Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ	**УТВЕРЖДАЮ**
Декан, председатель совета факультета КТ,ВТиЭ	**Проректор по учебной работе, председатель методического совета ДГТУ**
_____ Ш.А.Юсуфов	_____ Н.С.Суракатов
подпись ФИО	подпись ФИО
16 10 2018г.	18 10 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.36 Аудит информационных технологий и систем обеспечения ИБ

для специальности 10.05.03-«Информационная безопасность автоматизированных систем»

специализация «Безопасность открытых информационных систем»

факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, с которым связается дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) Специалист по защите информации
бакалавр (специалист)

Форма обучения очная : курс 5 семестр 9 :

Всего трудоемкость в зачетных единицах (часах) 3 ЗЕТ (108 часов)

Лекции 34 (час): зачет 9 семестр

практические (семинарские) занятия - (час): экзамен - (семестр)

лабораторные занятия 17 (час): самостоятельная работа 57 (час):

курсовой проект (работа, РГР)-(семестр).

Зав. кафедрой ИБ _____ **Г.И. Качаева**
подпись

Начальник УО _____ **Э.В. Магомаева**
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ от 15.10.2018г., протокол № 2

Зав. выпускающей кафедрой по данной специальности _____ **Г.И. Качаева**

ОДОБРЕНО
Методической комиссией по укрупненным группам специальностей и направлению подготовки
10.00.00- «Информационная безопасность»
Председатель МК
_____ Мелехин В.Б.
подпись ФИО

«15» 10 2018г.

АВТОР ПРОГРАММЫ

Качаева Г.И., к.э.н., ст. преп. каф. ИБ
ПОЛНОСТЬЮ: ученая степень, ученое звание, должность

_____

1. Цели и задачи дисциплины

1.1 Цели дисциплины

Целью освоения дисциплины является формирование у студентов знаний и умений в области теории и практики информационной безопасности и защиты информации в компьютерных системах.

1.2 Задачи дисциплины

- ознакомление с общими сведениями о TCP/IP;
- изучение преимуществ и возможностей протокола DHCP;
- изучение основных параметров конфигурирования DNS серверов и зон
- изучение основных параметров настройки маршрутизации.
- формирование умения определять рациональные меры защиты АС и оценивать уровень эффективности их защиты;

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Аудит информационных технологий и систем обеспечения ИБ» относится к дисциплинам базовой части учебного плана.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Операционные системы, Организация ЭВМ и вычислительных систем, Безопасность операционных систем, Безопасность сетей ЭВМ, Информационная безопасность открытых систем, Разработка и эксплуатация защищенных АС, Комплексное обеспечение ИБ автоматизированных систем.

Последующими дисциплинами являются: Преддипломная практика, Защита ВКР.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

В результате изучения дисциплины студент должен

Знать:

- о политиках безопасности и мерах защиты в открытых информационных системах;
- о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;

Уметь:

- осуществлять мониторинг и аудит сетевой безопасности;
- осуществлять администрирование открытых информационных систем
- осуществлять управление информационной безопасностью открытых информационных системах;

Владеть:

- навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем виртуальных систем

4. Структура и содержание дисциплины «Аудит информационных технологий и систем обеспечения ИБ»

Общая трудоемкость дисциплины составляет 4 зачетные единицы – 108 часов, в том числе: лекционных -34 часа, лабораторных - 17 часов, СРС – 57 часов, форма отчетности зачет в 9 семестре.

