при работе в локальной сети?
a. С отсутствием шифрования передаваемых сообщений.
b. С избыточной конфигурацией передаваемой между устройствами и приводящей к перегрузке компьютеров.
c. С широковещательной рассылкой сообщений и возможностью установки нелегальных DHCP-серверов.
d. С отсутствием балансировки нагрузки между DHCP-серверами, приводящей к выводу их из строя.
Ответ - c
5. Укажите тип сообщения протокола DHCPv4 , которое использует ПК для поиска DHCP-серверов в локальной сети.
a. DHCPACK
b. DHCPDISCOVER
c. DHCPOFFER
d. DHCPREQUEST
Ответ - b
6.Укажите протокол и порт, используемый сервером ДНС для передачи сообщений системы доменных имен.
a. Протокол tcp и порт 22
b. Протокол udp и порт 53
c. Протокол udp и порт 5060
d. Протокол tcp и порт 80
Ответ - b
7. Какое утверждение не соответствует характеристикам протокола SNMP?
a. Протокол использует базу управляющей информации для хранения ссылок на данные.
b. Для передачи сообщений используется протокол UDP.
c. Сообщество public по умолчанию используется для записи данных на устройство.
d. Ловушка (trap) является асинхронным уведомлением о произошедших событиях на устройстве.
Ответ - c
8. Какой из перечисленных сетевых параметров не передается в сообщении RA компьютеру при автоматической настройке сетевой конфигурации методом SLAAC?
a. Префикс
b. Длина префикса
c. Шлюз
d. Адрес ДНС сервера
Ответ - d
9. Какой из перечисленных терминов не является частью модели информационной безопасности AAA?
a. Аутентификация

b. Администрирование
c. Авторизация
d. Аккаунтинг
Ответ - b
10. Выберите утверждение, верно описывающее атаку IP spoofing.
a. Способ подбора паролей на устройстве пользователя.
b. Множественная широковещательная рассылка пакетов на атакуемое устройство.
c. Метод перегрузки маршрутизатора посылкой фрагментированных пакетов.
d. Подбор сетевого адреса злоумышленником для обхода фильтрующих списков.
Ответ - d
11. Какой из перечисленных алгоритмов является алгоритмом множественного доступа с контролем несущей и обнаружения коллизий.
a. CSMA/CD.
b. Алгоритм трехстороннего рукопожатия.
c. Алгоритм CRC64.
d. CSMA/CA.
Ответ - a
12. Какое сетевое устройство ограничивает широковещательный трафик.
a. Повторитель (хаб).
b. L2 коммутатор.
c. Маршрутизатор.
d. Точка доступа.
Ответ - c.
13. В каких из перечисленных приложений желательно использование протокола UDP.
a. Веб-серфинг с помощью браузера.
b. Потоковая передача видео.
c. Обмен данными между базами данных.
d. Обмен почтой.
Ответ - b
14. Каково предназначение поля TTL в служебном заголовке ip-пакета.
a. Обеспечивает механизм проверки целостности данных.
b. Зарезервировано для будущего использования.
c. Определяет адрес назначения пакета.
d. Определяет число маршрутизаторов, через которые может пройти пакет.
Ответ - d

ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

1. Поясните, как с помощью анализатора трафика определить основные данные сетевых устройств, участвующих в обмене данными – ARP, IP-адреса, применяемые протоколы на 2-4 уровнях.
2. Поясните, как выполняется процесс обработка IP-пакета на транзитном маршрутизаторе.
3. Поясните, как применяются правила маршрутизации IP-пакета, указанные в таблице маршрутизации транзитного маршрутизатора
4. Объясните процесс обмена сообщениями протокола ARP в ходе установления соответствия IP и MAC-адреса стороны получателя на стороне отправителя.
5. Поясните процесс коммутирования Ethernet-кадров в коммутаторе Ethernet с использованием таблицы коммутации.
6. Поясните процесс заполнения таблицы коммутации в ходе коммутирования Ethernet-кадров в коммутаторе Ethernet.
7. С использованием подхода VLSM (Variable Length Subnet Mask) укажите оптимальную сетевую маску для IPv4 адресации подсети, включающей 27 рабочих станций и 1 шлюз.
8. С использованием подхода VLSM (Variable Length Subnet Mask) укажите оптимальную сетевую маску для IPv4 адресации подсети, включающей 7 рабочих станций и 1 шлюз.
9. С использованием подхода VLSM (Variable Length Subnet Mask) укажите оптимальную сетевую маску для IPv4 адресации подсети, включающей 45 рабочих станций и 1 шлюз.
10. Для трех офисных зданий, в которых располагаются коммерческий, технический и юридический отделы одного предприятия, предложите вариант организации локальной сети с использованием трех коммутаторов и технологии VLAN 802.1Q. Поясните принцип работы.
11. Для трех офисных зданий, в которых располагаются коммерческий, технический и юридический отделы одного предприятия, предложите вариант организации локальной сети с резервированием с

