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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B4A6F7AAA383423E375F0ECF5610EF68
Владелец: Глебов Владимир Владимирович
Действителен: с 10.07.2025 до 03.10.2026

УТВЕРЖДАЮ:
Директор АПИ НГТУ:
_____ Глебов В.В.
(подпись) *(ФИО)*
«_25_» __01_____2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04 Обеспечение информационной безопасности в инфокоммуникациях
(индекс и наименование дисциплины по учебному плану)

для подготовки магистров

Направление подготовки: 11.04.03 Конструирование и технология электронных средств
(код и наименование направления подготовки)

Направленность: Информационные технологии проектирования радиоэлектронных средств
(наименование профиля, программы магистратуры)

Форма обучения: очная, очно-заочная
(очная, очно-заочная, заочная)

Год начала подготовки: 2025

Объем дисциплины: 144 / 4
(часов/з.е.)

Промежуточная аттестация: экзамен
(экзамен, зачет с оценкой, зачет)

Выпускающая кафедра: КиТ РЭС
(аббревиатура кафедры)

Кафедра-разработчик: КиТ РЭС
(аббревиатура кафедры)

Разработчик(и): Ямпурин Н.П., д.т.н., профессор
(ФИО, ученая степень, ученое звание)

г. Арзамас
2025 г.

Рабочая программа дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 11.04.03 Конструирование и технология электронных средств, утвержденного приказом Минобрнауки России от 22 сентября 2017 г. № 956 на основании учебного плана, принятого Ученым советом АПИ НГТУ,

протокол от 29.01.2025 г. № 1

Рабочая программа одобрена на заседании кафедры-разработчика, протокол от 16.01.2025 г. № 1

Заведующий кафедрой _____ _____Жидкова Н.В.__

(подпись) *(ФИО)*

Рабочая программа рекомендована к утверждению УМК АПИ НГТУ,

протокол от 29.01.2025 г. № 1

Зам. директора по УР _____Шурыгин А.Ю.

(подпись)

Рабочая программа зарегистрирована в учебном отделе № 11.04.03-04

Начальник УО _____Мельникова О.Ю.

(подпись)

Заведующая отделом библиотеки _____Старостина О.Н.

(подпись)

Оглавление

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель освоения дисциплины (модуля)

Целью освоения дисциплины «Обеспечение информационной безопасности в инфокоммуникациях» является ознакомление студентов с основными понятиями и определениями информационной безопасности ;источниками, рисками и формами атак на информацию; методами, средствами и системами защиты информации в инфокоммуникационных сетях; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей и защитой от вредоносных программ.

1.2. Задачи освоения дисциплины (модуля)

К основным задачам освоения дисциплины относятся:

- ознакомление с информационным противоборством в мире и Доктриной РФ ;
- знакомство с терминологией и основными понятиями информационной безопасности ;
- изучение методов и технологий защиты информации в инфокоммуникациях;
- классификация, математические модели, алгоритмы и методы криптографической защиты информации;
- ознакомление со стандартами и современными тенденциями развития инфокоммуникационной безопасности;
- ознакомление с политикой безопасности предприятий и компаний в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Обеспечение информационной безопасности в инфокоммуникациях» включена в перечень дисциплин обязательной части, определяющих направленность ОП. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП.

Дисциплина базируется на следующих дисциплинах: «Информатика», «САПР в электронике», « Схемотехническое проектирование», «Применение пакетов прикладных программ в проектировании электронных средств».

Результаты обучения, полученные при освоении дисциплины «Обеспечение информационной безопасности в инфокоммуникациях», необходимы при изучении дисциплины « Компьютерное и схемотехническое проектирование электронных средств» и при подготовке выпускной квалификационной работы.

Рабочая программа дисциплины «Обеспечение информационной безопасности в инфокоммуникациях» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

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

Процесс изучения дисциплины «Обеспечение информационной безопасности в инфокоммуникациях» направлен на формирование элементов ощепрофессиональных и профессиональных компетенций ОПК-4 и ПКС-2 в соответствии с ФГОС ВО и ОП ВО по направлению подготовки 11.04.03 Конструирование и технология электронных средств.

Таблица 3.1 – Формирование компетенций дисциплинами

Код компетенции / наименование дисциплин, формирующих компетенцию совместно	Семестры формирования дисциплины Компетенции берутся из УП по направлению подготовки бакалавра / магистра			
	1	2	3	4
ОПК-4. Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач				
Научно-исследовательская работа				
Математическое моделирование устройств и систем				
Применение пакетов прикладных программ в проектировании электронных средств				
Обеспечение информационной безопасности в инфокоммуникациях				
Компьютерное и схемотехническое проектирование электронных средств				
Технологическая (проектно-технологическая) практика				
Выполнение и защита ВКР				
ПКС-2. Способен проектировать устройства, приборы и системы электронной техники с учетом заданных требований				
Иностранный язык для научно-исследовательской работы				
Современные технологии электронных средств				
Элементы теории конформных отображений для ЭС				
Проектирование микроэлектронных устройств				
Схемотехническое проектирование				
Математическое моделирование устройств и систем				
Применение пакетов прикладных программ в проектировании электронных средств				
Патентоведение				
САПР в электронике				
Кадровый менеджмент				
Обеспечение информационной безопасности в инфокоммуникациях				
Коммерциализация результатов научных исследований и разработок				
Компьютерное и схемотехническое проектирование электронных средств				
Объектно-ориентированное программирование				
Проектно-технологическая практика				
Преддипломная практика				
Выполнение и защита ВКР				

Перечень планируемых результатов обучения по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях», соотнесенных с планируемыми результатами освоения ОП, представлен в табл. 3.2.

