ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА РАДИОФИЗИКИ И ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

УТВЕРЖДАЮ:
проректор по научно-методической и учебной работе
_____ Е.И. Скафа
«22» апреля 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «ЗАЩИТА ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СЕТЯХ»

Направление подготовки:	10.04.01 Информационная безопасность
Магистерская программа:	Информационная безопасность
Образовательная программа:	академическая магистратура
Квалификация:	магистр
Форма обучения:	очная

Донецк 2020

УТВЕРЖДАЮ:
Декан физико-технического
факультета
_____ С. А. Фоменко
«17» апреля 2020 г.

МП

Программа составлена с учетом Федерального государственного образовательного стандарта высшего образования направления подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 01 декабря 2016г. № 1513;
учебного плана и основной образовательной программы Информационная безопасность направления подготовки 10.04.01 Информационная безопасность разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчики:
д.т н., профессор кафедры радиофизики
и инфокоммуникационных технологий _____ В.В. Данилов

ассистент кафедры РФ и ИКТ _____ Я.И. Рушечников

Программа учебной дисциплины утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол №17 от «06» апреля 2020 г.

Заведующий кафедрой радиофизики
и инфокоммуникационных технологий _____ Данилов В.В.

Программа учебной дисциплины одобрена учебно-методической комиссией физико-технического факультета
Протокол №5 от «15» апреля 2020 г.

Председатель учебно-методической
комиссии факультета _____ В.Н. Котенко

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Защита информации в виртуальных сетях» относится к вариативной части профессионального блока. Трудоемкость освоения дисциплины составляет 3 зач.ед. или 108 час. Изучается во 2 семестре, по дисциплине предусмотрен экзамен.

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Операционные системы», «Компьютерные сети», «Защита информации в компьютерных сетях», «Пакеты прикладных программ для научных расчетов». Освоение дисциплины обеспечивает формирование у студентов современных навыков по разработке и внедрению виртуальных сетей в существующие информационные системы.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины		
Направление подготовки	10.04.01 Информационная безопасность	
Магистерская программа	Информационная безопасность	
Образовательная программа	академическая магистратура	
Квалификация	магистр	
Количество содержательных модулей	2	
Дисциплина базовой / вариативной части образовательной программы	вариативная часть	
Формы контроля (МК, экзамен, зачет)	Модульный контроль, сдача лабораторных работ, экзамен	
Показатели	очная форма обучения	заочная форма обучения
Количество зачетных единиц (кредитов)	3	
Год подготовки	1	
Семестр	2	
Количество часов	108	
- лекционных	14	
- практических, семинарских	14	
- лабораторных	28	
- самостоятельной работы	52	
в т.ч. индивидуальное задание		
Недельное количество часов,	8	
в т.ч. аудиторных	3	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Изучить основные возможности обеспечения безопасности в виртуальных сетях.

Задачи:

1) Изучить способы прототипирования виртуальных компьютерных сетей с использованием специальных инсталляционных пакетов.
2) Изучить способы развёртывания и сопровождения специальных систем, обеспечивающих работу виртуальных сетей.
3) Изучить основные достоинства и недостатки виртуальных сетей.

4) Изучить разнообразие виртуальных сетевых технологий.

5) Проанализировать средства аудита безопасности виртуальных сетей.

Требования к результатам освоения дисциплины. Процесс изучения дисциплины «Защита информации в виртуальных сетях» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ направления подготовки 10.04.01 Информационная безопасность (квалификация «магистр») и основной образовательной программы высшего профессионального образования направления подготовки 10.04.01 Информационная безопасность.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ГОС ВПО по данному направлению подготовки (профилю):

а) общекультурных (ОК):

- способностью к абстрактному мышлению, анализу, синтезу (ОК - 1);
- способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения (ОК - 2).

б) общепрофессиональных (ОПК):

- способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК -1);
- способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК – 2).

в) профессиональных (ПК):

проектная деятельность:

- способностью анализировать направления развития информационных (телекоммуникационных), прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1);
- способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);
- способностью производить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3);
- способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4).