использованием трех коммутаторов и технологии/протокола RSTP. Поясните принцип работы.
12. Для схемы из 5 Ethernet-коммутаторов, соединенных друг с другом в кольцо (кольцевая топология) поясните принцип работы технологии/протокола RSTP с момента включения всех устройств.
13. Объясните принцип работы «скользящего» окна в рамках обмена по протоколу TCP.

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

1. Объясните процедуру установления TCP-сессии между двумя участниками.
2. Поясните процесс коммутации Ethernet-кадров с использованием технологии VLAN 802.1Q.
3. Поясните принцип работы протокола динамической маршрутизации RIP в схеме из 4 последовательно соединенных маршрутизаторов.
4. Объясните механизм выбора оптимального пути с использованием алгоритма Дейкстры в рамках работы протокола OSPF в схеме из 4 маршрутизаторов, соединенных непосредственно друг с другом и имеющих по одному независимому интерфейсу, включенному в изолированные сегменты сетей.
5. Укажите практические примеры применения мультиплексирования с частотным разделением сигналов. Поясните принцип работы.
6. Укажите практические примеры применения спектрального мультиплексирования сигналов. Поясните принцип работы.
7. Укажите практические примеры применения мультплексирования сигналов с разделением по времени. Поясните принцип работы.
8. Поясните принцип организации и работы потока E1 (передача с мультиплексирование по времени).

2) открытые задания (тестовые, средний уровень сложности):

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации

1. Для чего используется технология DHCP Snooping.
Технология DHCP Snooping используется для блокировки ответов нелегального DHCP сервера, работающего в локальной сети.
2. Как работает технология DHCP Snooping.
Работа DHCP Snooping происходит на коммутаторах сети. В данном случае коммутатор анализирует DHCP сообщения, передаваемые через его собственные порты, и реализует фильтрацию на основе нескольких правил.
3. Дайте определение модели AAA.
Модель AAA - представляет архитектуру, в которой используется единая политика доступа в сеть, доступа к сетевым устройствам.
4. Каково значение каждой из букв в сокращении AAA.
Три основных компонента в модели: 1. Аутентификация 2. Авторизация 3. Аккаутинг
5. Какие протоколы реализуют модель AAA.
Используются протоколы Radius, Tacacs+ . Оба имеют клиент-серверную архитектуру. Требуют наличие ip-связности между устройствами.
6. Каковы задачи технологии трансляции сетевых адресов.
Технология трансляции сетевых адресов (NAT) позволяет осуществлять преобразования ip адреса устройства, находящегося в локальной сети, в ip адрес граничного устройства, через которое осуществляется выход данных в сеть Интернет. Зачастую роль граничного устройства выполняет маршрутизатор со специальным программным обеспечением, выполняющим функции NAT.
7. Для чего используется динамический нат.
Динамический NAT использует подход, в котором группа частных адресов транслируется в один свободный адрес из группы публичных ip адресов, настроенных на маршрутизаторе. Для выполнения трансляции на маршрутизаторе должен быть создан пул публичных адресов. Дополнительно при помощи списков доступа обычно задается подсеть частных адресов, которые будут транслироваться в публичные адреса.
8. Что такое сервис мониторинга сети.
Под сервисом мониторинга сети понимается набор служб, обеспечивающих контроль оборудования в локальной сети. Обычно в виде службы мониторинга выступает отдельный сервер, на котором развернуто специальное программное обеспечение. Основной задачей программных служб является контроль сетевого и инфраструктурного оборудования посредством специальных протоколов.
9. Приведите пример программных продуктов, реализующих сервис мониторинга сети.
Это программные сервисы cacti, zabbix, nagios
10. Для чего необходим ДНС сервер в локальной сети.

