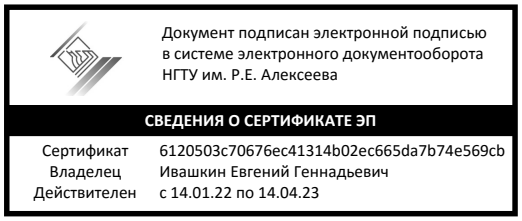
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

Институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)



УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“__10__”_____06_____2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.3.1 Безопасность сетевых протоколов
(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения: очная
Год начала подготовки 2020, 2021

Выпускающая кафедра ИСУ

Кафедра-разработчик ИСУ

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация Зачет с оценкой

Разработчик: Кобляков Д.А., старший преподаватель

Нижний Новгород

2021

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИ от 19 сентября 2017 года № 926 на основании учебного плана принятого УМС НГТУ

протокол от _10.06.21__ №___6 __

Рабочая программа одобрена на заседании кафедры протокол от _09.06.2021_ № __10____
Зав. кафедрой к.т.н, доцент Тимофеева О.П. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 10.06.2021_____№_1

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.03.02-б-50___

Начальник МО _____

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

1. Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения безопасности и целостности передаваемых данных в информационных системах.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Безопасность сетевых протоколов» способствует подготовке студентов к решению следующих профессиональных задач:

1. Проведение оценки соблюдения требований информационной безопасности в операционных системах.
2. Проектирование систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Безопасность сетевых протоколов» Б1.В.ДВ.3.1 включена в перечень вариативной части дисциплин (формируемой участниками образовательных отношений) по выбору (запросу студентов), направленный на углубление уровня освоения компетенций. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по данному направлению подготовки.

Дисциплина базируется на дисциплинах математического блока и блока программирования программы бакалавриата по направлению «Информационные системы и технологии». Предшествующими курсами, на которых непосредственно базируется дисциплина «Безопасность сетевых протоколов», являются:

- «Операционные системы»
- «Методы и средства защиты информации»

Дисциплина «Безопасность сетевых протоколов» является основополагающей для изучения следующих дисциплин: «Защита программного обеспечения», так же практики: по получению профессиональных умений и опыта профессиональной деятельности и выполнения выпускной квалификационной работы.

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

Дисциплина «Безопасность сетевых протоколов» формирует компетенции ПКС-2 и ПКС-3 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Дисциплинарная часть компетенции ПКС-2 «Способен проектировать и обеспечивать функционирование информационных систем»: способен оценивать безопасность передачи данных в современных операционных системах.

Дисциплинарная часть компетенции ПКС-3 «Способен обеспечивать безопасность и целостность данных информационных систем»: способен разрабатывать и применять на практике методы и алгоритмы защиты, обеспечивающие безопасность и целостность передаваемых данных информационных систем.

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»							
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
ПКС-2 (Способен проектировать и обеспечивать функционирование информационных систем)								
Электротехника и электроника								
Защита программного обеспечения								
Операционные системы								
Инструментальные средства информационных систем защиты информации								
Безопасность сетевых протоколов								
Защита информационных процессов в компьютерных системах и сетях								
Теория и методология информационной безопасности								
Безопасность информационных технологий								
Программирование сигнальных микропроцессоров фирмы Техас Инструментс								
Практика по получению профессиональных умений и опыта профессиональной деятельности								
Преддипломная практика								
Выполнение и защита ВКР								
ПКС-3: Способен обеспечивать безопасность и целостность данных информационных систем								
Основы криптографических методов								
Защита программного обеспечения								
Теоретико-числовые основы криптологии								
Безопасность сетевых протоколов								
Защита информационных								