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине		
ОПК-4. Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач	ИОПК-4.3. Использует современные программные средства (CAD) моделирования, оптимального проектирования и конструирования приборов, схем и электронных устройств различного функционального назначения.	**Знать:** Основные требования к информационной безопасности при проектировании и конструировании приборов, схем и электронных устройств различного функционального назначения с целью оптимизации их параметров.	**Уметь:** Рассчитывать и анализировать основные характеристики и параметры устройств защиты информации с целью отбора оптимальных проектных решений на всех этапах проектного процесса.	**Владеть:** Навыками программирования криптографических алгоритмов на основе языков высокого уровня.
ПКС-2. Способен проектировать устройства, приборы и системы электронной техники с учетом заданных требований	ИПКС-2.3. Проектирует электронные приборы, схемы и устройства различного функционального назначения, выбирая оптимальный вариант, оценивая его достоинства и недостатки	**Знать:** Информационное противоборство в современном мире, основные требования к информационной безопасности, в том числе защите гостайны. Доктрину информационной безопасности РФ, классификацию угроз информационной безопасности и средства их предотвращения, парирования, нейтрализации. Криптографические методы защиты информации: шифры докомпьютерной эпохи, симметричные алгоритмы шифрации, шифрация с открытым ключом, электронная цифровая подпись. Построение систем защиты информации при проектировании и конструировании приборов, схем и электронных устройств.	**Уметь:** Согласовывать технические условия и задания при проектировании и конструировании приборов, схем и электронных устройств . Осуществлять расчет основных показателей качества при проектировании и конструировании приборов, схем и электронных устройств	**Владеть:** Навыками анализа, уточнения и согласования технического задания на проектируемое устройство, прибор и систему электронной техники, определения вариантов построения информационной безопасности устройства, прибора и системы электронной техники и/или его составляющих. Выбором программно-аппаратных средств устройства, прибора или системы электронной техники путем сопоставления различных вариантов с учетом технических и экономических требований.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам

Общая трудоемкость дисциплины составляет 4 зач. ед. или 144 часа, распределение часов по видам работ по семестрам представлено в таблице 4.1.

Таблица 4.1 – Распределение трудоемкости дисциплины по видам работ по семестрам для студентов очного обучения / заочного обучения

Вид учебной работы	Трудоемкость в час	
	Всего час.	В т.ч. по семестрам
		8 семестр/ 9 семестр
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоемкость дисциплины по учебному плану	**144/144**	**144/144**
1. Контактная работа:	**48/38**	**48/38**
1.1. Аудиторная работа, в том числе:	**42/32**	**42/32**
занятия лекционного типа (Л)	10/8	10/8
занятия семинарского типа (ПЗ – семинары, практические занятия и др.)	16/12	16/12
лабораторные работы (ЛР)	16/12	16/12
1.2. Внеаудиторная, в том числе	**6/6**	**6/6**
курсовая работа (проект) (КР/КП) (консультация, защита)	–	–
текущий контроль, консультации по дисциплине	4/4	4/4
контактная работа на промежуточном контроле (КРА)	2/2	2/2
2. Самостоятельная работа (СРС)	**96/106**	**96/106**
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.)	60/70	60/70
Подготовка к экзамену (контроль)	36/36	36/36
Подготовка к зачету / зачету с оценкой (контроль)	–	–

4.2 Содержание дисциплины, структурированное по разделам, темам

Таблица 4.2 – Содержание дисциплины, структурированное по темам, для студентов очной/очно-заочной формы обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	**Наименование разделов, тем**	**Виды учебной работы (час)**				**Вид СРС**
		Контактная работа			**Самостоятельная работа студентов**	
		Лекции	**Лабораторные работы**	**Практические занятия**		
7 семестр/7 семестр						
	Раздел 1.Информация в современном обществе и необходимость ее защиты					
	Тема1.1. Введение, термины и определения. Виды информации в обществе. Информационное противоборство в современном мире.	3/2			20/22	Подготовка к лекциям [6.1.1], [6.1.3]