Самым распространенным примером применения ДНС сервера является то, когда ДНС сервер используется для разрешения адреса, заданного в символьной форме в ip адрес узла.

ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

1. Для чего необходим DHCP сервер в локальной сети.
DHCP сервер принимает запросы на получение сетевой конфигурации от клиентских компьютеров. После обработки запроса DHCP сервер выдает персональному компьютеру нужные сетевые реквизиты.
2. Является ли безопасным использование утилиты telnet
Нет, так как данные передаются по сети в открытом виде и могут быть просмотрены сторонним лицом.
3. Для чего используется технология VLAN.
Технология виртуальных локальных сетей позволяет разделять устройства сети на различные группы. С точки зрения продвижения трафика рабочие станции, находящиеся в одном влан, ведут себя так, как будто подключены к одной линии связи. Компьютеры пользователей могут находиться в разных точках организации, распределены географически, но при этом им будут доступны все ресурсы, предоставляемые конкретной группе.
4. Перечислите преимуществам использования технологии влан.
1. Обеспечение безопасности в сети. Группы компьютеров, объединенные в один влан, создают собственную виртуальную сеть, ограничивая передачу данных между остальными компьютерами других сетей. 2. Уменьшение стоимости сети. При расширении сети и добавлении устройств вносятся меньшие затраты на установку дополнительного оборудования и прокладку кабельной системы. 3. Увеличение производительности сети. Связано с объединением рабочих станций в широковещательную группу, и уменьшением передачи широковещательного трафика. 4. Облегчение в управлении сетью.

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

1. Для чего необходима настройка транкового порта коммутатора.
Для передачи маркированного трафика между коммутаторами, необходимо дополнительно сконфигурировать соединяющие порты. Порт коммутатора, который соединен с другим коммутатором и служит для передачи информации об влан, называется транковым портом. Для работы сети, содержащей несколько коммутаторов, необходимо перевести в режим транка порт на каждом коммутаторе. В противном случае возникнут ошибки при передаче данных, и связность между устройствами будет нарушена.
2. Дайте определение голосового влана.
В некоторых сетевых устройствах дополнительно вводится голосовой влан. Кадры трафика, помеченного данным вланом, используются для передачи голосовых данных IP телефонии. Поэтому некоторые производители оборудования создают на своих устройствах голосовые вланы. Из особенностей голосового влана обычно следует то, что данные в нем обладают определенным приоритетом при передаче между коммутаторами. Благодаря этому становится возможным поддерживать определенный уровень качества обслуживания данного трафика. Стандартов в выборе числового значения голосового влана у различных производителей не принято, поэтому в качестве голосового влана обычно выступает определенный влан данных с приоритетом по передаче данных.
3. Перечислите группы частных адресов.
Частные адреса принимают диапазон значений от 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255. Особенностью данных сетей является то, что они не маршрутизируются в глобальной сети и поэтому могут быть неуникальными для различных предприятий и учреждений. Для выделения и использования частных сетей не нужно делать запросов к служебным организациям Интернет. Поэтому фактически любая организация может их использовать для своей внутренней сети. При использовании частных ip адресов доступ в глобальную сеть не возможен.
4. Дайте определение полностью определенному имени в ДНС.
Полностью определенным доменным именем (FQDN) называют однозначно идентифицирующее ресурс доменное имя, включающее в себя имена всех родительских доменов, включая корневой. Имя ресурса aa.portal.asu.ru. является полностью определенным доменным именем.
19. Что необходимо для работы системы доменных имен.
Процесс работы системы доменных имен сводится к взаимодействию между клиентом и сервером.

На сервере, который отвечает за определенную зону, работает специальная служба DNS. На транспортном уровне за данной службой закреплен отдельный порт 53. При обмене сообщениями между клиентом и сервером используется протокол UDP. На DNS-сервере в виде отдельных текстовых файлов находится описание соответствующей зоны со списком доменных имен и соответствующих им значений адресов хостов, например, aaa.asu.ru = 192.168.10.5.
5. Какие существуют типы получаемых клиентом ответов от сервиса ДНС в локальной сети.
В зависимости от сервера, который ответил на запрос, ответы бывают следующих двух видов. Авторитативный ответ является ответом DNS-сервера, ответственного за конкретную зону. Неавторитативный ответ - это ответ на запрос от одного из кеширующих серверов.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).