научно-исследовательская деятельность:

- способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК - 5);
- способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок (ПК - 6);
- способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК - 8).

педагогическая деятельность:

- способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК - 11);

организационно-управленческая деятельность:

- способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК - 12);

В результате изучения учебной дисциплины студент должен.

Знать:
- разнообразие технологий виртуальных сетей;
- недостатки и преимущества каждой из технологий;
- аспекты безопасности, на которые влияет внедрение виртуальных сетей;

Уметь:
– осуществлять развёртывание и конфигурирование систем виртуальных сетей
– проводить аудит систем на соответствие критериям информационной безопасности;
– осуществлять внедрение современных методов обеспечения безопасности (таких как механизмы туннелирования и сквозного шифрования);

Владеть:
– знаниями по работе с серверными реализациями операционных систем;
– методикой поиска уязвимостей в сетях ip сетях;
– навыками работы с сертифицированными средствами анализа защищенности.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Порядковый номер и тема	Краткое содержание темы
Содержательный модуль 1	
Тема 1. Базовые концепции VPN	Терминология VPN. Место VPN в иерархии сетевой модели ISO/OSI. Базовые возможности VPN. Ограничения VPN. Архитектура VPN а так же сферы применения данной технологии.
Тема 2. Внутренние процессы в сетях VPN	IP туннелирование. IPSec туннелирование. TLS туннелирование. Организация VPN на уровне сетевого интерфейса. Построение маршрута.
Тема 3. Криптографическая подсистема VPN	Инфраструктура открытых ключей. Сертификаты. Отзыв сертификатов. Перевыпуск сертификатов
Тема 4. Исследование серверных реализаций VPN	Технология PPTP (Point-to-Point Tunneling Protocol). Технология PPPoE (Point-to-point protocol over Ethernet). Технология L2TP(*Layer 2 Tunneling Protocol).* Технология OpenVPN
Содержательный модуль 2	
Тема 5. Конфигурирование и развёртывание серверных реализаций VPN.	Установка и настройка сервера PPTP. Установка и настройка сервера PPPoE. Установка и настройка сервера L2TP.Установка и настройка сервера OpenVPN
Тема 6. Клиентская сторона VPN	Роль клиента в организации виртуальной сети. Функции безопасности клиента. Уязвимости исходящие от клиентов. Конфигурирование клиентских устройств. Концепция BYOD.
Тема 7. Специальные средства туннелирования	Аппаратные средства формирования туннеля виртуальной сети. Специальные устройства с интегрированными сервисами безопасности. Устройства формирования безопасного канала точка-точка со сквозным шифрованием
Тема 8. Облачные провайдеры VPN	Архитектура облачных серверов VPN. Достоинства и недостатки данных реализаций.

Тематический план													
Названия содержательных модулей и тем	**Количество часов**												
	Очная форма обучения						**Заочная форма обучения**						
	всего	в т.ч.					всего	в т.ч.					
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Тема 1. Базовые концепции VPN	14	2		6	6								
Тема 2. Внутренние процессы в сетях VPN	13	2		4	7								
Тема 3. Криптографическая подсистема VPN	13	2		4	7								
Тема 4. Исследование серверных реализаций VPN	13	2		4	7								
Итого по содержательному модулю 1	**53**	**8**		**18**	**27**								
Тема 5. Конфигурирование и развёртывание серверных реализаций VPN.	12	2		4	6								
Тема 6. Клиентская сторона VPN	15	2		6	7								
Тема 7. Специальные средства туннелирования	15	4		4	7								
Тема 8. Облачные провайдеры VPN	13	2		4	7								
Итого по содержательному модулю 2	**55**	**10**		**18**	**27**								
Всего по дисциплине	**108**	**18**		**36**	**54**								

