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.ОД.7 Защита программного обеспечения
(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 180/5
часов/з.е
Промежуточная аттестация Экзамен

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-40___

Начальник МО _____

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

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения безопасности и целостности информации, основанное на методах защиты программного обеспечения.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Защита программного обеспечения» способствует подготовке студентов к решению следующих профессиональных задач:

1. Проведение оценки соблюдения требований по защите информации в операционных системах.
2. Обоснование решений в области использования конкретных средств защиты программного обеспечения.

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Защита программного обеспечения» Б1.В.ОД.7 включена в обязательный перечень дисциплин вариативной части (формируемой участниками образовательных отношений), определяющий направленность образовательной программы. 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 «Защита программного обеспечения», являются:

- «Операционные системы»
- «Основы криптографических методов»
- «Объектно-ориентированное программирование»

Дисциплина «Защита программного обеспечения» является основополагающей для преддипломной практики и выполнения выпускной квалификационной работы.

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

Дисциплина «Защита программного обеспечения» 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 эффективность защиты программного обеспечения 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 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:*** – основные принципы организации и алгоритмы функционирования подсистем безопасности в современных операционных системах и оболочках; – принципы разработки защищенного программного обеспечения.	***Уметь:*** – обеспечивать заданные требования к безопасности программного обеспечения, оценивать эффективность защиты.		Выполнение и сдача 1 лабораторной работы	
ПКС-3 Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.2. Обеспечивает защиту и целостность данных в информационных системах	***Знать:*** – исторические шифры, основные алгоритмы симметричного шифрования, функции хэширования, протоколы цифровой подписи, базовые протоколы проверки подлинности и обмена ключами, – основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности	***Уметь:*** – обосновывать решения в области использовании конкретных криптографических протоколов при проектировании современные защищенных программных комплексов, – проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов – на основе международного опыта квалифицированно анализировать информационные риски	***Владеть:*** – современными международными стандартами в области криптографических алгоритмов и протоколов криптографической защиты информации	Выполнение и сдача 2х лабораторных работ	Экзамен – 20 билетов

			в области криптографических протоколов,			

Освоение дисциплины причастно к ТФ B/03.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу оценки соблюдения требований по защите информации в операционных системах.

Освоение дисциплины причастно к ТФ B/01.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу применения конкретных средств защиты программного обеспечения.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 5 зач.ед. 180 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
		8 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**180**	**180**
1. Контактная работа:	**76**	**76**
1.1 Аудиторная работа, в том числе:	**70**	**70**
занятия лекционного типа (Л)	30	30
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	-	-
лабораторные работы (ЛР)	40	40
1.2 Внеаудиторная, в том числе	**6**	**6**
курсовая работа (проект) (КР/КП) (консультация, защита)	-	-
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**77**	**77**
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.)	77	77
Подготовка к экзамену (контроль)	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					
8 семестр										
Раздел 1. Проблемы безопасности операционных систем										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.2	**Тема 1.1.** Основные понятия информационной безопасности. Защитные механизмы операционных систем	1					Подготовка к лекциям [6.1.3,6.1.4]			
	Тема 1.2. Модель безопасности операционной системы Windows	2					Подготовка к лекциям [6.1.2, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Тема 1.3. Уязвимости современных методов защиты ПО	2				5	Подготовка к лекциям [6.1.2, 6.1.3, 6.1.4]	Разбор конкретных ситуаций		
	Итого по 1 разделу	**5**			**1**	**5**				
Раздел 2. Исследование защищенности программных систем										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.2	**Тема 2.1.** Критерии защищенности	1				2	Подготовка к лекциям [6.1.2 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.2. Оценка эффективности систем защиты программного обеспечения	4				4	Подготовка к лекциям [6.1.2 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 2.3. Обзор промышленных средств защиты программного обеспечения	2				8	Подготовка к лекциям [6.1.1 – 6.1.4]	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. Отладка программ с помощью GDB		10			10	Подготовка к лабораторной работе. [6.1.1 – 6.1.4, 6.1.7]	Мозговой штурм	10	
	Итого по 2 разделу	**7**	**10**		**1**	**24**				
Раздел 3. Методы защиты программного обеспечения										
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.2	**Тема 3.1.** Протоколы аутентификации	**2**				**2**	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.2. Защита от программных закладок	**2**				**2**	Подготовка к лекциям [6.1.1 – 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.3. Защита при помощи электронных ключей	**2**				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 3.4. Обеспечение целостности и достоверности программного кода	**2**				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 3.5. Защита от несанкционированного копирования	**2**				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Тема 3.6. Противодействие «взлому» программного обеспечения	**2**				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.4]	Разбор конкретных ситуаций		
	Лабораторная работа №2. Защита при помощи электронных ключей		**20**			**20**	Подготовка к лабораторной работе. [6.1.1 – 6.1.4, 6.1.7]	Мозговой штурм	20	
	Итого по 3 разделу	**12**	**20**		**1**	**32**				
Раздел 4. Применение криптографических методов защиты										