4.1.Содержание дисциплины

	Раздел дисциплины Тема лекции и вопросы	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости *(по срокам текущих аттестаций в семестре)*
				ЛК	ПЗ	ЛР	СР	
1.	**Лекция № 1 Тема:** «Введение в администрирование в ИС».		1	2		1	2	Вх. Контр.
2.	**Лекция № 2 Тема:** «Функции и процедуры администрирования».		2	2		1	2	
3.	**Лекция № 3 Тема:** «Службы администрирования».		3	2		1	2	
4.	**Лекция № 4 Тема:** «Эксплуатация и сопровождение информационных систем».		4	2		1	2	
5.	**Лекция № 5 Тема:** «Инсталляция информационных систем».		5	2		1	2	АКР №1
6.	**Лекция № 6 Тема:** «Оперативное управление и регламентные работы».		6	2		1	3	
7.	**Лекция № 7 Тема:** «Управление и обслуживание технических средств».		7	2		1	4	
8.	**Лекция № 8 Тема:** «Аппаратно-программные платформы администрирования операционных систем».		8	2		1	4	
9.	**Лекция № 9 Тема:** «Аппаратно-программные платформы администрирования баз данных».		9	2		1	4	
10.	**Лекция № 10 Тема:** «Аппаратно-программные платформы администрирования службы каталогов».		10	2		1	4	АКР №2
11.	**Лекция №11 Тема: «Уровни и модели TCP/IP»** IP-адресация. Разбиение IP-сетей на подсети и создание подсетей. Установка и конфигурирование TCP/IP на примере Windows Server 2008.	9	11	2		1	4	
12.	**Лекция № 12 Тема: «Организация сетевого графика»** Анализ сетевого трафика средствами «Сетевого монитора». Устранение неполадок подключений TCP/IP.		12	2		1	4	
13.	**Лекция № 13 Тема: «Сравнение DNS и NetBIOS»** Сравнение DNS и NetBIOS. DNS в сетях Windows Server 2008. Развертывание DNSсерверов. Настройка DNS-клиентов. Настройка параметров DNS-сервера. Настройка свойств зоны и передачи. Настройка дополнительных свойств DNS-сервера.		13	2		1	4	
14.	**Лекция № 14 Тема: «Основы теории защиты информации в компьютерных**		14	2		1	4	

	системах. Критерии информационной безопасности» Основные понятия теории защиты информации: угрозы безопасности: математические модели политики безопасности: общие критерии безопасности информационных технологий						
15.	**Лекция № 15 Тема: «Ошибки DNS»** Средства устранения неполадок DNS. Средства мониторинга DNS.	15	2		1	4	АКР №3
16.	**Лекция № 16 Тема: «Мероприятия по выявлению каналов утечки информации»** Специальные проверки. Порядок проведения специальной проверки технических средств	16	2		1	4	
17.	**Лекции № 17 Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»** Аутентификация данных: алгоритмы безопасного хеширования: ЭЦП криптосистем RSA и Эль Гамаля: алгоритм цифровой подписи DSA: отечественные алгоритмы цифрой подписи	17	2		1	4	
	Итого по дисциплине		**34**		**17**	**57**	**зачет**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторных занятий	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	Тема: Введение в администрирование в ИС.	№№ 1-8	2
2	Лк №2	Тема: Функции и процедуры администрирования.	№№ 1-8	2
3	Лк №3	Тема: Службы администрирования.	№№ 1-8	2
4	Лк № 4	Тема: Эксплуатация и сопровождение информационных систем.	№№ 1-8	2
5	Лк № 5	Тема: Инсталляция информационных систем.	№№ 1-8	2
6	Лк №6	Тема: Оперативное управление и регламентные работы.	№№ 1-8	2
7	Лк № 7	Тема: Управление и обслуживание технических средств.	№№ 1-8	2
8	Лк №8	Тема: Аппаратно-программные платформы администрирования операционных систем.	№№ 1-8	2
9	Лк №9	Тема: Аппаратно-программные платформы администрирования баз данных.	№№ 1-8	2
10	Лк №10	Тема: Аппаратно-программные платформы администрирования службы каталогов.	№№ 1-8	
11	Лк №11	Тема: «Уровни и модели TCP/IP»	№№ 1-8	2
12	Лк №12	Тема: «Организация сетевого трафика»	№№ 1-8	2
13	Лк №13	Тема: «Сравнение DNS и NetBIOS»	№№ 1-8	2
14	Лк №14	Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»	№№ 1-8	2

15	Лк №15	Тема: «Ошибки DNS»	№№ 1-8	2
16	Лк №16	Тема: «Мероприятия по выявлению каналов утечки информации»	№№ 1-8	2
17	Лк №17	Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»	№№ 1-8	2
Итого по дисциплине				**34**