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)				Вид СРС
		Контактная работа			Самостоятельная работа студентов	
		Лекции	Лабораторные работы	Практические занятия		
ОПК-4 **ИОПК-4.3** **ПКС-4** **ИПКС-4.1**	Тема 1.2. Национальный Интерес РФ в информационной сфере. Доктрина информационной безопасности РФ. Тема 1.3. Свойства и характеристики информации, её классификация. Необходимость и потребность в защите информации. 1.4.Основные понятия защиты информации, ее структурирование. Методы и средства защиты от угроз информационной безопасности.					
	Практическое занятие№1 Методы и средства технологий защиты информации			4/4		Подготовка к лабораторным занятиям [6.3.1]
	Итого по 1 разделу	**3/2**		**4/4**	**20/22**	
	Раздел 2.Инфокоммуникационная безопасность и криптографические методы ее обеспечения					
	Тема 2.1. Атаки и их классификация. Криптографическая защита информации, схема канала секретной связи. Тема 2.2. Криптоанализ и схемы атак на шифрсообщения. Модель сетевой безопасности. Тема 2.3. Шифры докомпьютерной эпохи ,моноалфавитные и полиалфавитные шифры. Современная классификация систем шифрования. Тема 2.4. Симметричные алгоритмы шифрации: модели шифрации и классификация шифров. Шифры Фейстеля, DES, ГОСТ 28147-89, Rijndael. Тема 2.5. Протоколы распределения ключей при симметричном шифровании: «широкоротой» лягушки, Цербера. Тема 2.6. Алгоритмы шифрации с открытым ключом: RSA, Эль-Гамаль. Электронная цифровая подпись и хэш-функция. Тема 2.7. .Методы аутентификации сообщений.	4/3			20/24	Подготовка к лекциям [6.1.2], [6.1.2]
	Практическое занятие №2. Основные принципы, алгоритмы и системы шифрации.			8/4		Подготовка к практическим занятиям [6.3.3]
	Лабораторная работа №1. Реализация криптографичес-ких алгоритмов с помощью языков программирования. Лабораторная работа №2.Шифрование данных с помощью алгоритма DES.		4/4 4/4			Подготовка к лабораторным занятиям [6.3.1]
	Итого по 2 разделу	**4/3**	**8/8**	**8/4**	**20/24**	
	Раздел 3. Программно-аппаратные средства обеспечения инфокоммуникационной безопасности					
	Тема 3.1. Виды несанкционированного доступа и защита от него. Тема 3.2. Вирусы: классификация, схемы функционирования , защита. Тема 3.3. Виртуализация каналов. Тема 3.4 . Технические каналы утечки информации.	3/2			20/24	Подготовка к лекциям [6.1.1], [6.1.3]

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)				Вид СРС
		Контактная работа			Самостоятельная работа студентов	
		Лекции	Лабораторные работы	Практические занятия		
	Практическое занятие№3. Методы и средства межсетевой и внутрисетевой защиты процессов переработки информации			4/4		Подготовка к практическим занятиям [6.1.3]
	Лабораторная работа №3. Антивирусное программное обеспечение Лабораторная работа №4. Технология виртуализации. Изучение виртуальной машины как средства защиты данных.		4/4 4/0			Подготовка к лабораторным занятиям [6.3.1]
	Итого по 4 разделу	**3/2**	**8/4**	**4/4**	**20/24**	
	ИТОГО за семестр	**10/8**	**16/12**	**16/12**	**60/70**	
	ИТОГО по дисциплине	**10/8**	**16/12**	**16/12**	**60/70**	

Таблица 4.3 - Используемые активные и интерактивные образовательные технологии

Вид занятий	Наименование используемых активных и интерактивных образовательных технологий
Лекции	Технология развития критического мышления Дискуссионные технологии
Практические занятия	Технология развития критического мышления Дискуссионные технологии Тестовые технологии Технологии работы в малых группах Технология коллективной работы Информационно-коммуникационные технологии

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

5.1. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Оценочные процедуры текущего контроля успеваемости по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях» проводятся преподавателем дисциплины.

Для оценки текущего контроля **знаний** используются тесты, сформированные в системе MOODLE.

Тесты по разделам 1-3 содержат всего 80 тестовых вопросов, время на проведение тестирования раздела 10 минут. На каждый тест дается 2 попытки.

Для оценки текущего контроля **умений** и **навыков** проводятся практические занятия в форме выполнения заданий. При выполнении практического задания преподавателем оценивается качество выполненного задания, срок его выполнения, качество и срок оформления отчета, ответы на вопросы преподавателя.

Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации представлены в табл. 5.1.

Студент допускается к промежуточной аттестации (экзамену), если в результате изучения разделов дисциплины в ходе текущего контроля ответил верно на 60% вопросов тестов и предоставил отчеты по всем практическим работам.

Билет для промежуточной аттестации содержит 2 теоретических вопроса, время на подготовку ответов - 45 минут. Промежуточная аттестация считается пройденной, если студент набрал не менее 3 баллов.

Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации представлены в табл. 5.2.

Итоговая оценка по дисциплине формируется по результатам текущего контроля и промежуточной аттестации (таблица 5.3).