процессов в компьютерных системах и сетях								
Теория и методология информационной безопасности								
Безопасность информационных технологий								
Техническая защита информации								
Интеллектуальные системы защиты информации								
Защита информации в сетях передачи данных								
Основы построения масштабируемых сетей передачи данных								
Практика по получению профессиональных умений и опыта профессиональной деятельности								
Преддипломная практика								
Выполнение 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
ПКС-2. Способен проектировать и обеспечивать функционирование информационных систем	ИПКС-2.2. Обеспечивает функционирование информационных систем	***Знать:*** – принципы функционирования основных защищенных сетевых протоколов	***Уметь:*** – проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности в конкретной ситуации	***Владеть:*** – средствами защиты информации для обеспечения заданных свойств информационной безопасности	Выполнение и сдача лабораторной работы	Вопросы для устного собеседования на зачете с оценкой - 20 вопросов
ПКС-3 Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.1. Способен обеспечивать защиту информации при передаче данных в информационных системах	***Знать:*** – методы и средства проектирования, реализации и оценки защищенных сетевых систем; – стандарты по оценке защищенных сетевых систем и их теоретические основы, – принципы защиты информации и обеспечения информационной безопасности, – об основных угрозах информационной безопасности и их источниках; – понятия конфиденциальной информации, персональных данных и государственной тайны.	***Уметь:*** – разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы; – реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем; – выбирать методы и средства построения систем защиты информации.	***Владеть:*** – навыками проектирования защищенных сетей; – навыками комплексного анализа и оценки сетевой безопасности	Выполнение и сдача лабораторных работ	Вопросы для устного собеседования на зачете с оценкой - 20 вопросов

Освоение дисциплины причастно к ТФ D/03.6 (ПС 06.001 «Программист»), решает задачу проектирования систем защиты информации.

Освоение дисциплины причастно к ТФ B/01.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу оценки соблюдения требований информационный безопасности в операционных системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. 144 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
		6 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**38**	**38**
1.1 Аудиторная работа, в том числе:	**34**	**34**
занятия лекционного типа (Л)	17	17
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)	**106**	**106**
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.)	79	79
Подготовка к зачёту с оценкой	27	27

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.2-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					
6 семестр										
Раздел 1. Основы вычислительных сетей										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.1	**Тема 1.1.** Сетевая архитектура	1				1	Подготовка к лекциям [6.1.1]			
	Тема 1.2. Основы организации и функционирования сетей	1				2	Подготовка к лекциям [6.1.1]			
	Итого по 1 разделу	**2**				**3**				
Раздел 2. Технологии обеспечения безопасности в сетях										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.1	**Тема 2.1.** Типовые угрозы сетевой безопасности	1				2	Подготовка к лекциям [6.1.1 – 6.1.2]	Разбор конкретных ситуаций		
	Тема 2.2. Защита топологии сети	1				2	Подготовка к лекциям [6.1.1 – 6.1.2]	Разбор конкретных ситуаций		
	Тема 2.3. Защита сетевого трафика и компонентов сети	1				2	Подготовка к лекциям [6.1.1 – 6.1.2]	Разбор конкретных ситуаций		
	Тема 2.4. Средства повышения надежности функционирования сетей	1				2	Подготовка к лекциям [6.1.1 – 6.1.2]	Разбор конкретных ситуаций		
	Тема 2.5. Регламентирующие документы в области безопасности вычислительных сетей	1				2	Подготовка к лекциям [6.1.1 – 6.1.2]	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					
	Лабораторная работа №1. Протокол сетевой безопасности IPSec		6			10	Подготовка к лабораторной работе. [6.1.1 – 6.1.3, 6.1.6]	Мозговой штурм	6	
	Итого по 2 разделу	**5**	**6**		**1**	**20**				
Раздел 3. Построение защищенных сетей на базе сетевых операционных систем										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.1	**Тема 3.1.** Сетевые операционные системы (ОС) NetWare, Windows, UNIX	1				2	Подготовка к лекциям [6.1.2, 6.1.4, 6.1.5]	Разбор конкретных ситуаций		
	Тема 3.2. Политика безопасности	1				2	Подготовка к лекциям [6.1.2, 6.1.4, 6.1.5]	Разбор конкретных ситуаций		
	Тема 3.3. Критерии оценки безопасности сетевых ОС	1				2	Подготовка к лекциям [6.1.2, 6.1.4, 6.1.5]	Разбор конкретных ситуаций		
	Лабораторная работа №2. Групповые политики Microsoft Windows		4			10	Подготовка к лабораторной работе. [6.1.2 – 6.1.5, 6.1.6]	Мозговой штурм	4	
	Итого по 3 разделу	**3**	**4**		**1**	**16**				
Раздел 4. Глобальная сеть Интернет										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.1	**Тема 4.1.** Стандарты и протоколы Интернет	1				2	Подготовка к лекциям [6.1.2, 6.1.5]			
	Тема 4.2. Функционирование, разработка и сопровождение приложений для Интернет	1				2	Подготовка к лекциям [6.1.3 - 6.1.5]			
	Лабораторная работа №3. Безопасность сетей на		3			10	Подготовка к лабораторной работе. [6.1.3 – 6.1.6, 6.1.6]	Мозговой штурм	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					
	прикладном уровне. Использование Центра Сертификации Microsoft Windows									
	Итого по 4 разделу	**2**	**3**		**1**	**14**				
Раздел 5. Безопасности сети Интернет										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.1	**Тема 5.1.** Защита каналов связи в Интернет	1				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 5.2. Уязвимости и защита базовых протоколов и служб	1				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 5.3. Защита электронного документооборота	1				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 5.4. Защита рабочего места пользователя сети Интернет	1				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 5.5. Комплексная защита подключения к Интернет	1				2	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Лабораторная работа №4. Разграничение доступа и управление сетевыми ресурсами сети Microsoft Windows		2			8	Подготовка к лабораторной работе. [6.1.2 – 6.1.5, 6.1.6]	Мозговой штурм	2	
	Лабораторная работа №5. Управление учетными записями пользователей,		2			8	Подготовка к лабораторной работе. [6.1.2 – 6.1.5, 6.1.6]	Мозговой штурм	2	

