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

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ	**УТВЕРЖДАЮ**
Декан, председатель совета факультета КТВТиЭ	**Проректор по учебной работе, председатель методического совета ДГТУ**
_____ Ш. А. Юсуфов	_____ Н. С. Суракатов
«17» 10 2018 г.	«22» 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.35 Виртуальные частные сети

Специальность 10.05.03 – Информационная безопасность

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

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника Специалист по защите информации

Форма обучения очная ; курс4; семестр 8;

Всего трудоемкость в зачетных единицах (часах) 2ЗЕТ (72 часа)

Лекции 17 (час); экзамен - семестр

практические (семинарские) занятия - (час); зачет 8 (семестр)

лабораторные занятия 17 (час); самостоятельная работа 38(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».

Программа одобрена на заседании выпускающей кафе́дры 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 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**

Цель дисциплины - изучение технологий, методов и средств обеспечения информационной безопасности (ИБ) объектов на примере виртуальные частных сетей (ВЧС), используемых в интранетах организаций.

1.2 Задачи дисциплины

Задачи изучения дисциплины:

привитие обучаемым основ культуры обеспечения ИБ объектов;

- формирование у обучаемых понимания технологий построения ВЧС как одного из средств обеспечения ИБ

объектов;

- ознакомление обучаемых с основными практическими приемами построения ВЧС;

- обучение различным средствам построения ВЧС.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Виртуальные частные сети» относится к базовой части учебного плана

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: языки программирования.

Последующими дисциплинами являются: Защита программ и данных

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3).

В результате изучения дисциплины студент должен

Знать: методы концептуального проектирования технологий обеспечения ИБ объектов; -принципы организации технического, программного и информационного обеспечения ИБ объектов; -основные тенденции и закономерности обеспечения ИБ объектов и средств их реализации; -основные стандарты обеспечения ИБ объектов; -подходы к интеграции средств обеспечения ИБ объектов в единую систему обеспечения ИБ; -комплексный подход к обеспечению ИБ объектов;

Уметь: осуществлять выбор функциональной структуры системы обеспечения ИБ объектов; -обосновывать принципы организации технического, программного и информационного обеспечения ИБ объектов; -проектировать и реализовывать комплексную защиту информации на объектах в соответствии со стандартами по оценке защищенных систем; -применять стандартные решения для защиты информации на объектах и квалифицированно оценивать их качество; -осуществлять управление и администрирование средств защиты объектов; -организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения ИБ объектов.

Владеть: терминологией и системным подходом к обеспечению ИС объектов; -навыками обеспечения ИБ простых объектов; -навыками управления и администрирования средств защиты информации на объектах;

4. Структура и содержание дисциплины «Виртуальные частные сети»

Общая трудоемкость дисциплины составляет 2 зачетных единиц – 72 часа, в том числе: лекционных -17часов, лабораторных - 17 часов, СРС – 38часов, форма отчетности зачет в 8 семестре.

4.1.Содержание дисциплины

	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделясеместра	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: «Базовые сведения о технологиях обеспечении ИБ объектов».** Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов	5	1.2	2		2	4	Вх. Контр.
2.	**Лекция №2** **Тема: «Межсетевые экраны (МЭ)»** Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ.		3.4	2		2	4	
3.	**Лекция № 3** **Тема: «Базовые сведения о VPN»** Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи.		5.6	2		2	5	АКР №1
4.	**Лекция №4** **Тема: «Туннелирование в VPN»** Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPNагентов		7.8	2		2	4	
5.	**Лекция № 5** **Тема: «Протокол PPTP»** Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.		9.10	2		2	4	АКР №2

6.	**Лекция № 6** **Тема: «Протокол L2TP»** Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.		11.12	2		2	5	
7.	**Лекции № 7** **Тема: «Протокол IPSec»** Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов	7	13.14	2		2	4	
8.	**Лекция №8** **Тема: «Основные технологии построения защищенных систем»** Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты		15.16	2		2	4	АКР №3
9.	**Лекция №9** **Тема: «Виды, протоколы и безопасность VLAN»** VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.		17	1		1	4	
	Итого по дисциплине			**17**		**17**	**38**	**зачет**