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1.	Тема: Введение в администрирование в ИС.	2	№№ 1-8	Опрос, реферат, статья
2.	Тема: Функции и процедуры администрирования.	2	№№ 1-8	Опрос, реферат, статья
3.	Тема: Службы администрирования.	2	№№ 1-8	Опрос, реферат, статья
4.	Тема: Эксплуатация и сопровождение информационных систем.	2	№№ 1-8	Опрос, реферат, статья
5.	Тема: Инсталляция информационных систем.	2	№№ 1-8	Опрос, реферат, статья
6.	Тема: Оперативное управление и регламентные работы.	3	№№ 1-8	Опрос, реферат, статья
7.	Тема: Управление и обслуживание технических средств.	4	№№ 1-8	Опрос, реферат, статья
8.	Тема: Аппаратно-программные платформы администрирования операционных систем.	4	№№ 1-8	Опрос, реферат, статья
9.	Тема: Аппаратно-программные платформы администрирования баз данных.	4	№№ 1-8	Опрос, реферат, статья
10.	Тема: Аппаратно-программные платформы администрирования службы каталогов.	4	№№ 1-8	Опрос, реферат, статья
11.	Тема: «Уровни и модели TCP/IP»	4	№№ 1-8	Опрос, реферат, статья
12.	Тема: «Организация сетевого трафика»	4	№№ 1-8	Опрос, реферат, статья
13.	Тема: «Сравнение DNS и NetBIOS»	4	№№ 1-8	Опрос, реферат, статья
14.	Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»	4	№№ 1-8	Опрос, реферат, статья
15.	Тема: «Ошибки DNS»	4	№№ 1-8	Опрос, реферат, статья
16.	Тема: «Мероприятия по выявлению каналов утечки информации»	4	№№ 1-8	Опрос, реферат, статья
17.	Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»	4	№№ 1-8	Опрос, реферат, статья
Итого		**57**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Основные принципы обеспечения информационной безопасности в информационных системах
4. Основные направления и методы реализации угроз информационной безопасности.
5. Основные понятия программно-технического уровня информационной безопасности.
6. Методы обеспечения информационной безопасности.
7. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
8. Понятие защищенной ОС.
9. Локальные сети
10. Глобальные сети
11. Цифровые сети с интеграцией услуг (ISDN – ЦСИС)
12. Особенности защищенных телекоммуникационных сетей
13. Маршрутизация и управление в телекоммуникационных сетях
14. Стратегии межсетевого взаимодействия.
15. Теоретические основы автоматизации управления.
16. Методы проектирования автоматизированных систем. .

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа №1

1. Введение в администрирование в ИС.
2. Функции и процедуры администрирования.
3. Службы администрирования.
4. Эксплуатация и сопровождение информационных систем.
5. Инсталляция информационных систем.

Аттестационная контрольная работа №2

1. Оперативное управление и регламентные работы.
2. Управление и обслуживание технических средств.
3. Аппаратно-программные платформы администрирования операционных систем.
4. Аппаратно-программные платформы администрирования баз данных.
5. Аппаратно-программные платформы администрирования службы каталогов.

Аттестационная контрольная работа №3

1. IP-адресация.
2. Разбиение IP-сетей на подсети и создание надсетей.
3. Установка и конфигурирование TCP/IP на примере Windows Server 2008.
4. Анализ сетевого трафика средствами «Сетевого монитора».
5. Устранение неполадок подключений TCP/IP.
6. Сравнение DNS и NetBIOS.
7. DNS в сетях Windows Server 2008.
8. Развертывание DNSсерверов.
9. Настройка DNS-клиентов.
10. Настройка параметров DNS-сервера.
11. Настройка свойств зоны и передачи.
12. Настройка дополнительных свойств DNS-сервера.
13. Основные понятия теории защиты информации: угрозы безопасности; математические модели политики безопасности: общие критерии безопасности информационных технологий
14. Средства устранения неполадок DNS.
15. Средства мониторинга DNS.