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					
	групп и сетевых ресурсов									
	Итого по 5 разделу	**5**	**4**		**1**	**26**				
	Подготовка к зачёту с оценкой					**27**				
	Итого за семестр	**17**	**17**	**-**	**4**	**106**			17	

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

1. Примерный перечень вопросов при защите лабораторных работ:

– в чем достоинства и недостатки дискреционной политики безопасности?
– в чем достоинства и недостатки мандатной политики безопасности?
– в чем заключается тождественность объектов и тождественность субъектов компьютерной системы?
– кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
– каковы возможные пути нарушения политики безопасности в компьютерной системе?
– какие факторы влияют на определение размеров доменов безопасности?
– какая информация хранится в реестре Windows?
– какие существуют способы аутентификации пользователей?
– в чем слабость парольной аутентификации?
– как может быть повышена надежность аутентификации с помощью паролей?
– какой может быть реакция системы на попытку подбора паролей?
– кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей?
– как должны храниться пароли в базе учетных записей пользователей?
– в чем смысл объединения пользователей в группы?
– какие события безопасности должны фиксироваться в журнале аудита?
– какие параметры определяют политику аудита?
– целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
– целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
– как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
– нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

2. Примерный перечень вопросов для зачета с оценкой:

– Постановка задачи распределенной обработки данных.
– Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей
– Основные сетевые стандарты и протоколы.
– Сетевые операционные системы.
– Средства взаимодействия процессов в сетях.
– Распределенная обработка информации в системах клиент-сервер, одноранговые сети, локальные и глобальные сети.
– Неоднородные вычислительные сети
– Основы классификации сетевых угроз и атак.
– Примеры типовых атак и рекомендации по построению систем защиты.
– Влияние человеческого фактора на сетевую безопасность
– Маршрутизаторы, межсетевые экраны (МЭ).

- Основные механизмы применения МЭ.
- Абонентское шифрование.
- Виртуальные частные сети.
- Защита компонентов сети от НСД.
- Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
- Электронная цифровая подпись и пакетное шифрование.
- Криптографические сетевые протоколы.

