УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
«03» июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.В.ОД.6 Основы построения защищенных компьютерных сетей»
индекс по учебному плану, наименование

для подготовки **специалистов**
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2022
Курс 5
Семестр 10

В рабочую программу 2022г вносятся изменения:

1) Таблицу 7.2 читать в следующей редакции:

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.ru/

2) Пункт 9 читать в следующей редакции:

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес места нахождения помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы
Лаборатория «Автоматизированных систем в защищенном исполнении» №6041 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1.Учебный лабораторный стенд "Системы видеонаблюдения" – 1 шт. 2.Учебный лабораторный стенд "Видеонаблюдение в ip-сетях" – 1 шт. 3.Учебный лабораторный стенд "Промышленная автоматизация" (ст.1) – 1 шт. 4.Учебный лабораторный стенд "Промышленная автоматизация"(ст.2) – 1 шт.	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

5.Учебный лабораторный стенд "Удаленная настройка ИС" – 1 шт. 6.Учебный лабораторный стенд "Беспроводные компьютерные сети в АСУ" – 1 шт. 7. Посадочных мест - 13. Для ивалидов и лиц с ОВЗ: переносной радиокласс, клавиатура адаптированная **Программное обеспечение:** Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. Splunk 8. Zeek Network Security Monitor 9. Security Onion 10. OpenVPN 11. IP scanner 12. Nemesis 13. Eyercap	
Мультимедийная аудитория №6421 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 30 7. Рабочее место для преподавателя – 1 шт. **Программное обеспечение:** 1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

Программа актуализирована для 2022 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)

«_15_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС протокол № _9___ от «_15_» ___05___2024_г.

И.о. заведующий кафедрой _____Ляхманов Д.А.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____«03» июня 2024 г.

Методический отдел УМУ:_____ «03» июня 2024 г.

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
"_22_" __04___2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.6 Основы построения защищенных компьютерных сетей
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная
Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 108/3
часов/з.е
Промежуточная аттестация Зачет

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки «Информационная безопасность автоматизированных систем», утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 г. № 1457 на основании учебного плана, принятого УМС НГТУ

протокол от 20.04.2022г № 18.

Рабочая программа одобрена на заседании кафедры протокол от _21.04.2023___№ 4
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от __21.04.2023___№ 4

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-51__
Начальник МО _____ Н.Р. Булгакова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является освоение дисциплинарных компетенций в области защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Основы построения защищенных компьютерных сетей» способствует подготовке студентов к решению следующих профессиональных задач:

1. Освоение программных и аппаратных технологий защиты сетей;
2. Изучение методов проектирования, развертывания и сопровождения информационных сетей;
3. Изучение методов обследования и анализа защищенных вычислительных сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Основы построения защищенных компьютерных сетей» Б1.В.ОД.6 включена в перечень вариативной части дисциплин (формируемой участниками образовательных отношений), направленный на углубление уровня освоения компетенций. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина базируется на дисциплинах блока защиты информации и блока информационные технологии «Основы информационной безопасности», «Сети и системы передачи информации».

Дисциплина «Основы построения защищенных компьютерных сетей» является основополагающей для практик: практика по получению профессиональных умений и опыта профессиональной деятельности, преддипломная практика.

.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)[1]

Дисциплина «Основы построения защищенных компьютерных сетей» формирует компетенции ПК-2, ПК-3 совместно с дисциплинами и практиками, указанными в таблице 3.1

Дисциплинарная часть компетенции ПК-2 «Способен проводить разработку и анализ объектов информационной безопасности»: способен понимать и применять на практике методы и средства обеспечения защиты данных в информационных сетей

Дисциплинарная часть компетенции ПК-3 «Способен администрировать и проводить аудит автоматизированных систем»: способен понимать и применять на практике методы и средства анализа защищённости информационных сетей

