Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ _Василенко В.Н._
(подпись) (Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Виртуальные частные сети

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

1. Цели и задачи дисциплины

Целью преподавания дисциплины "Виртуальные частные сети" является изучение методов и средств построения и эксплуатации беспроводных технологий для обеспечения информационной безопасности на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации в беспроводных коммуникациях.

Задачи дисциплины:

- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- управление информационной безопасностью автоматизированных систем;
- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате	изучения учебной дисциплины обучающийся должен:	
			Знать	Уметь	Владеть
1	ОПК-8	Способность к освоению новых образцов программных, технических средств и информационных технологий	Программные, технические средства и информационные технологии	Применять знания для освоения новых программных и технических средств	Навыками работы с новыми программными, техническими средствами ИТ
2	ПК-23	Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Основные компоненты, формирующие VPN	Осуществлять выбор подходящей VPN	Приемами и методами выбора архитектуры VPN
3	ПК-27	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной	Политики информационной безопасности автоматизированных систем, управленческий трафик, SMTP и DNS	Реализовывать частные политики информационной безопасности виртуальных частных сетей	Технологиями реализации политик безопасности и управленческого трафика

		системы, осуществлять мониторинг безопасности автоматизированной системы			

3. Место дисциплины в структуре ОП ВО

Дисциплина «Виртуальные частные сети» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

- Мультимедиатехнологии
- Компьютерная и инженерная графика
- Безопасность сетей ЭВМ
- Защита web-сайтов
- Система обнаружения компьютерных атак
- Сети и системы передачи информации
- Техническая защита информации
- Учебная практика, практика по получению первичных профессиональных умений
- Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности
- Программно-аппаратные средства обеспечения информационной безопасности
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности

Дисциплина является предшествующей для защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 4 зачетных единицы.

Виды учебной работы	Всего часов	Семестр
		10
Общая трудоемкость дисциплины	**144**	**144**
Контактная работа, в.т.ч. аудиторные занятия:	**40**	**40**
Лекции	20	20
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	20	20
в том числе в форме практической подготовки	20	20
Консультации текущие	1	1
Консультации перед экзаменом	2	2
Вид аттестации – экзамен	0,2	0,2
Самостоятельная работа:	**68**	**68**
Проработка конспекта лекций (подготовка к тесту и собеседованию)	10	10
Проработка материалов по учебнику (подготовка к	31	31

тесту и собеседованию)		
Реферат	12/1	12
Решение ситуационных задач	15/5	15
Подготовка к экзамену (контроль)	**33,8**	**33,8**

5 Содержание дисциплины, структурированное по разделам с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела	Трудоемкость раздела, час
1	Введение в технологию VPN	Компоненты, формирующие VPN. Развитие VPN. Необходимость VPN. Потребности бизнеса в VPN. Сетевая безопасность в VPN. Требования безопасности.	8
2	Преимущества и недостатки VPN	Полезные свойства VPN. Экономический эффект проектирования сетей. Преимущества для провайдеров. Конкурентоспособность. Стоимость технологии VPN. Гарантии качества обслуживания.	8
3	Архитектура VPN	Выбор подходящей VPN. VPN на основе брандмауэра. VPN на основе черного ящика. VPN на основе маршрутизатора. VPN на основе удаленного доступа. VPN на основе набора прокси. VPN с мультисервисными приложениями. VPN на основе программного обеспечения. Коммутация туннелей для VPN. Сравнение производительности.	18
4	Топологии VPN	Введение в топологию. Топология соединения брандмауэра/VPN и клиента. Топология VPN для соединения между ЛВС. Топология соединения VPN/брандмауэр и интранет/экстранет. Топология VPN на сонове ATM. Топология аппаратной VPN. Топология VPN/NAT. Топология коммутатора VPN. Вложенные туннели.	18
5	Реализация VPN	Размещение архитектуры VPN. Проблемы маршрутизации, адресации IP/NAT и удаленного доступа. Вопросы DNS/SMTP	20
6	Инсталляция VPN	Получение и присвоение IP-адресов. Реализация политики безопасности, управленческого трафика, SMTP и DNS. Услуги VPN поставщиков услуг. Услуги автономных VPN.	14
7	Сопровождение VPN	Избыточные линии. Обновление ПО. Техническая поддержка на месте. Телефонная поддержка. Система поддержки удаленных пользователей. Мониторинг. Сигнализация. Ведение журналов. Корреляция событий. Шифрование и инкапсуляция. Управление ключами. Генераторы случайных чисел. Сертификаты. Качество обслуживания.	12
8	Безопасность VPN	Криптография. Шифрование. Безопасная коммуникация и аутентификация.	10

