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

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ **Ш. А. Юсуфов**
«18» 10 **20 18 г.**

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ **Н. С. Суракатов**
«24» 10 **20 18 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В.ДВ.9 Организация работы администратора безопасности автоматизированных систем

Направление 10.03.01 – Информационная безопасность

Профиль Безопасность автоматизированных систем

Факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника бакалавр

Форма обучения очная ; курс4; семестр 8;

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

Лекции 16 (час): зачет - семестр

практические (семинарские) занятия - (час): экзамен 8 семестр (1зет = 36 часов)

лабораторные занятия 16 (час): самостоятельная работа 40 (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 направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных систем».

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

Зав. выпускающей кафедрой по данному направлению _____ **Г.И. Качаева**

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

«15» 10 2018г.

АВТОР ПРОГРАММЫ

Качаева Г.И., к.э.н., ст. преп. каф. ИБ
И.О.Ф. уч. степень, ученое звание, подпись

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.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Организация работы администратора безопасности автоматизированных систем» относится к дисциплинам по выбору.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Криптографические протоколы, Технология построения защищенных АС, Безопасность операционных систем, Моделирование автоматизированных информационных систем, Криптографические методы защиты информации, Безопасность систем баз данных.

Последующими дисциплинами являются: Преддипломная практика, Защита ВКР

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
- способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
- способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
- способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);
- способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);
- способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).
- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

В результате изучения дисциплины студент должен

Знать:

- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;

Уметь:

- – использовать программные и аппаратные средства персонального компьютера; – формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

Владеть:

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;

4. Структура и содержание дисциплины «Организация работы администратора безопасности автоматизированных систем»

Общая трудоемкость дисциплины составляет 3 зачетных единиц – 108 часов, в том числе: лекционных -16 часов, лабораторных - 16 часов, СРС – 40 часов, форма отчетности экзамен в 8 семестре.

4.1.Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя 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: «Уровни и модели TCP/IP.»** IP-адресация. Разбиение IP-сетей на подсети и создание надсетей. Установка и конфигурирование TCP/IP на примере Windows Server 2008.	8	1	2		2	5	Вх. Контр.
2.	**Лекция №2** **Тема: «Организация сетевого трафика»** Анализ сетевого трафика средствами «Сетевого монитора». Устранение неполадок подключений TCP/IP.		2	2		2	5	
3.	**Лекция № 3** **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.		3	2		2	5	
4.	**Лекция №4** **Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»** Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий		4	2		2	5	
5.	**Лекция № 5** **Тема: «Ошибки DNS»** Средства устранения неполадок DNS. Средства мониторинга DNS.		5	2		2	5	АКР №1

6.	**Лекция № 6** **Тема: «Мероприятия по выявлению каналов утечки информации»** Специальные проверки. Порядок проведения специальной проверки технических средств	8	6	2		2	5	
7.	**Лекции № 7** **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		7	2		2	5	
8.	**Лекция №8** **Тема: «Управление DHCP в сетях Windows»** Анализ DHCP-трафика. Мониторинг DHCP с применением журнала аудита. Устранение неполадок DHCP. Настройка Windows Server 2008 для маршрутизации в локальной сети. Настройка маршрутизации вызовов по требованию.		8	2		2	5	
	Итого по дисциплине			**16**		**16**	**40**	**Экзамен (1 зет=36 часов)**

4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбочей программы	Наименование лабораторного (практического, семинарского) занятия	Рекомендуемая литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	Тема: «Уровни и модели TCP/IP»	№№ 1-8	2
2	Лк №2	Тема: «Организация сетевого трафика»	№№ 1-8	2
3	Лк №3	Тема: «Сравнение DNS и NetBIOS»	№№ 1-8	2
4	Лк № 4	Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»	№№ 1-8	2
5	Лк № 5	Тема: «Ошибки DNS»	№№ 1-8	2
6	Лк №6	Тема: «Мероприятия по выявлению каналов утечки информации»	№№ 1-8	2
7	Лк № 7	Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»	№№ 1-8	2
8	Лк №8	Тема: «Управление DHCP в сетях Windows»	№№ 1-8	2
Итого по дисциплине				**16**

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	Формаконтроля СРС
1.	Тема: «Уровни и модели TCP/IP»	5	№№ 1-8	Опрос, реферат, статья
2.	Тема: «Организация сетевого трафика»	5	№№ 1-8	Опрос, реферат, статья
3.	Тема: «Сравнение DNS и NetBIOS»	5	№№ 1-8	Опрос, реферат, статья
4.	Тема: «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности»	5	№№ 1-8	Опрос, реферат, статья
5.	Тема: «Ошибки DNS»	5	№№ 1-8	Опрос, реферат, статья

6.	Тема: «Мероприятия по выявлению каналов утечки информации»	5	№№ 1-8	Опрос, реферат, статья
7.	Тема: «Методы идентификации и аутентификации пользователей компьютерных систем»	5	№№ 1-8	Опрос, реферат, статья
8.	Тема: «Управление DHCP в сетях Windows»	5	№№ 1-8	Опрос, реферат, статья
Итого		**40**		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки 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. 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 экзамен

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) «Организация работы администратора безопасности автоматизированных систем»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой

№ п/п	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	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1	Лк, лб, срс	Организация работы администратора БАС	Михаилов 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.Н.	СГТУ, 2013. – 280 с	http://www.iprbookshop.ru/24451	
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
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	
ИНТЕРНЕТ РЕСУРСЫ						
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.				
	http://fstec.ru/	http://fstec.ru/				

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 на факультете имеется комплект технических средств обучения в составе:

- интерактивная доска;

– переносной компьютер (в конфигурации не хуже: процессор IntelCore 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);

– проектор (разрешение не менее 1280x1,024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных систем».

Рецензент от выпускающей кафедры по направлению 10.03.01 Информационная безопасность

подпись З.Г. Родионова

ФИО