Таблица 5.1 – Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации

Код и наименование компетенции	Код и наименование индикатора компетенции	Показатели контроля успеваемости	Критерии и шкала оценивания		Форма контроля
			1 балл	0 баллов	
ОПК-4. Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач	ИОПК-4.3. Использует современные программные средства (CAD) моделирования, оптимального проектирования и конструирования приборов, схем и электронных устройств различного функционального назначения.	**Знать:** Основные требования к информационной безопасности при проектировании и конструировании приборов, схем и электронных устройств различного функционального назначения с целью оптимизации их параметров.	Верно выполнено 60 процентов и более вопросов каждого теста*	Верно выполнено менее 60 процентов вопросов каждого теста	а) Контроль посещения лекций б) Контроль участия в дискуссиях на лекциях в) Проверка конспектов лекций г) Тестирование д) Контроль выполнения самостоятельной работы
		Уметь: Рассчитывать и анализировать основные характеристики и параметры устройств защиты информации с целью отбора оптимальных проектных решений на всех этапах проектного процесса.	Практические задания выполнены качественно, оформлены в срок и в полном объеме**	Практические задания не выполнены и не оформлены	Контроль выполнения и защиты лабораторных работ и практических заданий: ЛР№3,4, ПЗ №3-5. Контроль выполнения самостоятельной работы
		Владеть: Навыками программирования криптографических алгоритмов на основе языков высокого уровня.	Практические задания выполнены качественно, оформлены в срок и в полном объеме**	Практические задания не выполнены и не оформлены	Контроль выполнения и защиты лабораторных работ и практических заданий: ЛР№3, ПЗ №4,5. Контроль выполнения самостоятельной работы (РГР)
ПКС-2. Способен проектировать устройства, приборы и системы электронной техники с учетом заданных требований	ИПКС-2.3. Проектирует электронные приборы, схемы и устройства различного функционального назначения, выбирая оптимальный вариант, оценивая его достоинства и недостатки	**Знать:** Информационное противоборство в современном мире, основные требования к информационной безопасности, в том числе защите гостайны. Доктрину информационной безопасности РФ, классификацию угроз информационной безопасности и средства их предотвращения, парирования, нейтрализации . Криптографические методы защиты информации: шифры докомпьютерной эпохи, симметричные алгоритмы шифрации, шифрация с открытым ключом, электронная цифровая подпись. Построение систем защиты информации при проектировании и конструировании приборов, схем и электронных устройств.	Верно выполнено 60 процентов и более вопросов каждого теста*	Верно выполнено менее 60 процентов вопросов каждого теста	а) Контроль посещения лекций б) Контроль участия в дискуссиях на лекциях в) Проверка конспектов лекций г) Тестирование д) Контроль выполнения самостоятельной работы

Код и наименование компетенции	Код и наименование индикатора компетенции	Показатели контроля успеваемости	Критерии и шкала оценивания		Форма контроля
			1 балл	0 баллов	
		Уметь: Согласовывать технические условия и задания при проектировании и конструировании приборов, схем и электронных устройств. Осуществлять расчет основных показателей качества при проектировании и конструировании приборов, схем и электронных устройств	Практические задания выполнены качественно, оформлены в срок и в полном объеме**	Практические задания не выполнены и не оформлены	Контроль выполнения и защиты лабораторных работ и практических заданий: ЛР№3,4, ПЗ №3-5. Контроль выполнения самостоятельной работы
		Владеть: Навыками анализа, уточнения и согласования технического задания на проектируемое устройство, прибор и систему электронной техники, определения вариантов построения информационной безопасности устройства, прибора и системы электронной техники и/или его составляющих . Выбором программно-аппаратных средств устройства, прибора или системы электронной техники путем сопоставления различных вариантов с учетом технических и экономических требований.	Практические задания выполнены качественно, оформлены в срок и в полном объеме**	Практические задания не выполнены и не оформлены	Контроль выполнения и защиты лабораторных работ и практических заданий: ЛР№3, ПЗ №4,5. Контроль выполнения самостоятельной работы (РГР)

**) за каждый тест назначается по 1 баллу;*

***) за каждое практическое занятие назначается по 1 баллу.*

Таблица 5.2 – Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации (экзамен)

Код и наименование компетенции	Код и наименование индикатора компетенции	Показатели контроля успеваемости	Критерии и шкала оценивания			Форма контроля
			2 балла	1 балл	0 баллов	
ОПК-4. Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач	ИОПК-4.3. Использует современные программные средства (CAD) моделирования, оптимального проектирования и конструирования приборов, схем и электронных устройств различного функционального назначения.	**Знать:** Основные требования к информационной безопасности при проектировании и конструировании приборов, схем и электронных устройств различного функционального назначения с целью оптимизации их параметров.	Представлен развернутый ответ на вопрос	Представлен не полный ответ на вопрос	Ответ на вопрос отсутствует	Ответ на теоретический вопрос билета
			Представлен развернутый ответ на вопрос	Представлен не полный ответ на вопрос	Ответ на вопрос отсутствует	Ответ на дополнительные вопросы
		Уметь: Рассчитывать и анализировать основные характеристики и параметры устройств защиты информации с целью отбора оптимальных проектных решений на всех этапах проектного процесса.	Задание решено верно	Задание решено с ошибками	Задание не решено	Решение задач билета
ПКС-2. Способен проектировать устройства, приборы и системы электронной техники с учетом заданных требований	ИПКС-2.3. Проектирует электронные приборы, схемы и устройства различного функционального назначения, выбирая оптимальный вариант, оценивая его достоинства и недостатки	**Знать:** Информационное противоборство в современном мире, основные требования к информационной безопасности, в том числе защите гостайны. Доктрину информационной безопасности РФ, классификацию угроз информационной безопасности и средства их предотвращения, парирования, нейтрализации. Криптографические методы защиты информации: шифры докомпьютерной эпохи, симметричные алгоритмы шифрации, шифрация с открытым ключом, электронная цифровая подпись .Построение систем защиты информации при проектировании и конструировании приборов, схем и электронных устройств.	Представлен развернутый ответ на вопрос	Представлен не полный ответ на вопрос	Ответ на вопрос отсутствует	Ответ на теоретический вопрос билета
			Представлен развернутый ответ на вопрос	Представлен не полный ответ на вопрос	Ответ на вопрос отсутствует	Ответ на дополнительные вопросы
		Уметь: Согласовывать технические условия и задания при проектировании и конструировании приборов, схем и электронных устройств. Осуществлять расчет основных показателей качества при проектировании и конструировании приборов, схем и электронных устройств.	Задание решено верно	Задание решено с ошибками	Задание не решено	Решение задач билета