Таблица 3.1 - Формирование компетенций дисциплинами

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ПК-2 (Способен проводить разработку и анализ объектов информационной безопасности)											
Анализ вредоносного программного обеспечения											
Защищенное администрирование информационных систем											
Комплексная защита информации											
Интеллектуальный анализ данных											
Разработка и эксплуатация автоматизированных систем в защищенном исполнении											
Основы построения защищенных компьютерных сетей											
Шаблоны проектирования программного обеспечения											
Методы проектирования программного обеспечения											
Проектно-технологическая практика											
Практика по получению опыта контрольно-аналитической деятельности											
Эксплуатационная практика											
Практика по получению умений и опыта профессиональной деятельности											
Преддипломная практика											
Подготовка и защита ВКР											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ПК-3 (Способен администрировать и проводить аудит автоматизированных систем)											
Защищенное администрирование информационных систем											
Разработка и эксплуатация автоматизированных систем в защищенном исполнении											
Основы построения защищенных компьютерных сетей											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
Организация ЭВМ и вычислительных систем											
Аппаратные средства вычислительной техники											
Администрирование UNIX-подобных систем											
Практика по получению опыта контрольно-аналитической деятельности											
Эксплуатационная практика											
Преддипломная практика											
Подготовка и защита ВКР											

Таблица 3.2 - Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ПК-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПК-2.1. Разрабатывает защищенные открытые информационные системы ИПК-2.2. Выполняет анализ защищенности информационных систем	***Знать:*** - основные понятия информационной безопасности в компьютерных сетях (ИПК-2.1, 2.2) - технологии обеспечения безопасности в локальных сетях (ИПК-2.1, 2.2) - основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля (ИПК-2.1, 2.2) - типовые угрозы сетевой безопасности (ИПК-2.1, 2.2) - основные критерии анализа сетевой безопасности (ИПК-2.2) - принципы построения защищенных телекоммуникационных систем (ИПК-2.1, 2.2)	***Уметь:*** - выполнять процедуры анализа сетевой безопасности (ИПК-2.2) - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях (ИПК-2.1, 2.2) - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты (ИПК2.1, 2.2)	***Владеть:*** - методами обеспечения безопасности телекоммуникационных связей и административный контроль (ИПК-2.1, 2.2) - средствами повышения надежности и безопасности функционирования сетей (ИПК-2.1, 2.2) - методами анализа результатов работы средств обнаружения вторжений (ИПК-2.2)	Набор индивидуальных заданий (лабораторных работ)	Вопросы для устного собеседования

ПК-3. Способен администрировать и проводить аудит автоматизированных систем	ИПК-3.3. Выполняет техническое обслуживание и сопровождение аппаратного обеспечения и сетевого оборудования открытых информационных систем	***Знать:*** – основные понятия информационной безопасности в компьютерных сетях – принципы построения защищенных телекоммуникационных систем	***Уметь:*** – выполнять процедуры анализа сетевой надежности и безопасности – применять криптографические протоколы и межсетевые экраны для защиты информации в сетях	***Владеть:*** – средствами повышения надежности и безопасности функционирования сетей – средства анализа конфигураций информационных сетей	Набор индивидуальных заданий (лабораторных работ)	Вопросы для устного собеседования

Освоение дисциплины причастно к ТФ С/02.7 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу разработки требований по защите информации в компьютерных сетях.

Освоение дисциплины причастно к ТФ С/03.7 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу анализа информационной безопасности в компьютерных сетях.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. ед. 108 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		10 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**55**	**55**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**53**	**53**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	49	49
Подготовка к зачёту	4	4

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.1 - Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Основные понятия информационной безопасности в компьютерных сетях										
ПК-2 - ИПК-2.1 ПК-2 - ИПК-2.2 ПК-3 - ИПК-3.3	**Тема 1.1** Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология.	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 1.2 Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Итого по 1 разделу	**4**				**4**				
Раздел 2. Технологии обеспечения безопасности в локальных сетях)										
ПК-2 - ИПК-2.1 ПК-2 - ИПК-2.2 ПК-3 - ИПК-3.3	**Тема 2.1** Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование.	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 2.2 Защита сетевого трафика и компонентов сети. Защита	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа									
	Тема 2.3 Средства повышения надежности функционирования сетей. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 2.4 Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: “ Cisco Packet Tracer ”		2			4	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: “ Cisco Packet Tracer		2			4	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Cisco Packet Tracer – Виртуальные локальные сети ”									
	Итого по 2 разделу	**8**	**4**	**8**		**16**				
Раздел 3. Обеспечение безопасности сетей на базе сетевых операционных систем.										
ПК-2 - ИПК-2.1 ПК-2 - ИПК-2.2 ПК-3 - ИПК-3.3	**Тема 3.1** Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля	4				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 3.2. Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа	4	2			2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема лабораторной работы: Установка программного обеспечения через домен		2			4	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: Обновление программного обеспечения и операционной системы		2			4	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Итого по 3 разделу	**8**	**6**		**1**	**12**				
Раздел 4. Обеспечение безопасности межсетевого взаимодействия										
ПК-2 - ИПК-2.1	**Тема 4.1.**	4			**1**	**2**	Подготовка к лекциям			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
ПК-2 - ИПК-2.2 ПК-3 - ИПК-3.3	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет						[6.1.1, 6.1.2, 6.1.3]			
	Тема 4.2. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети.	4				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 4.3. Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	2				**4**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: Одноранговые сети		2			**4**	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3, 6.1.4]			
	Тема лабораторной работы: Настройка домена.		2			**4**	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Групповые политики									
	Тема лабораторной работы: Высокоуровневые службы		3			**4**	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Итого по 4 разделу	**10**	**7**	**3**	**1**	**16**				
Раздел 5. Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот										
ПК-2 - ИПК-2.1 ПК-2 - ИПК-2.2 ПК-3 - ИПК-3.3	**Тема 5.1.** Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.	2			**1**	**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 5.2. Классы сканеров безопасности и особенности применения. Защита от вирусов. Защита электронного документооборота	2				**3**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 5 разделу	**4**			**1**	**5**				
	Подготовка к зачёту					**8**				
	Итого за семестр	**34**	**17**		**4**	**53**				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Перечень вопросов, выносимых на промежуточную аттестацию (зачет).