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информатика и системы управления».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется **традиционная** система, при которой успеваемость студентов оценивается по четырех балльной шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.1–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
ПКС-2. Способен проектировать и обеспечивать функционирование информационных систем	ИПКС-2.2. Обеспечивает функционирование информационных систем	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы безопасности и целостности информации; не во всех случаях правильно оперирует основными понятиями информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы безопасности и целостности информации; не во всех случаях находит правильные ответы на задаваемые вопросы	Знает материал на достаточно хорошем уровне; представляет основные концепции безопасности и целостности информации; подтверждает теоретические знания отдельными практическими примерами по защите данных в информационных системах; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала безопасности и целостности информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов по защите информации
ПКС-3. Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.1. Способен обеспечивать защиту информации при передаче данных в информационных системах.	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы безопасности и целостности информации; не во всех случаях правильно оперирует основными понятиями информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы безопасности и целостности информации; не во всех случаях находит правильные ответы на задаваемые вопросы	Знает материал на достаточно хорошем уровне; представляет основные концепции безопасности и целостности информации; подтверждает теоретические знания отдельными практическими примерами по защите данных в информационных системах; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала безопасности и целостности информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов по защите информации

Таблица 5.2 - Критерии оценивания

Оценка	Критерии оценивания
Высокиий 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. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7338-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/158939

6.1.2. Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118219

6.1.3. Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600

6.2 Справочно-библиографическая литература

6.1.4. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

6.1.5. Староверова, Н. А. Операционные системы : учебник для спо / Н. А. Староверова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 412 с. — ISBN 978-5-8114-8984-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/186048

6.3 Перечень журналов по профилю дисциплины:

Использование журналов не предусмотрено при изучении дисциплины.

6.4 Методические указания, рекомендации и другие материалы к занятиям

6.1.6 Метод. указания для лабораторных работ по дисциплине «Безопасность сетевых протоколов», для студентов направления подготовки 09.03.02 «Информационные системы и технологии» дневной формы обучения / НГТУ; Сост.: Д.А. Кобляков, Н.Новгород, 2021

Электронные варианты всех методических указаний отправляются на электронные адреса групп.

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	Лань	https://e.lanbook.com/
2	Юрайт	https://biblio-online.ru/

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
-	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html)
	Linux (https://www.linux.com/)
	OpenOffice (FreeWare) https://www.openoffice.org/ru/
	JDK 8 и выше (https://adoptopenjdk.net/)
	Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework)
	Eclipse (https://www.eclipse.org/) Intellij Idea (https://www.jetbrains.com/ru-ru/idea/)
	git (https://git-scm.com/), github (https://github.com/)
	Maven (https://maven.apache.org/), Gradle (https://gradle.org/)
	Редактор блок-схем (https://app.diagrams.net/)
	Анализатор сетевого трафика Wireshark (https://www.wireshark.org/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.4 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 инфор-	https://cyberpedia.su/21x47c0.html

	мационных справочных систем	
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/accenv/

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:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы бакалавриата для студентов очного обучения, включает в себя компьютерные классы

1. ***Ауд. 4408 кафедры «Информатика и системы управления» - лаборатория Информационных технологий.***

Компьютеры, оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов.

- 8 рабочих мест на базе тонких клиентов DellWise,
- мультимедийный проектор BenQ PB6240,
- ноутбук Lenovo V130-151KB,
- стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.

Пакеты ПО (лицензионное):

- Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021).

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Linux Ubuntu 20.04 (https://releases.ubuntu.com/20.04/)
- git (https://git-scm.com/)

– Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/)

Также, для 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	Оснащенностьаудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	**6421** учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 12	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе AMD Athlon 2.8Ггц, 4 Гб ОЗУ, 250 ГБ HDD, монитор 19” – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• Microsoft Windows7 (подписка DreamSpark Premium, договор №Tr113003 от 25.09.14) • Gimp 2.8 (свободное ПО, лицензия GNU GPLv3); • Microsoft Office Professional Plus 2007 (лицензия № 42470655); • OpenOffice 4.1.1 (свободное ПО, лицензия ApacheLicense 2.0) • AdobeAcrobatReader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNU LGPL); Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021).
	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	• Проектор Accer – 1шт; • ПК на базе IntelCoreDuo 2.93 ГГц, 2 Гб ОЗУ, 320 Гб HDD, монитор Samsung 19` – 11 шт.. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14); • Microsoft Office (лицензия № 43178972); • Adobe Design Premium CS 5.5.5 (лицензия № 65112135); • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNULGPL); • Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021) • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018); Gimp 2.8 (свободное ПО, лицензия GNUGPLv3)

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 «Безопасность сетевых протоколов», используются совре-

менные 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 оценкой с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с заданиями, вопросами, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент последовательно, четко и логически излагает учебный материал; справляется с заданиями, вопросами, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже трех по оценочной системе, что соответствует допороговому уровню.

