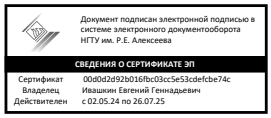
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

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



УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“_22___”_____04_____2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.4.1 Теория и методология информационной безопасности
(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 2025

Выпускающая кафедра ИСУ

Кафедра-разработчик ИСУ

Объем дисциплины 144/5
часов/з.е
Промежуточная аттестация Экзамен

Разработчик: Васильев Р.А., к.т.н., доцент

Нижний Новгород

2025

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 __12.12.24__ №___5__

Рабочая программа одобрена на заседании кафедры протокол от _30.03.2025_ № __9____
Зав. кафедрой к.т.н, доцент Тимофеева О.П. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от ____22.04.2025_____№__3__

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.03.02 – б-53
Начальник МО _____Е.Г. Севрюкова _

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 защиты и целостности данных в информационных системах.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Теория и методология информационной безопасности» способствует подготовке студентов к решению следующих профессиональных задач:

1. Исследование и анализ угроз безопасности информации и программного обеспечения.
2. Обеспечения защиты и целостности данных в информационных системах
3. Применение программно-аппаратных средств защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Теория и методология информационной безопасности» Б1.В.ДВ.4 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 блоказащиты информации программы бакалавриатапо направлению «Информационные системы и технологии». Предшествующими курсами, на которых непосредственно базируется дисциплина «Теория и методология информационной безопасности», являются:

- «Основы криптографических методов»,
- «Безопасность сетевых протоколов».

Дисциплина «Теория и методология информационной безопасности» является основополагающей для практики: преддипломная.

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

Дисциплина «Теория и методология информационной безопасности» формирует компетенцию 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 понимать и применять на практике методы, обеспечивающие информационную безопасность объектов.

Дисциплинарная часть компетенции ПКС-3 «Способен обеспечивать безопасность и целостность данных информационных систем»: способен понимать и применять на практике методы, 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-2.1 Проектирует информационные системы	***Знать:*** – принципы поиска и сравнения средств обеспечения информационной безопасности – технологии поиска и анализа решений –	***Уметь:*** – анализировать существующие решения – осуществлять корректное сравнение систем обеспечения безопасности данных	***Владеть:*** – средствами поиска и анализа решений в информационных сетях и литературных источниках	Выполнение сквозного индивидуального задания – реферата (кейс из 10 заданий)	Набор экзаменационных билетов
ПКС-3. Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.2 Обеспечивает защиту и целостность данных в информационных системах		***Уметь:*** – анализировать существующие решения – осуществлять корректное сравнение систем обеспечения безопасности данных	***Владеть:*** – средствами поиска и анализа решений в информационных сетях и литературных источниках	Выполнение сквозного индивидуального задания – реферата (кейс из 10 заданий)	Набор экзаменационных билетов

Освоение дисциплины причастно к ТФ B/03.6, B/01.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу исследования принципов анализа угроз безопасности информации и применения программно-аппаратных средств защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работпо семестрам

Общая трудоёмкость дисциплины составляет 5зач.ед. 144 часа, распределение часов по видам работ семестрам представлено в таблице 4.1.

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

Вид учебной работы	Трудоёмкость в час	
	Всего час.	В т.ч. по семестрам
		7 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**74**	**74**
1.1 Аудиторная работа, в том числе:	**68**	**68**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	34	34
лабораторные работы (ЛР)		
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)	**34**	**34**
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.)	34	34
Подготовка к экзамену(контроль)	**36**	**36**