1. Обеспечение безопасности телекоммуникационных связей и административный контроль.
2. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак.
3. Влияние человеческого фактора на сетевую безопасность.
4. Защита топологии сети. Виртуальные локальные сети.
5. Функции коммутаторов. Персональные экраны. Абонентское шифрование.
6. Защита сетевого трафика и компонентов сети.
7. Защита компонентов сети от НСД. Безопасность ресурсов сети.
8. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
9. Средства повышения надежности функционирования сетей.
10. Защита от сбоев электропитания, аппаратного и программного обеспечения.

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информационная безопасность вычислительных систем и сетей».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При промежуточном контроле успеваемость студентов оценивается по системе «зачтено», «не зачтено».

Таблица 5.4 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо» /** «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично» /** «зачтено» 90-100% от max рейтинговой оценки контроля
ПК-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПК-2.1. Разрабатывает защищенные открытые информационные системы ИПК-2.2. Выполняет анализ защищенности информационных систем	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы защиты информации в информационных сетях; не во всех случаях правильно оперирует основными понятиями по защите информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов по принципам защиты информации в информационных сетях ; не во всех случаях выполняет корректное сравнение систем обеспечения безопасности данных	Знает материал на достаточно хорошем уровне; представляет основные принципы защиты информации в информационных сетях; подтверждает теоретические знания отдельными практическими примерами по защите информации; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по принципы защиты информации в информационных сетях ; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов по защите информации
ПК-3. Способен администрировать и проводить аудит автоматизированных систем	ИПК-3.3. Выполняет техническое обслуживание и сопровождение аппаратного обеспечения и сетевого оборудования открытых информационных систем	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы защиты информации в информационных сетях; не во всех случаях правильно оперирует основными понятиями по защите информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов по принципам защиты информации в информационных сетях ; не во всех случаях выполняет корректное сравнение систем обеспечения безопасности данных	Знает материал на достаточно хорошем уровне; представляет основные принципы защиты информации в информационных сетях; подтверждает теоретические знания отдельными практическими примерами по защите информации; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по принципы защиты информации в информационных сетях ; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов по защите информации

Таблица 5.5 - Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Ракитин, Р. Ю. Компьютерные сети : учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул : АлтГПУ, 2019. — 340 с. — ISBN 978-5-.88210-942-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139182

6.1.2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.3. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657

6.3 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению лабораторных работ по дисциплине «Основы построения защищенных компьютерных сетей» в электронном варианте находятся на кафедре «Информатика и системы управления». Электронные варианты методических указаний по выполнению лабораторных работ отправляются на электронные адреса групп.