Таблица 5.3 – Соответствие набранных баллов и оценки за промежуточную аттестацию

Баллы за текущую успеваемость*	Баллы за промежуточную аттестацию		Оценка
	Суммарное количество баллов**	Баллы за решение задач**	
0 баллов	0…2 баллов	0 баллов	«неудовлетворительно»
13 баллов	3 балла	не менее 1 балла	«удовлетворительно»
13 баллов	4…5 баллов	не менее 2 баллов	«хорошо»
13 баллов	6 баллов	не менее 2 баллов	«отлично»

**) – количество баллов рассчитывается в соответствии с таблицей 5.1.;*
***) – количество баллов рассчитывается в соответствии с таблицей 5.2.*

5.2. Оценочные средства для контроля освоения дисциплины

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

Для текущего контроля знаний и умений студентов по дисциплине проводится комплексная оценка, включающая:

выполнение лабораторных работ (выполнение заданий , ответы на контрольные вопросы) с оформлением отчетов ;

выполнение практических заданий (участие в работе семинаров, ответы на контрольные вопросы), выступление с докладами по тематике практических занятий;

тестирование по всем разделам дисциплины.

Типовые контрольные вопросы для лабораторных работ

Раздел 2. Инфокоммуникационная безопасность и криптографические методы ее обеспечения

Лабораторная работа №1. Реализация криптографических алгоритмов с помощью языков программирования.

1. Какие методы взлома шифров докомпьютерной эпохи Вы знаете?
2. Перечислите полиалфавитные шифры и укажите их шифростойкость?
3. Для шифров, указанных в работе, привести алгоритмы шифрования.
4. Почему шифры докомпьютерной эпохи обязательно можно взломать современными средствами вычислительной техники?

Лабораторная работа №2. Шифрование данных с помощью алгоритма DES.

1. Какие методы взлома шифра DES Вы знаете?
2. Перечислите методы повышения криптостойкости алгоритма DES.
3. Для шифра DES привести алгоритм шифрования.
4. Почему шифр DES обязательно можно взломать современными средствами вычислительной техники?

Раздел 3. Программно-аппаратные средства обеспечения инфокоммуникационной безопасности

Лабораторная работа №3. Антивирусное программное обеспечение

1. Какие типы вирусных угроз Вы знаете?
2. Какие антивирусные пакеты Вы знаете? Какие типы защит обеспечивает современный антивирусный пакет?
3. Что такое база сигнатур и зачем требуется её обновление?
4. Зачем может потребоваться загрузка антивирусного пакета с помощью LiveCD?

Лабораторная работа №4. Технология виртуализации. Изучение виртуальной машины как средства защиты данных.

1. Что такое «песочница» и в чем преимущества ее использования?
2. Приводит ли использование виртуальной машины к потере производительности?
3. Какие операционные системы могут быть установлены в качестве гостевых?
4. Как использование виртуальной машины может повысить безопасность компьютера?

Типовые задания для лабораторных работ

Раздел 2. Инфокоммуникационная безопасность и криптографические методы ее обеспечения

Лабораторная работа №1. Реализация криптографических алгоритмов с помощью языков программирования.

Задание №1. Разработать программу, реализующую шифрование и дешифрование алгоритмом простой замены (шифр Цезаря), вариант указывается преподавателем.

Вариант	Исходная фраза	Ключ	Алфавит
1	HELLOWORLD	9	Латиница (26)
2	MOTHERLAND	8	
3	DICTIONARY	7	
4	GRADUATE	6	
5	ENCODING	5	
6	SYNCHROPHASOTRON	4	
7	ETHERNET	3	
8	VALIDATOR	10	
9	CYBERNETICS	19	
10	RESIDENT	18	
11	CRYPTOANALYSIS	12	
12	ENCAPSULATION	21	
13	REPLICATION	22	
14	CORRELATION	15	
15	DISPERSION	13	
16	MAGNITUDE	11	

Задание №2. Разработать программу, реализующую шифрование и дешифрование алгоритмом полиалфавитной замены (шифр Виженера), вариант указывается преподавателем.

Вариант	Исходная фраза	Ключ	Алфавит
1	HELLOWORLD	CABLE	Латиница (26)
2	MOTHERLAND	STORE	
3	DICTIONARY	MARIA	
4	GRADUATE	TODAY	
5	ENCODING	ALBUM	
6	SYNCHROPHASOTRON	OCEAN	
7	ETHERNET	VENUS	
8	VALIDATOR	STAGE	
9	CYBERNETICS	LEVEL	
10	RESIDENT	HOMER	
11	CRYPTOANALYSIS	HOUSE	
12	ENCAPSULATION	CODER	
13	REPLICATION	CIPHER	
14	CORRELATION	STORM	
15	DISPERSION	PHONE	
16	MAGNITUDE	LAWER	

Типовые тестовые задания для текущего контроля

Тесты для текущего контроля знаний обучающихся сформированы в системе MOODLE и находятся в свободном доступе на странице курса «Обеспечение информационной безопасности в инфокоммуникациях» по адресу: https://sdo.api.nntu.ru/course/view.php?id=43.

Раздел 1. Информация в современном обществе и необходимость ее защиты.

1.1. Основой обеспечения информационной безопасности РФ является :
а) Доктрина информационной безопасности РФ ;
б) кибербригада Министерства Обороны РФ;
в) Центр по кибертерроризму в Сколково.
ANSWER: а)

1.2. Защищаемая информация классифицируется по:
а) уровню насыщенности;
б) степени секретности;
в) принадлежности;
г) уровню важности;
д) носителям информации;
е) объему информации.
ANSWER: б),в),г).