4.2Содержание 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. Введение										
ПКС-2 - ИПКС-2.1 ПКС-3 - ИПКС-3.2	**Тема 1.1** История развития	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 1.2 Текущий уровень развития и тенденции	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 1 разделу	**4**				**4**				
Раздел 2. Законодательные и организационные аспекты										
ПКС-2 - ИПКС-2.1 ПКС-3 - ИПКС-3.2	**Тема 2.1** Законодательные акты РФ	2			1	2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 2.2 Свойства информационной безопасности	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 2.3 Каналы утечек и способы противодействия	2		6		2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3], подготовка к практике	Разбор конкретных ситуаций		
	Итого по 2 разделу	**6**		**6**	**1**	**6**				
Раздел 3. Защита информационных сетей										
ПКС-2 - ИПКС-2.1 ПКС-3 - ИПКС-3.2	**Тема 3.1**Типы атак и принципы их организации	2			1	2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 3.2.Уязвимости современных сетей и протоколов	2		16		2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3], подготовка к практике			
	Тема 3.3.Средства обеспечения безопасности передачи данных	2				2	Подготовка к лекциям [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					
	Тема 3.4.Построение защищенных сетей	2				2				
	Итого по 3 разделу	**8**		**16**	**1**	**8**				
Раздел 4. Основы компьютерной вирусологии										
ПКС-2 - ИПКС-2.1 ПКС-3 - ИПКС-3.2	**Тема 4.1.** Типы вредоносного программного обеспечения	2			**1**	**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 4.2. Файловые и загрузочные вирусы	2		**6**		**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3], подготовка к практике			
	Тема 4.3. Руткиты и инструменты сокрытия	2				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 4.4. Антивирусные средства и инструменты	2				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 4 разделу	**8**		**6**	**1**	**8**				
Раздел 5. Основы криптографии										
ПКС-2 - ИПКС-2.1 ПКС-3 - ИПКС-3.2	**Тема 5.1.** Принципы современного шифрования данных	2			**1**	**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 5.2. Асимметричное шифрование	2				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 5.3. Критерии оценки алгоритмов шифрования	2				**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 5.4. Средства и инструменты расшифровки данных	2		6		**2**	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3], подготовка к практике			
	Итого по 5 разделу	**8**		**6**	**1**	**8**				

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					
	Итого за семестр	**34**		**34**	**6**	**34**				

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

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Перечень вопросов, выносимых на промежуточную аттестацию (экзамен)

1) Определение, основные понятия и общее содержание проблемы информационной безопасности.
2) Нормативные документы по защите информации
3) Угрозы информационной безопасности
4) Уязвимости информационной безопасности
5) Методы защиты информации от несанкционированного доступа.
6) Методы идентификации и аутентификации.
7) Основы криптографических методов защиты информации.

Для выполнения процедур оценивания составлен паспорт оценочных средств.

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 контроля и оценки успеваемости студентов.

При промежуточном контроле успеваемость студентовоценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.3–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-2.1 Проектирует информационные системы	Изложение учебного материала бессистемное, неполное, не освоеныбазовые 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 освоеныбазовые 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 5.5 - 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. 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. — Режим доступа: для авториз. пользователей.

6.1.2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/185333. — Режим доступа: для авториз. пользователей.

6.3Методические указания, рекомендации и другие материалы к занятиям

Электронные варианты методическихуказаний по выполнению практических работ по дисциплине «Теория и методология информационной безопасности»отправляются на электронные адреса групп.

6.3.1. Теория и методология информационной безопасности [Электронные текстовые данные]: метод.указания к прак. работе по дисциплине «Теория и методология информационной безопасности» для студентов направления подготовки бакалавра 09.03.02 «Информационные системы и технологии» дневной формы обучения / НГТУ; Сост.: Д.А.Ляхманов.Н.Новгород, 2021.

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	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.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/)

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

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице8.1указан 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 и проведения практическихзанятий для студентов очного обучения, включает в себя компьютерные классы

1. ***Ауд. 4403 кафедры «Информатика и системы управления» - лаборатория Программирования АСО и У***

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

- 10 АРМ (терминалов);
- мультимедийный проектор Vivitek H 1180,
- экран настенный LMP 100109,
- сетевая купольная PTZ-камера AXIS M5014.