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					
ПКС-2 - ИПКС-2.2 ПКС-3 - ИПКС-3.2	**Тема 4.1.** Стандарты систем шифрования	**2**				**2**	Подготовка к лекциям [6.1.5, 6.1.6]			
	Тема 4.2. Аутентичность информации	**2**				**2**	Подготовка к лекциям [6.1.3 - 6.1.6]			
	Тема 4.3. Криптографические протоколы	**2**				**2**	Подготовка к лекциям [6.1.3 - 6.1.6]			
	Лабораторная работа №3. Изучение криптографических протоколов		**10**			**10**	Подготовка к лабораторной работе. [6.1.3 – 6.1.6, 6.1.7]	Мозговой штурм	10	
	Итого по 4 разделу	**6**	**10**		**1**	**16**				
	Подготовка к экзамену (контроль)				**2**	**27**				
	Итого за семестр	**30**	**40**	**-**	**6**	**77**			40	

4. 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:

– Что такое отладка программного обеспечения?
– В каком режиме работает отладчик GDB?
– Какие параметры командной строки использует GDB?
– Каким образом должны быть подготовлены программы, чтобы их можно было исследовать с помощью GDB?
– Как влияет уровень детализации отладочной информации на размер исполняемого файла?
– Можно ли выделить отладочную информацию в отдельный файл? Если да, то каким образом?
– Что такое «точка останова»? Сколько точек останова можно задать в процессе отладки программы? Можно ли задать условие срабатывания точки останова?
– Какую информацию можно получить в процессе отладки программы?
– Рассказать об утилите HASP Envelope
– Рассказать об утилите тестирования HASP
– Рассказать об утилите HASPEdit
– Что такой идентификатор HASP
– Как шифруются и дешифруются данные для распознавания ключа HASP
– Дать определение протокола.
– Перечислить задачи защиты информации, в которых используются криптографические протоколы.
– Способы классификации криптографических протоколов.
– Классификация криптографических протоколов по функциональному назначению.
– Назначение протокола аутентификации сообщений.
– Назначение протокола идентификации.
– Назначение протокола обмена секретами.
– Перечислить основные виды атак на протоколы.

2. Примерный перечень вопросов для экзамена:

– Симметричные криптосистемы.
– Алгоритм DES. Разновидности алгоритма DES и атаки на них.
– Алгоритм AES.
– Классификация угроз
– Асимметричные криптосистемы.
– Однонаправленные функции.
– Алгоритм RSA.
– Классы безопасности
– Аудит, учет использования системы защиты
– Анализ ОС Unix с точки зрения защищенности
– Алгоритмы RC4, RC5, RC6
– Упаковщики/шифраторы
– ЭЦП. Основные понятия и функциональность. Процедуры постановки и проверки подписи.
– Хэш-функция. Требования к хэш-функциям.

- Системы «привязки» ПО
- Методы защиты программ от исследования
- Управление ключами. Генерация ключей. Хранение ключей и распределение ключей.
- Идентификация, аутентификация, авторизация.

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-3.2. Обеспечивает защиту и целостность 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.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057

6.1.2. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

6.1.3. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

6.1.4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247

6.2 Справочно-библиографическая литература

6.1.5. 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

6.1.6. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-9346-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189446

6.3 Перечень журналов по профилю дисциплины:

Использование журналов не предусмотрено при изучении дисциплины.

6.4 Методические указания, рекомендации и другие материалы к занятиям

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

6. 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/)
	Отладчик GDB (https://www.sourceware.org/gdb/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.4указан 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

7. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице8.1 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

8. 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)

9. 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 «Защита программного обеспечения», 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 экзамена 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.

10. 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

10.1.1. 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. Экзамен для студентов очной формы обучения в 8 семестре.

Проводится в виде устного собеседования по типовым вопросам.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов очной формы обучения:

1. Основные понятия информационной безопасности
2. Классификация угроз
3. Классы безопасности.
4. Политика безопасности
5. Защитные механизмы операционных систем.
6. Идентификация и аутентификация
7. Авторизация. Разграничение доступа к объектам ОС
8. Аудит, учет использования системы защиты
9. Анализ ОС Unix с точки зрения защищенности
10. Анализ ОС Windows NT/2000 с точки зрения защищенности
11. Системы защиты ПО: классификация, основные методы защиты.
12. Упаковщики/шифраторы.
13. Системы защиты от несанкционированного копирования
14. Парольные защиты
15. Системы «привязки» ПО.
16. Программно-аппаратные средства защиты
17. Средства защиты с «ключевыми дисками»
18. Средства исследования программ.
19. Методы защиты программ от исследования
20. Методы защиты программ от несанкционированных изменений
21. Методы противодействия динамическим способам снятия защиты программ от копирования
22. Программные закладки: методы защиты.
23. Социальная инженерия - методы противодействия

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.ОД.7 Защита программного обеспечения**»**
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 4
Семестр 8
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.