Раздел 2. Сетевая безопасность и криптографические методы ее обеспечения

2.1. Какое из утверждений не относится к принципу Керхкоффа
а) в секрете держится алгоритм шифрации;
б) в секрете держится ключ шифрации;
в) передача информации идет по секретным (закрытым) каналам.
ANSWER: в)

2.2. Какие системы шифрации являются алгоритмами шифрации с открытым ключом?
а) DES;
б) стандарт ГОСТ 28147-89;
в) Rijndael;
г) RSA;
д) Эль – Гамаль.
ANSWER: г),д)

Раздел 3. Программно-аппаратные средства обеспечения инфокоммуникационной безопасности

3.1. Какое из определений соответствует понятию конфиденциальность информации:

а) состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность

б) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно

в) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

г) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

ANSWER: а)

3.2. Выберите функции, которые может выполнять межсетевой экран:
а) фильтрация данных
б) трансляция адресов
в) анализ трафика на наличие зловредного кода
г) использование экранирующих агентов

ANSWER: а),б),г).

Типовые задания для практических занятий

Раздел 1. Информация в современном обществе и необходимость ее защиты.

Практическое занятие№1. Методы и средства технологий защиты информации

Тематика докладов к практическому(семинарскому) занятию

1. Критерии оценки безопасности компьютерных систем («Оранжевая книга»США).
2. Методы и средства обеспечения хранения и переработки информации в компьютерных системах(КС).
3. Основные положения Доктрины ИБ РФ в редакции 2016 года.
4. Основные задачи обеспечения ИБ РФ.
5. Основные задачи обеспечения безопасности функционирования информации в КС.
6. Классификация методов предотвращения угроз несанкционированного доступа в КС и их характеристика.
7. Классификация организационных и правовых методов и средств предотвращения угроз ИБ и их описание.
8. Классификация криптографических методов предотвращения угроз ИБ
9. Дайте характеристику основных групп методов защиты процессов переработки информации в КС.
10. Классификация методов и средств нейтрализации угроз ИБ и их описание
11. Классификация методов предотвращения угроз несанкционированного доступа в КС и их описание.
12. Классификация организационных и правовых методов и средств предотвращения угроз ИБ и их описание.

Раздел 2. Инфокоммуникационная безопасность и криптографические методы ее обеспечения

Практическое занятие№2. Основные принципы, алгоритмы и системы шифрации

Тематика докладов к практическому(семинарскому) занятию

1. Стандарт шифрования данных DES: алгоритм и области использования.
2. Блочный шифр MARS: алгоритмы и области использования.
3. Алгоритм RSA и области его использования.
4. Алгоритм Эль-Гамаль.
5. Алгоритм Rijndael: общие сведения и области использования.
6. Режимы ECB и CBC стандарта шифрования DES.
7. Коды аутентификации сообщений (MAC): CBC-MAC.
8. Коды аутентификации сообщений (MAC): HMAC.
9. Шифр Фейстеля.
10. Алгоритм поточной шифрации, его недостатки и преимущества.
11. Поточные шифры на основе регистра сдвига с линейной ОС.
12. Схема блочного алгоритма шифрования, блочный шифр RC5.
13. Схема блочного алгоритма шифрования, блочный шифр RC6.
14. Поточный шифр RC4 и его особенности.
15. Поточные шифры с комбинацией регистров сдвига с ОС.
16. Распределение симметричных ключей: протокол Нидхейма-Шредера.
17. Распределение симметричных ключей: протокол Отвей-Риса.
18. Алгоритм Рабина-Карпа.
19. Распределение ключей в протоколе Диффи-Хеллмана.
20. Криптография с открытым ключом: схема цифровой подписи с приложением.
21. Криптография с открытым ключом: схема цифровой подписи с восстановлением сообщения.
22. Применение алгоритма RSA для подписи с восстановлением сообщения.
23. Хэш-функции и их использование.
24. Алгоритм цифровой подписи DSA.
25. Алгоритм цифровой подписи Шнорра.

26. Алгоритм цифровой подписи Ниберга-Руппеля.
27. Алгоритм International Data Encryption Algorithm.
28. Режимы OFB и CFB стандарта шифрования DES.
29. Компьютерная стеганография и ее применение.
30. Защита документов Microwave Office от несанкционированного доступа.
31. Новый алгоритм шифрования Symmetric Encryption Algorithm (SEA).
32. Блочный алгоритм шифрования: Serpent.
33. Блочный алгоритм шифрования:IDEA.
34. Блочный алгоритм шифрования:Blow fish.
35. Алгоритм цифровой подписи ГОСТ Р 34.10-94

Раздел 3. Программно-аппаратные средства обеспечения инфокоммуникационной безопасности

Практическое занятие№3. Методы и средства межсетевой и внутрисетевой защиты процессов переработки информации