6.3.1. Основы построения защищенных компьютерных сетей [Электронные текстовые данные]: метод. указания к лаб. работе по дисциплине «Основы построения защищенных компьютерных сетей» для студентов направления подготовки специалиста 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: Д.А. Ляхманов. Н.Новгород,.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД

и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 - Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	«Консультант студента - Электронная библиотека технического вуза»	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	«Юрайт» (коллекция «Легендарные книги»)	https://urait.ru/
4	«Техэксперт» - «Нормы, правила, стандарты и законодательство России»	https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resursy/tehekspert.pdf

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1. Windows 7 32 bit корпоративная; VL 49477S2 2.Microsoft Office Professional Plus 2007 (лицензия № 42470655); 3. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 4. Microsoft Windows 7 MSDN (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14)	Свободно распространяемое программное обеспечение: Операционная система Ubuntu Linux 20, GNS3, Snort, Wareshark, OpenVPN, Libre Office, Splunk, Zeek Network Security Monitor, Security Onion, OpenVPN, IP scanner, Nemesis, Eyercap, Apache OpenOffice, Браузер Google Chrome, Браузер Mozilla Firefox, McAfee Security Scan, Adobe Acrobat

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4 – Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	2	3
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда»

специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/ovz/.

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	Учебная аудитория № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 74 7. Рабочее место для преподавателя – 1 шт.	1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)
2	Лаборатория «Автоматизированные системы в защищенном исполнении» - аудитория № 6041 учебно-лабораторного корпуса № 6 для проведения учебных занятий и практической подготовки обучающихся. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Учебный лабораторный стенд "Системы видеонаблюдения" – 1 шт. 2. Учебный лабораторный стенд "Видеонаблюдение в ip-сетях" – 1 шт. 3. Учебный лабораторный стенд "Промышленная автоматизация" (ст.1) – 1 шт. 4. Учебный лабораторный стенд "Промышленная автоматизация"(ст.2) – 1 шт. 5. Учебный лабораторный стенд "Удаленная настройка ИС" – 1 шт. 6. Учебный лабораторный стенд "Беспроводные компьютерные сети в АСУ" – 1 шт. 7. Рабочее место студента - 13.	Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. Splunk 8. Zeek Network Security Monitor 9. Security Onion 10. OpenVPN 11. IP scanner 12. Nemesis

			13. Eyercap
3	Помещение для самостоятельной работы обучающихся № 6545 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Рабочие места, оснащенные ПК на базеCore 2 Duo с мониторами – 5 шт. 2. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 3. Доска интерактивная ScreenMedia-M. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета. 4. Посадочных мест - 12, шесть оснащены ПК. 5. Принтер Xerox Phaser 3300 MFP	1. Microsoft Windows 7 MSDN реквизиты договора - подписка (подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18), 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Основы построения защищенных компьютерных сетей», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с учетом текущей успеваемости.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.4 Методические указания по освоению дисциплины на практических занятиях типа

Практические занятия не предусмотрены учебным планом

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Для текущего контроля знаний студентов по дисциплине проводится **комплексная оценка знаний,** включающая

- выполнение и защита лабораторных работ **для студентов очной формы обучения**;

Варианты заданий для лабораторных работ приведены в учебно-методическом пособии по проведению лабораторных работ.

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

Зачет для студентов очной формы обучения в 10 семестре

Типовые вопросы для промежуточной аттестации в форме зачета для студентов очной формы обучения

Вопросы, направленные на проверку компетенции ПК-2:

1. Обеспечение безопасности телекоммуникационных связей и административный контроль.
2. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак.
3. Влияние человеческого фактора на сетевую безопасность.
4. Защита топологии сети. Виртуальные локальные сети.
5. Функции коммутаторов. Персональные экраны. Абонентское шифрование.
6. Защита сетевого трафика и компонентов сети.
7. Защита компонентов сети от НСД. Безопасность ресурсов сети.
8. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
9. Средства повышения надежности функционирования сетей.
10. Защита от сбоев электропитания, аппаратного и программного обеспечения.
11. Контроль и распределение нагрузки на вычислительную сеть.
12. Регламентирующие документы в области безопасности вычислительных сетей.

Вопросы, направленные на проверку компетенции ПК-3:

13. Сетевые операционные системы Windows, Unix/Linux.
14. Критерии оценки безопасности сетевых ОС.
15. Основные критерии анализа сетевой безопасности. Общая процедура анализа.
16. Основные механизмы обеспечения безопасности и управления распределенными ресурсами.
17. Обеспечение надежности инфраструктуры Интернет.
18. Защита каналов связи в Интернет.
19. Виды используемых в Интернет каналов связи.
20. Уязвимости и защита базовых сетевых протоколов и служб
21. Безопасность WWW и электронной почты.
22. Системы обнаружения и противодействия вторжениям.
23. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.
24. Классы сканеров безопасности и особенности применения. Защита от вирусов.

25. Защита электронного документооборота.

В полном объеме оценочные средства имеются на кафедре «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.