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: «Базовые сведения о технологиях обеспечении ИБ объектов»	№№ 1-10	2
2	Лк №2	Тема: «Межсетевые экраны (МЭ)»	№№ 1-10	2
3	Лк №3	Тема: «Базовые сведения о VPN»	№№ 1-10	2
4	Лк № 4	Тема: «Туннелирование в VPN»	№№ 1-10	2
5	Лк № 5	Тема: «Протокол PPTP»	№№ 1-10	2
6	Лк №6	Тема: «Протокол L2TP»	№№ 1-10	2
7	Лк № 7	Тема: «Протокол IPSec»	№№ 1-10	2
8	Лк №8	Тема: «Основные технологии построения защищенных систем»	№№ 1-10	2
9	Лк №9	Тема: «Виды, протоколы и безопасность VLAN»	№№ 1-10	1
Итого по дисциплине				**17**

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: «Базовые сведения о технологиях обеспечении ИБ объектов»	4	№№ 1-10	Опрос, реферат, статья
2.	Тема: «Межсетевые экраны (МЭ)»	4	№№ 1-10	Опрос, реферат, статья
3.	Тема: «Базовые сведения о VPN»	5	№№ 1-10	Опрос, реферат, статья
4.	Тема: «Туннелирование в VPN»	4	№№ 1-10	Опрос, реферат, статья
5.	Тема: «Протокол PPTP»	4	№№ 1-10	Опрос, реферат, статья
6.	Тема: «Протокол L2TP»	5	№№ 1-10	Опрос, реферат, статья
7.	Тема: «Протокол IPSec»	4	№№ 1-10	Опрос, реферат, статья
8.	Тема: «Основные технологии построения защищенных систем»	4	№№ 1-10	Опрос, реферат, статья
9.	Тема: «Виды, протоколы и безопасность VLAN»	4	№№ 1-10	Опрос, реферат, статья
Итого		**38**		

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. Что такое программное обеспечение?
2. Жизненный цикл программного обеспечения.
3. Модели разработки программного обеспечения
4. Объектно-ориентированный подход.
5. Модель «водопада» разработки программного обеспечения.
6. Определение, краткая характеристика. Агрегацией и композиция классов.
7. Понятия и соотношение. Интерфейсы. Проектирование классов. Структура класса.
8. Диаграммы состояний объекта. Способы проектирование методов класса.
9. Парадигмы программирования: визуальная, функциональная, процедурная, объектно-ориентированная и т.д.
10. Объектно-ориентированная парадигма: понятия объекта, класса объектов; основные понятия объектно-ориентированного программировании (инкапсуляция, наследование и полиморфизм); классы и объекты; интерфейсы и реализация.

Контрольные вопросы для проверки текущих знаний студентов

Аттестационная контрольная работа №1

1. Состав и классификация средств обеспечения ИБ объектов.
2. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов
3. Назначение и функции МЭ.
4. Основные компоненты МЭ.
5. Принцип работы МЭ, варианты позиционирования МЭ.
6. Руководящий документ Гостехкомиссии РФ по МЭ.
7. Профили защиты для МЭ.
8. Основные типы МЭ.
9. Различные подходы к определению VPN, определение компании Check Point Software Technologies.
10. Цели и задачи применения VPN-технологий.
11. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи.

Аттестационная контрольная работа №2

1. Туннелирование.
2. Механизм туннелирования как основа построения VPN.
3. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.
4. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.
5. Базовая схема VPN.
6. VPN-агенты.
7. Функции VPN агентов
8. Функции протокола.
9. Компоненты PPTP.
10. Сценарии работы протокола.
11. Архитектура PPTP.
12. Управляющее соединение и управляющие сообщения.
13. Инкапсуляция данных при передаче.
14. Аутентификация, контроль доступа и шифрование.
15. Настройка VPN на базе протокола PPTP в среде Windows 2000.