Тематика докладов к практическому(семинарскому) занятию

1. Методы и средства ограничения доступа к компонентам ЭВМ.
2. Программно-аппаратные средства защиты ПЭВМ.
3. Методы и средства обеспечения ИБ в ОС.
4. Защита процессов переработки информации в СУБД.
5. Методы и средства закрытия речевых сигналов в телефонных каналах.
6. Функциональные схемы механической и оборонительной систем защиты.
7. Технические средства охранной сигнализации.
8. Алгоритмы защиты БД Access.
9. Системы безопасности SQL Server
10. Модель безопасности Windows NT.
11. Методы защиты инсталляционных дисков от копирования.
12. Методы противодействия исследованию алгоритма работы системы защиты.
13. Виртуальные ЛВС и их использование для защиты информации.
14. Межсетевая безопасность: протоколы IEEE 802.1x.
15. Межсетевая безопасность: системы туннелирования и протоколы PPP и PPPoE.
16. Виртуальные ЛВС на базе протокола IEEE 802.1Q.
17. Протоколы WEP и WPA и их сравнительный анализ по уровню безопасности.
18. Протоколы TKIP и IEEE 802.11i и их сравнение по уровню безопасности.
19. Протоколы STPи основные типы атак на виртуальные ЛВС.
20. Протоколы IEEE 802. 1X и их использование для контроля доступа
21. Виртуальные частные сети и защита информации в каналах связи.

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

Перечень вопросов для подготовки к зачету

1. Информация в современном обществе и необходимость её защиты.
2. Источники информации в современном обществе.
3. Основные положения “Доктрины информационной безопасности“РФ.
4. Свойства и характеристики информации: доступность.
5. Свойства и характеристики информации: ценность.
6. Свойства и характеристики информации: мера.
7. Государственная и коммерческая тайна, их разновидности.
8. Основные понятия защиты информации: утечка, модификация , утрата.
9. Основные понятия защиты информации: объект защиты.
10. Основные понятия защиты информации: угроза безопасности информации.
11. Классификация методов защиты процессов переработки информации в КС.
12. Классификация средств защиты процессов переработки информации в КС.
13. Методы и средства технологии защиты от угроз ИБ.

14. Схема шифрации и дешифрации в криптографии .Принцип Керххоффа
15. Цели и задачи криптографии , ее место в защите информации.
16. Классификация криптографических методов и средств предотвращения угроз ИБ.
17. Атаки и их классификация.
18. Модель сетевой безопасности.
19. Криптоанализ и его разновидности.
20. Классификация современных систем шифрации.
21. Шифры сдвига и методы их взлома.
22. Шифры перестановки и их криптоустойчивость.
23. Шифры полиалфавитной замены и их криптоустойчивость.
24. Модель шифрации и классификация симметричных алгоритмов шифрации.
25. Поточные симметричные алгоритмы шифрации.
26. Блочные симметричные алгоритмы шифрации.
27. Алгоритм шифрации Фейстеля.
28. Алгоритм шифрации DES и его криптостойкость.
29. Режимы работы блочных шифровальщиков : ECB и CBC.
30. Режимы работы блочных шифровальщиков : CFB и OFB
31. Алгоритмы AES .
32. Распределение ключей и время жизни ключа.
33. Общие сведения о протоколах распределения ключей.
34. Схема автоматического распределения ключей.
35. Протоколы распределения ключей: «широкоротой лягушки».
36. Криптография с открытым ключом и её математические основы.
37. Алгоритм RSA и его криптостойкость.
38. Сравнение схем симметричного шифрования и с открытым ключом.
39. Алгоритм шифрации Эль-Гамаль.
40. Протокол Диффи- Хеллмана : функционирование и недостатки.
41. Цифровые сертификаты и схема их использования.
42. Задачи и алгоритмы электронной подписи.
43. Схема использования электронной цифровой подписи.
44. Криптографическая ХЭШ – функция и ее назначение.
45. Методы аутентификации сообщений.
46. Разделение доступа с помощью межсетевых экранов
47. Архитектура сети с использованием МСЭ.
48. Виды несанкционированного доступа и защита от них.
49. Системы обнаружения вторжений и их классификация.
50. Архитектуры систем обнаружения вторжений
51. Компьютерные вирусы , их классификация, дайте краткую характеристику классических вирусов, «червей» и «троянов».
52. Методы защиты от вредоносных программ
53. Что такое виртуальная частная сеть и для чего её используют?
54. Использование VPN в беспроводных сетях.
55. Какие технические каналы утечки информации Вы знаете?
56. Что такое «закладки» и их классификация?
57. Дайте классификацию акустических и телефонных устройств перехвата информации.
58. Какие технические методы защиты информации от утечки Вы знаете?

Итоговый тест для проведения промежуточной аттестации

Итоговый тест для проведения промежуточной аттестации обучающихся сформирован в системе MOODLE и находятся в свободном доступе на странице курса «Обеспечение информационной безопасности в инфокоммуникациях» по адресу: https://sdo.api.nntu.ru/course/view.php?id=43.

Регламент проведения промежуточной аттестации в форме тестирования в MOODLE

Кол-во заданий в банке вопросов	Кол-во заданий, предъявляемых студенту	Время на тестирование, мин.
80	30	30

5.3. Процедура оценивания результатов обучения по дисциплине

Процедура оценивания результатов обучения по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях» состоит из следующих этапов:

1. Текущий контроль (описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации представлены в табл. 5.1, задания в п. 5.2.1).

2. Промежуточная аттестация (описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации представлены в табл. 5.2, задания в п. 5.2.2).

Для элементов компетенции ПКС-2 формируемых в рамках дисциплины, приводится процедура оценки результатов обучения (табл. 5.4).