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	*Название темы*	*Количество часов*
1	Базовые концепции VPN	2
2	Внутренние процессы в сетях VPN	2
3	Криптографическая подсистема VPN	2
4	Исследование серверных реализаций VPN	2
5	Конфигурирование и развёртывание серверных реализаций VPN	2
6	Клиентская сторона VPN	2
7	Специальные средства туннелирования	2
8	Облачные провайдеры VPN	2
9	Заключительное занятие.	2
	ВСЕГО	**18**

Темы лабораторных занятий

№ п/п	*Название темы*	*Количество часов*
1	Установка и конфигурирование многофункциональной операционной системы с интегрированными сервисами безопасности	2
2	Настройка Point-to-site VPN на pfSense	2
3	Исследование безопасности обмена данных через VPN	2
4	Настройка серверных и клиентских реализаций PPTP	4
5	Настройка серверных и клиентских реализаций PPPoE	4
6	Настройка серверных и клиентских реализаций L2TP	4
7	Аудит протокола SSL/TLS	4
8	Исследование облачных vpn решений.	2
9	Средства аудита VPN сетей.	2
10	Заключительное занятие.	2
	ВСЕГО	**28**

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов

Самостоятельная работа студентов по курсу «Безопасность IP-телефонии» предусматривает:
– систематическое ведение конспекта лекций и проработку лекционного материала;
– изучение дополнительной литературы и интернет-источников, в т.ч. рекомендуемых этой программой;
– добросовестную подготовку к лабораторным занятиям;
– самостоятельное решение задач лабораторных работ;
– своевременное выполнение и качественное оформление отчётов по лабораторным работам.

№ п/п	*Название темы*	*Количество часов*
1	Распространение VPN	10
2	Провайдинг интернет услуг с использование VPN.	8
3	Сравнение VPN и прокси сервера.	10
4	Уязвимости VPN Клиентов	8
5	Уязвимости VPN Серверов	8
6	Уязвимости облачных реализаций VPN.	8
	ВСЕГО	**52**

7. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Что такое VPN?
2. Особенности клиентской реализации VPN.
3. Сферы использования VPN.
4. Туннелирование в виртуальных сетях.
5. Адресация в виртуальных сетях.
6. Архитектура виртуальных сетей.
7. Виды туннелирования.
8. Что такое Tun/Tap интерфейс
9. Процесс установки маршрута VPN
10. Принятие и отправка пакетов по туннелю.

8. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра радиофизики и инфокоммуникационных технологий
Программа подготовки: магистратура
Дисциплина «Защита информации в виртуальных сетях»
Направление подготовки: 10.04.01 Информационная безопасность, семестр 2.

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА ВАРИАНТ №1

1. Адресация в виртуальных сетях

2. Что такое Tun/Tap интерфейс

3. Особенности клиентской реализации VPN.

Утверждено на заседании кафедры. Зав. кафедрой РФ и ИКТ _____ В.В. Данилов

№ ____ от _____201_г. Экзаменатор _____ Я.И.Рушечников

Критерии оценивания модульного контроля

Номер задания	*Количество баллов*
1	5
2	5
3	8
Всего	18

9. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Теоретические вопросы к экзамену

1. Что такое VPN?
2. Особенности клиентской реализации VPN.
3. Сферы использования VPN.
4. Туннелирование в виртуальных сетях.
5. Адресация в виртуальных сетях.
6. Архитектура виртуальных сетей.
7. Виды туннелирования.
8. Что такое Tun/Tap интерфейс
9. Процесс установки маршрута VPN
10. Принятие и отправка пакетов по туннелю.
11. Мониторинг интерфейсов VPN.
12. Криптографическая подсистема виртуальной сети
13. Технология PPPoE. Особенности и ключевые возможности.
14. Технология L2TP. Особенности и ключевые возможности.
15. Технология PPTP. Особенности и ключевые возможности.
16. Технология OpenVPN. Особенности и ключевые возможности.
17. Аудит виртуальных сетей.
18. Совместное использование VPN и других технологий

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра радиофизики и инфокоммуникационных технологий
Программа подготовки: магистратура
Дисциплина «Защита информации в виртуальных сетях»
Направление подготовки: 10.04.01 Информационная безопасность, семестр 2.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Мониторинг интерфейсов VPN. Что такое Tun/Tap интерфейс

2. Что такое Tun/Tap интерфейс

3. Технология PPTP. Особенности и ключевые возможности.