Пакеты ПО (лицензионное):

- Dr.Web(с/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024),
- MATLAB R2008a DVD KIT-WIN & UNIX/MAC (№ лицензии 527840, № заказа 2035235 Softline от 05.05.2008).

Пакеты ПО (распространяемое по свободной лицензии):

- ApacheOpenOffice;
- Eclipse (https://www.eclipse.org/)
- 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	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 +GeFORCE 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 ZNFC-CR5D-5U3U-JKGP от 20.05.2024)
	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	1. Рабочие места студента, оснащенные ПК на базе IntelCore i5 с мониторами – 8 шт. 2. Рабочие места студента, оснащенные ПК на базеCore 2 Duo с мониторами –2 шт. 3. Рабочее место преподавателя, оснащенное ПК на базе IntelCore i5 с монитором – 1 шт. 4. Проектор Accer, проекционный экран – 1 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета 5. Принтер HP LaserJet 1200 – 1 шт.	1. MicrosoftWindows 7 MSDN реквизиты договора - подписка DreamSparkPremium, договор № 0509/КМР от 15.10.18 2. Бесплатное ПО: Пакет программ OpenOffice, TrueConf, Браузер GoogleChrome, Браузер MozillaFirefox, Браузер Opera, McAfeeSecurityScan, AdobeAcrobatReader DC, AutoCAD2013

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихсяпо 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 «Теория и методология информационной безопасности», 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, практических 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 практических 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 форсированности компетенции применяетсябально-рейтинговаясистема 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 лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.4 Методические указания по освоению дисциплины на практическихзанятиях

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и

сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению реферата или эссе, требования к их оформлению, порядок сдачи

Примерная тематика рефератов

1. Угрозы ИБ
2. Многоуровневая (Мандатная) политика информационной безопасности
3. Мандатная модель информационной безопасности Белла и Лападула
4. Модели контроля целостности
5. Модель информационной безопасностиБиба
6. Модель информационной безопасностиКларка-Вильсона
7. Модель информационной безопасностиБрюэра и Неша («Китайская стена»)
8. Ролевая политикаинформационной безопасности
9. Модель «take-grant»
10. Модель Low-Water-Mark (LWM)

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6Методические 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 вРазделе 9. В аудиториях имеетсядоступ 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 рефератов**для студентов всех форм обучения**;

Примерная тематика рефератов

1. Многоуровневая (Мандатная) политика информационной безопасности
2. Мандатная модель информационной безопасности Белла и Лападула
3. Модели контроля целостности
4. Модель информационной безопасностиБиба
5. Модель информационной безопасности Кларка-Вильсона
6. Модель информационной безопасностиБрюэра и Неша («Китайская стена»)
7. Ролевая политика информационной безопасности
8. Модель «take-grant»
9. Модель Low-Water-Mark (LWM)

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

Примерная тематика практических занятий

1. Использование средств обнаружения вторжений
2. Средства управления информационной безопасность SIEM
3. Применение средств блокирования несанкционированной рассылки и перехвата данных
4. Противодействие сетевым червям типа malware вторжений
5. Применение средств шифрования и расшифровывания вторжений

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

Экзамен для студентов очной формы обучения в 7 семестре.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов очной формыобучения

1. Определение, основные понятия и общее содержание проблемы информационной безопасности.
2. Нормативные документы по защите информации
3. Угрозы информационной безопасности
4. Уязвимости информационной безопасности
5. Методы защиты информации от несанкционированного доступа.
6. Методы идентификации и аутентификации.
7. Основы криптографических методов защиты информации.
8. Многоуровневая (Мандатная) политика информационной безопасности
9. Мандатная модель информационной безопасности Белла и Лападула
10. Модели контроля целостности
11. Ролевая политика информационной безопасности

В полном объеме оценочные средства имеются на кафедре «ИСУ». Оценочные средства могут быть получены по требованию.