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 практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3Методические 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

Практические занятия по дисциплине не предусмотрены

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 контроля текущей успеваемости

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

11.1.1. Типовые задания для лабораторных работ

Типовые задания для лабораторных работ приведены в учебно-методических указаниях 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

11.2.1. Защита курсового проекта/ работы

Курсовая работа не предусмотрена учебным планом

11.2.2. Зачет с оценкой для студентов очной формы обучения в 6 семестре.

Проводится в виде устного собеседования по типовым вопросам.

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

1. Постановка задачи распределенной обработки данных.
2. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей
3. Основные сетевые стандарты и протоколы.
4. Сетевые операционные системы.
5. Средства взаимодействия процессов в сетях.
6. Распределенная обработка информации в системах клиент-сервер, одноранговые сети, локальные и глобальные сети.
7. Неоднородные вычислительные сети
8. Основы классификации сетевых угроз и атак.
9. Примеры типовых атак и рекомендации по построению систем защиты.
10. Влияние человеческого фактора на сетевую безопасность
11. Маршрутизаторы, межсетевые экраны (МЭ).
12. Основные механизмы применения МЭ.
13. Абонентское шифрование.
14. Виртуальные частные сети.
15. Защита компонентов сети от НСД.
16. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
17. Электронная цифровая подпись и пакетное шифрование.
18. Криптографические сетевые протоколы.
19. Управление ключами.
20. Защита от сбоев электропитания, аппаратного и программного обеспечения.
21. Контроль и распределение нагрузки на вычислительную сеть.
22. Организация сетей на базе операционных систем NetWare.
23. Организация вычислительных сетей на базе операционных систем Windows.

24. Организация вычислительных сетей на базе операционных систем Unix: основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.
25. Понятие политики безопасности. Типовые элементы политики безопасности.
26. Рекомендации по построению политики безопасности.
27. Основные шаги по реализации политики безопасности.
28. Поддержание и модификация политики безопасности.
29. Основные критерии анализа сетевой безопасности. Общая процедура анализа.
30. Методика подготовки экспертного заключения.
31. Основные механизмы обеспечения безопасности и управления распределенными ресурсами.
32. Обеспечение надежности инфраструктуры Интернет
33. Виды используемых в Интернет каналов связи.
34. Особенности их защиты.
35. Использование межсетевых экранов.
36. Виртуальные частные сети.
37. Защита программного окружения рабочей станции.
38. Защита персональных данных.
39. Защита от вирусов.
40. Протоколы маршрутизации. Семейство TCP/IP.
41. Службы поиска.
42. Безопасность WWW и электронной почты.
43. Безопасность Java.
44. Основные понятия электронного документооборота
45. Стандарты и протоколы защищенного документооборота

В полном объеме оценочные средства имеются на кафедре «Информатика и системы управления». Оценочные средства могут быть получены по требованию.

УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
“____”_____2021 г.

Лист актуализации рабочей программы дисциплины
«Б1.В.ДВ.3.1 Безопаєность сетевых протоколов»
индекс по учебному плану, наименование

для подготовки **бакалавров**/ специалистов/ магистров
Направление: 09.03.02 Информационные системы и технологии
Направленность: Безопасность информационных систем
Форма обучения очная
Год начала подготовки:2021

Курс 3
Семестр 6
В рабочую программу не вносятся изменения. Программа актуализирована для 2021 г. начала подготовки.

Разработчик (и): __Кобляков Д.А., старший преподаватель_____
(ФИО, ученая степень, ученое звание)
«__»_____20_г.
Рабочая программа пересмотрена и одобрена на заседании кафедры ИСУ
_____ протокол № _____ от «__» _____20__г.

Заведующий кафедрой ИСУ _____Тимофеева О.П.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИСУ _____«__» _____ 20__г.

Методический отдел УМУ:_____«__» _____ 20__ г.