Аттестационная контрольная работа №3

1. Основные функции и характеристики протокола.
2. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных.
3. Обработка входящих и исходящих данных.
4. Настройка VPN на базе протокола E2TP в среде Windows 2000.
5. Архитектура IPSec.
6. Функции, принцип работы, сценарии применения IPSec.
7. Обзор основных компонентов IPSec.
8. Главные базы данных IPSec: SPD, SAD, PAD.
9. Политики безопасности IPSec.
10. Ассоциации безопасности (SA): определение, назначение, процедуры управления.
11. Обработка IP-трафика.
12. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов

Перечень вопросов на зачет

1. Состав и классификация средств обеспечения ИБ объектов.
2. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов
3. Назначение и функции МЭ.
4. Основные компоненты МЭ.
5. Принцип работы МЭ, варианты позиционирования МЭ.
6. Руководящий документ Гостехкомиссии РФ по МЭ.
7. Профили защиты для МЭ.
8. Основные типы МЭ.
9. Различные подходы к определению VPN, определение компании Check Point Software Technologies.
10. Цели и задачи применения VPN-технологий.
11. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи.
12. Туннелирование.
13. Механизм туннелирования как основа построения VPN.
14. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.
15. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.
16. Базовая схема VPN.
17. VPN-агенты.

18. Функции VPN агентов
19. Функции протокола.
20. Компоненты PPTP.
21. Сценарии работы протокола.
22. Архитектура PPTP.
23. Управляющее соединение и управляющие сообщения.
24. Инкапсуляция данных при передаче.
25. Аутентификация, контроль доступа и шифрование.
26. Настройка VPN на базе протокола PPTP в среде Windows 2000.
27. Основные функции и характеристики протокола.
28. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных.
29. Обработка входящих и исходящих данных.
30. Настройка VPN на базе протокола E2TP в среде Windows 2000.
31. Архитектура IPSec.
32. Функции, принцип работы, сценарии применения IPSec.
33. Обзор основных компонентов IPSec.
34. Главные базы данных IPSec: SPD, SAD, PAD.
35. Политики безопасности IPSec.
36. Ассоциации безопасности (SA): определение, назначение, процедуры управления.
37. Обработка IP-трафика.
38. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов

.

Вопросы проверки остаточных знаний

1. Структуры данных
2. Динамические структуры данных
3. Деревья
4. Алгоритмы
5. Алгоритмы на графах
6. Алгоритмы сортировки
7. Алгоритмы поиска
8. Технологии проектирования и программирования
9. Объектно-ориентированный подход к разработке ПО
10. Технология создания программного кода»
11. Технологии коллективной разработки программного обеспечения
12. Технологические средства разработки программного обеспечения
13. Методы отладки и тестирования программ
14. Документирование и оценка качества программных продуктов

7. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Виртуальные частные сети»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой _____

№	Виды заня-тий (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	Компьютерные сети. Принципы, технологии, протоколы, учебник. Изд. 4-е.	Олифер В.Г., Олифер Н.А.	СПб.: Питер 2010 916 с.	http://www.iprbookshop.ru/61558	
2.	Лк, пр, срс	Безопасность сетей. Полное руководство: Пер. с англ.	Брэгг Р.	М: Эком 2006 912 с.	http://www.iprbookshop.ru/29257	
3.	Лк, пр, срс	Протоколы и ресурсы Internet.	Семенов Ю.А.	М.: Радио и связь 1996 320 с.	http://www.iprbookshop.ru/24451	
ДОПОЛНИТЕЛЬНАЯ						
4.	Лк, лб, срс	Обнаружение нарушений безопасности в сетях, 3-е изд.: Пер. с англ.	Норткат С., Новак Д.	М.:Вильямс 2003 448 с	http://www.iprbookshop.ru/73733.html	
5.	Лк, лб, срс	Системное и сетевое администрирование. Практическое руководство. 2-е изд	Лимончелли Т., Хоган К., Чейлап С.	М.: Символ-Плюс 2006 944 с.	http://www.iprbookshop.ru/73124514	
ИНТЕРНЕТ - РЕСУРСЫ						
6.	Лк, пз, лб, срс	http://www.interface.ru - энциклопедия информационных технологий				
7.	Лк, пз, лб, срс	http://window.edu.ru – единое окно доступа к образовательным ресурсам				
8.	Лк, пз, лб, срс	http://www.intuit.ru – интернет-университет				
9.	Лк, пз, лб, срс	http://www.e.lanbook.com/books "Электронно-библиотечная система				
10.	Лк, пз, лб, срс	www.twirpx.com ресурс для студентов и преподавателей				

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 1280x1024);

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 специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Рецензент _____ от выпускающей кафедры по специальности

подпись ФИО