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ (или С), час	СРО, час
1	Введение в технологию VPN	2	-	6
2	Преимущества и недостатки VPN	2	-	6
3	Архитектура VPN	2	4	12
4	Топологии VPN	4	6	8
5	Реализация VPN	2	6	12

6	Инсталляция VPN	2	4	8
7	Сопровождение VPN	4	-	8
8	Безопасность VPN	2	-	8

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Введение в технологию VPN	Компоненты, формирующие VPN. Развитие VPN. Необходимость VPN. Потребности бизнеса в VPN. Сетевая безопасность в VPN. Требования безопасности.	2
2	Преимущества и недостатки VPN	Полезные свойства VPN. Экономический эффект проектирования сетей. Преимущества для провайдеров. Конкурентоспособность. Стоимость технологии VPN. Гарантии качества обслуживания.	2
3	Архитектура VPN	Выбор подходящей VPN. VPN на основе брандмауэра. VPN на основе черного ящика. VPN на основе маршрутизатора. VPN на основе удаленного доступа. VPN на основе набора прокси. VPN с мультисервисными приложениями. VPN на основе программного обеспечения. Коммутация туннелей для VPN. Сравнение производительности.	2
4	Топологии VPN	Введение в топологию. Топология соединения брандмауэра/VPN и клиента. Топология VPN для соединения между ЛВС. Топология соединения VPN/брандмауэр и интранет/экстранет.	2
		Топология VPN на основе ATM. Топология аппаратной VPN. Топология VPN/NAT. Топология коммутатора VPN. Вложенные туннели.	2
5	Реализация VPN	Размещение архитектуры VPN. Проблемы маршрутизации, адресации IP/NAT и удаленного доступа. Вопросы DNS/SMTP	2
6	Инсталляция VPN	Получение и присвоение IP-адресов. Реализация политики безопасности, управленческого трафика, SMTP и DNS. Услуги VPN поставщиков услуг. Услуги автономных VPN.	2
7	Сопровождение VPN	Избыточные линии. Обновление ПО. Техническая поддержка на месте. Телефонная поддержка. Система поддержки удаленных пользователей. Мониторинг. Сигнализация.	2
		Ведение журналов. Корреляция событий. Шифрование и инкапсуляция. Управление ключами. Генераторы случайных чисел. Сертификаты. Качество обслуживания.	2
8	Безопасность VPN	Криптография. Шифрование. Безопасная коммуникация и аутентификация.	2

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, час
	Архитектура VPN	VPN на основе брандмауэра. VPN на основе черного ящика. VPN на основе маршрутизатора.	2

1		VPN на основе удаленного доступа. VPN на основе набора прокси. VPN с мультисервисными приложениями. VPN на основе программного обеспечения. Коммутация туннелей для VPN. Сравнение производительности.	2
2	Топологии VPN	Топология соединения брандмауэра/VPN и клиента. Топология VPN для соединения между ЛВС.	2
		Топология соединения VPN/брандмауэр и интранет/экстранет. Топология VPN на основе ATM.	2
		Топология аппаратной VPN. Топология VPN/NAT. Топология коммутатора VPN. Вложенные туннели.	2
3	Реализация VPN	Размещение архитектуры VPN.	2
		Проблемы маршрутизации, адресации IP/NAT и удаленного доступа.	2
		Вопросы DNS/SMTP	2
4	Инсталляция VPN	Получение и присвоение IPадресов. Реализация политики безопасности.	2
		Реализация управленческого трафика, SMTP и DNS. Услуги VPN поставщиков услуг. Услуги автономных VPN.	2