Утверждено на заседании кафедры. Зав. кафедрой РФ и ИКТ _____ В.В. Данилов

№ ____ от _____201_г. Экзаменатор _____ Я.И.Рушечников

Критерии оценивания экзамена

Номер задания	*Количество баллов*
1	10
2	10
3	10
4	10
5	10
Всего	**50 баллов**

10.ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

(Тестовые задания программой не предусмотрены)

10. КРИТЕРИИ ОЦЕНИВАНИЯ

По курсу предполагается проведение промежуточной аттестации в виде модульного контроля, выполнение практических и лабораторных работ и экзамена. Экзамен сдают студенты с целью повышения рейтинга.

Распределение баллов, которые могут получить студентыв процессе изучения дисциплины

Организационно-учебная работа студента	**СРС**		**Всего**
	Индивидуальная работа	**Модульный контроль**	
Max 10 баллов	max 72 баллов	max 18 баллов	100 баллов
Экспресс-опрос на лекциях и активность на лабораторных занятиях; проверка конспектов	Выполнение и защита лабораторных работ	Выполнение модульной контрольной работы	

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	**Оценка по 100-балльной шкале**	**Оценка по государственной шкале (экзамен, дифференцированный зачет)**	**Оценка по государственной шкале (зачет)**
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской.

Лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами, доской.

12. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
	Основная литература		
1.	Гордеев, А. В. Операционные системы Учеб. для студентов вузов, обучающихся по направлению подгот. бакалавров и магистров и направлению подгот. дипломир. специалистов "Информатика и вычисл. техника" / А. В. Гордеев. - 2-е изд. - СПб. и др. : Питер : Питер Принт, 2005. - 415 с.	5	
2.	IP-телефония» (третье издание) / Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. М.: Радио и связь, 2006. - 336 с.: ил. ISBN 5-256-01585-0	2	
3.	Технология обеспечения безопасности объектов [Текст] : учебное пособие для магистров высших учебных заведений, обучающихся по направлению подготовки 10.04.01 Информационная безопасность / [Шелехова О.Г.] ; ДОННУ. – Донецк : Цифровая типография, 2019. – 125 с.		+
	Дополнительная литература		
4.	Таненбаум, Э. Современные операционные системы / Э. Таненбаум ; [Перевод А. Леонтьев]. - 2-е изд. - СПб. и др. : Питер : Питер Принт, 2005. - 1037 с.	2	
5.	Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. - 233 с		+

13. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1.http://donnu.ru/ – сайт ДонНУ.
2.http://library.donnu.ru/ – сайт библиотеки ДонНУ.
3. www.ansoft.com – сайт компании Ansoft – разработчика программы HFSS

14. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);

3. Oracle Virtual Box;
4. Cisco packet tracer.

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При реализации программы дисциплины могут использоваться следующие виды электронного взаимодействия преподаватель-студент:

- размещение учебных материалов в облачных хранилищах преподавателей для использования студентами при подготовке к занятиям;
- рассылка по электронной почте материалов и заданий для выполнения, проверка выполненных заданий;
- поддержка странички преподавателя и групп преподаватель-студенты в социальных сетях для обеспечения текущего контроля работы студентов

Рабочая программа рассмотрена и переутверждена на заседании кафедры радиофизики и инфокоммуникационных технологий с изменениями (без изменений) на 2021 год.
Протокол № ___ от «_____» _____ 20____ г.

Заведующий кафедрой РФ и ИКТ _____В.В. Данилов

Рабочая программа рассмотрена и переутверждена на заседании кафедры радиофизики и инфокоммуникационных технологий с изменениями (без изменений) на 2022 год.
Протокол № ___ от «_____» _____ 20____ г.

Заведующий кафедрой РФ и ИКТ _____В.В. Данилов