Перечень вопросов на зачет

1. Разбиение IP-сетей на подсети и создание надсетей.
2. Установка и конфигурирование TCP/IP на примере Windows Server 2008.
3. Анализ сетевого трафика средствами «Сетевого монитора».
4. Устранение неполадок подключений TCP IP.
5. Сравнение DNS и NetBIOS.
6. DNS в сетях Windows Server 2008.
7. Развертывание DNSсерверов.
8. Настройка DNS-клиентов.
9. Настройка параметров DNS-сервера.
10. Настройка свойств зоны и передачи.
11. Настройка дополнительных свойств DNS-сервера.
12. Основные понятия теории защиты информации: угрозы безопасности: математические модели политики безопасности: общие критерии безопасности информационных технологий
13. Средства устранения неполадок DNS.
14. Средства мониторинга DNS.
15. Специальные проверки.
16. Порядок проведения специальной проверки технических средств
17. Аутентификация данных: алгоритмы безопасного хеширования:
18. ЭЦП криптосистем RSA и Эль Гамаля: алгоритм цифровой подписи DSA: отечественные алгоритмы цифрой подписи
19. Анализ DHCP-трафика.
20. Мониторинг DHCP с применением журнала аудита.
21. Устранение неполадок DHCP.
22. Настройка Windows Server 2008 для маршрутизации в локальной сети.
23. Настройка маршрутизации вызовов по требованию.

Вопросы проверки остаточных знаний

1. Введение в администрирование в ИС.
2. Функции и процедуры администрирования.
3. Службы администрирования.
4. Эксплуатация и сопровождение информационных систем.
5. Инсталляция информационных систем.
6. Оперативное управление и регламентные работы.
7. Управление и обслуживание технических средств.
8. Аппаратно-программные платформы администрирования операционных систем.
9. Аппаратно-программные платформы администрирования баз данных.
10. Аппаратно-программные платформы администрирования службы каталогов.
11. Уровни и модели TCP/IP
12. Организация сетевого трафика
13. Сравнение DNS и NetBIOS
14. Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности
15. Ошибки DNS
16. Мероприятия по выявлению каналов утечки информации
17. Методы идентификации и аутентификации пользователей компьютерных систем

7. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Аудит информационных технологий и систем обеспечения ИБ»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой

№	Виды занятий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
		ОСНОВНАЯ			в библ	на каф
1.	Лк, лб, срс	Организация работы администратора БАС	Михайлов М.К.	Московский технический университет связи и информатики. 2015. — 95 с	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Информационная безопасность и защита информации	Шаньгин В. Ф.	Электрон. текстовые дан. – Москва: ДМК Пресс, 2014. – 702 с	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Управление АС	Соловьев И.П.	СПГУ, 2013. – 280 с	http://www.iprbookshop.ru/24451	
		ДОПОЛНИТЕЛЬНАЯ				
4.	Лк, лб, срс	Защита информации предприятия [Электронный ресурс	Куликов М.Ю.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 590 с. 5-9556-0067-1.	http://www.iprbookshop.ru/73733.html	
5.	Лк, лб, срс	Методические указания к практическим занятиям и самостоятельной работы по дисциплине «Организация работы администратора БАС».	А.С. Алексеев	Самара: ФГБОУ ВПО «СамГТУ» ,2014	http://www.iprbookshop.ru/226151	
6.	ЛК,СР, КР	http://dstu.ru/nauka/biblioteka образовательный портал университета				
7.	ЛК,СР, КР	http://www.elibrary.ru научная электронная библиотека				
8.	ЛК,СР, КР	http://www.edu.ru веб-сайт системы федеральных образовательных порталов.				

7.2. Программное обеспечение

Интегрированные среды разработки программ Borland Developer Studio и Visual Studio .NET, базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы.

8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий и лабораторного практикума на основе интерактивных методов обучения необходим доступ в Интернет из компьютерного зала, наличие цифрового проектора для применения современных обучающих мультимедиа – технологий.

Программное обеспечение:

- операционная система Microsoft Windows;
- текстовый процессор Microsoft Word;
- web-браузер;
- среда программирования.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03-«Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры (работодателя) по специальности 10.05.03-«Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

_____ _____

подпись ФИО

Дополнения и изменения в рабочей программе
на 20__/____ учебный год

В рабочую программу вносятся следующие изменения

Рабочая программа пересмотрена и одобрена на заседании кафедры ____20

Заведующий кафедрой

Внесенные изменения утверждаю
Проректор по учебной работе

(печать)