5.2.3 Лабораторный практикум не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Введение в технологию VPN	Тест	6
		Собеседование	
		Реферат	
		Экзамен	
2	Преимущества и недостатки VPN	Тест	6
		Собеседование	
		Реферат	
		Экзамен	
3	Архитектура VPN	Тест	12
		Ситуационная задача	
		Экзамен	
4	Топологии VPN	Тест	8
		Собеседование	
		Реферат	
		Экзамен	
5	Реализация VPN	Тест	12
		Собеседование	
		Реферат	
		Ситуационная задача	
		Экзамен	
	Инсталляция VPN	Тест	

6		Собеседование	8
		Экзамен	
7	Сопровождение VPN	Тест	8
		Собеседование	
		Ситуационная задача	
		Экзамен	
8	Безопасность VPN	Реферат	8
		Собеседование	
		Экзамен	

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. (гриф МО) 4-е изд. – СПб.: Питер, 2016. – 944 с.: ил.
2. Абрамов Г.В., Архитектура ЭВМ и систем [Текст]: Учебное пособие. Воронеж, 2016
3. Платонов, В. В. Программно-аппаратные средства защиты информации [Текст] : учебник для студ. вузов / В. В. Платонов. М. : Академия, 2015. 336 с.

6.2 Дополнительная литература

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Сетевые операционные системы: Учебное пособие для студентов вузов. – СПб.: Питер, 2018.
2. Андрианов В.В. и др.,Обеспечение информационной безопасности бизнеса [Электронный ресурс]/.— М.: ЦИПСиР, 2011 (http://www.iprbookshop.ru/38525)
3. Ермаков А.Е. Основы конфигурирования корпоративных сетей Cisco [Электронный ресурс]: учебное пособие/ М.: Учебно-методический центр, 2015, (http://www.iprbookshop.ru/26823)
4. Гордеев В.А., Операционные системы. СПб. Питер, 2014
5. Савельев А. О., Решения Microsoft для виртуализации ИТинфраструктуры предприятий [Текст]: Интернет-Университет Информационных Технологий , 2014. (http://www.knigafund.ru/books/177879)
6. Запечников С.В. Основы построения виртуальных частных сетей [Электронный ресурс]: учебное пособие для вузов/ Запечников С.В., Милославская Н.Г., Толстой А.И.— М.: Горячая линия Телеком, 2014.— 248 с (http://www.iprbookshop.ru/37194)
7. Алексеев В.А. Маршрутизация и защита сетевого трафика в сетях TCP/IP [Электронный ресурс]: методические указания к проведению лабораторных работ / Алексеев В.А.— Липецк: ЛГТУ, ЭБС АСВ, 2015. (http://www.iprbookshop.ru/55104)
8. Терри Вильям Оглтри, Firewalls. Практическое применение межсете вых экранов [Электронный ресурс]/ -М.: ДМК Пресс, 2018 (http://www.iprbookshop.ru/7797)
9. Советов Б.Я., Цехановский В.В., Информационные технологии: теоретические основы: Учебное пособие.СПб.: Издательство «Лань», 2016. (https://e.lanbook.com/reader/book/71733)

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Ивлиев М.Н., Виртуальные частные сети [Электронный ресурс] : методические указания к самостоятельной работе обучающихся для студентов, обучающихся по направлению 10.05.03 «Информационная безопасность автоматизированных систем», очной формы обучения / М. Н. Ивлиев; ВГУИТ, Кафедра информационных технологий, моделирования и управления. Воронеж : ВГУИТ, 2016. 57 с. (http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/2708)

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа: (http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813). Загл. с экрана

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: ОС MS Windows XP, Microsoft Office 2007, эмулятор сети CISCO Packet Tracer (свободно распространяемое ПО); электронная образовательная среда ФГБОУ ВО “ВГУИТ”.

7 Материально-техническое обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Аудитория для проведения лекционных занятий (ауд.	Комплект мебели для учебного процесса – 30 шт.	

334)		
Аудитории для проведения практических занятий:		
Ауд. 332 – лаборатория сетей и систем передачи информации каф. ВМиИТ	Рабочие места на базе вычислительной техники – Core2 DuoE7300 (12 шт.); Стенд сетей передачи информации, состоящий из следующего оборудования: Межсетевой экран D-Link DFL-1600 серии NetDefend; Управляемый коммутатор CISCO881; Неуправляемый коммутатор D-Link DES-1016D; Точка доступа Mikrotik cAP2nD (RBcAP2nD); Маршрутизатор D-Link DIR-300;	Microsoft Windows Server 2003 Сублицензионный договор № 42082/VRN3 от 21 августа 2013 г. на право использование программы DreamSpark Electronic Software Deliver; Microsoft Office 2007, Microsoft Office Professional Plus 2007 (Access, Visio) Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com; Java 8 (бесплатное ПО) http://java.com/ru/; Oracle VM Virtual Box (бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox; SMath Studio (бесплатное ПО) Lazarus (бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus; DB Designer Fork; Ramus Educational 1.1.1, Start UML (бесплатное ПО) Cisco Packet Tracer 7.0 (бесплатное ПО) http://www.packettracernetwork.com/

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«Виртуальные частные сети»

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
- Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-27);

В результате освоения дисциплины студент должен:

Знать

основные компоненты, формирующие VPN; политики информационной безопасности автоматизированных систем.

Уметь

осуществлять выбор подходящей VPN; реализовывать частные политики информационной безопасности виртуальных частных сетей.

Владеть

приемами и методами выбора архитектуры VPN; технологиями реализации политик безопасности и управленческого трафика.

Содержание разделов дисциплины:

Компоненты, формирующие VPN. Развитие VPN. Необходимость VPN. Потребности бизнеса в VPN. Сетевая безопасность в VPN. Требования безопасности.

Полезные свойства VPN. Экономический эффект проектирования сетей. Преимущества для провайдеров. Конкурентоспособность. Стоимость технологии VPN. Гарантии качества обслуживания.

Выбор подходящей VPN. VPN на основе брандмауэра. VPN на основе черного ящика. VPN на основе маршрутизатора. VPN на основе удаленного доступа. VPN на основе набора прокси.

VPN с мультисервисными приложениями. VPN на основе программного обеспечения. Коммутация туннелей для VPN. Сравнение производительности.

Введение в топологию. Топология соединения брандмауэра/VPN и клиента. Топология VPN для соединения между ЛВС. Топология соединения VPN/брандмауэр и интранет/экстранет.

Топология VPN на основе ATM. Топология аппаратной VPN. Топология VPN/NAT. Топология коммутатора VPN. Вложенные туннели.

Размещение архитектуры VPN. Проблемы маршрутизации, адресации IP/NAT и удаленного доступа. Вопросы DNS/SMTP

Получение и присвоение IP-адресов. Реализация политики безопасности, управленческого трафика, SMTP и DNS.

Услуги VPN поставщиков услуг. Услуги автономных VPN.

Избыточные линии. Обновление ПО. Техническая поддержка на месте. Телефонная поддержка. Система поддержки удаленных пользователей. Мониторинг. Сигнализация.

Ведение журналов. Корреляция событий. Шифрование и инкапсуляция. Управление ключами. Генераторы случайных чисел. Сертификаты. Качество обслуживания.

Криптография. Шифрование. Безопасная коммуникация и аутентификация.