Таблицы 5.4 – Процедура, критерии и методы оценивания результатов обучения

Планируемые результаты обучения	Критерии оценивания результатов				Методы оценивания
	1 критерий – отсутствие усвоения «неудовлетворительно»	2 критерий – не полное усвоение «удовлетворительно»	3 критерий – хорошее усвоение «хорошо»	4 критерий – отличное усвоение «отлично»	
ОПК-4. Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач. **ИОПК-4.3.** Использует современные программные средства (CAD) моделирования, оптимального проектирования и конструирования приборов, схем и электронных устройств различного функционального назначения.					
Знать: Основные требования к информационной безопасности при проектировании и конструировании приборов, схем и электронных устройств различного функционального назначения с целью оптимизации их параметров.	Отсутствие усвоения знаний	Недостаточно уверенно понимает и может объяснять полученные знания	На достаточно высоком уровне понимает и может объяснять полученные знания	Отлично понимает и может объяснять полученные знания, демонстрирует самостоятельную познавательную деятельность	Тестирование Промежуточная аттестация
Уметь: Рассчитывать и анализировать основные характеристики и параметры устройств защиты информации с целью отбора оптимальных проектных решений на всех этапах проектного процесса.	Не демонстрирует умения	Не уверенно демонстрирует умения	Достаточно уверенно демонстрирует умения	Отлично демонстрирует умения	Выполнение и защита лабораторных работ. Выполнение и защита практических заданий. Промежуточная аттестация
Владеть: Навыками программирования криптографических алгоритмов на основе языков высокого уровня.	Не демонстрирует навыки	Не уверенно демонстрирует навыки	Достаточно уверенно демонстрирует навыки	Отлично демонстрирует самостоятельные навыки	Выполнение и защита лабораторных работ. Выполнение и защита практических заданий.
ПКС-2. Способен проектировать устройства, приборы и системы электронной техники с учетом заданных требований **ИПКС-2.3.** Проектирует электронные приборы, схемы и устройства различного функционального назначения, выбирая оптимальный вариант, оценивая его достоинства и недостатки					
Знать: Информационное противоборство в современном мире, основные требования к информационной безопасности, в том числе защите гостайны. Доктрину информационной безопасности РФ, классификацию угроз информационной безопасности и средства их предотвращения, парирования, нейтрализации . Криптографические методы защиты информации: шифры докомпьютерной эпохи, симметричные алгоритмы шифрации, шифрация с открытым ключом, электронная цифровая подпись .Построение систем защиты информации при проектировании и конструировании приборов,	Отсутствие усвоения знаний	Недостаточно уверенно понимает и может объяснять полученные знания	На достаточно высоком уровне понимает и может объяснять полученные знания	Отлично понимает и может объяснять полученные знания, демонстрирует самостоятельную познавательную деятельность	Тестирование Промежуточная аттестация

Планируемые результаты обучения	Критерии оценивания результатов				Методы оценивания
	1 критерий – отсутствие усвоения «неудовлетворительно»	2 критерий – не полное усвоение «удовлетворительно»	3 критерий – хорошее усвоение «хорошо»	4 критерий – отличное усвоение «отлично»	
схем и электронных устройств.					
Уметь: Согласовывать технические условия и задания при проектировании и конструировании приборов, схем и электронных устройств . Осуществлять расчет основных показателей качества при проектировании и конструировании приборов, схем и электронных устройств	Не демонстрирует умения	Не уверенно демонстрирует умения	Достаточно уверенно демонстрирует умения	Отлично демонстрирует умения	Выполнение и защита лабораторных работ. Выполнение и защита практических заданий. Промежуточная аттестация
Владеть: Навыками анализа, уточнения и согласования технического задания на проектируемое устройство, прибор и систему электронной техники, определения вариантов построения информационной безопасности устройства, прибора и системы электронной техники и/или его составляющих. Выбором программно-аппаратных средств устройства, прибора или системы электронной техники путем сопоставления различных вариантов с учетом технических и экономических требований.	Не демонстрирует навыки	Не уверенно демонстрирует навыки	Достаточно уверенно демонстрирует навыки	Отлично демонстрирует самостоятельные навыки	Выполнение и защита лабораторных работ. Выполнение и защита практических заданий.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Основная литература

6.1.1. Застела М.Ю. Информационная безопасность в сетях передачи данных: учеб. пособие / М.Ю. Застела, Н.П. Ямпурин. – Арзамас: АГПИ, 2012 г. в 2 частях: 1 часть – 119с. .; 2 часть – 116с.

6.1.2.Смарт Н. Криптография / Н.Смарт; перевод с англ.С.А.Кулешова. – М.: Техносфера, 2006.– 472с.

6.1.3. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студентов ВУЗов/ В.П. Мельников, С.А. Клейменов, А.М. Петраков.- М.: ИЦ «Академия»,2006.

6.2 Дополнительная литература

6.2.1. Ямпурин, Н.П. Основы теории информации и кодирования: Учебное пособие / Н. П. Ямпурин, Д. В. Яблонский. - 2-е изд., перераб. и доп. ; Рекомендовано УМО по математике. - Арзамас : АГПИ, 2011. - 96 с.

6.2.2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks».

6.3 Методические указания, рекомендации и другие материалы к занятиям

6.3.1 Ямпурин Н.П. Информационная безопасность и защита информации: Лабораторный практикум для студентов всех форм обучения направлений 09.03.02-Информационные системы и технологии, 11.04.03-Конструирование и технология электронных средств / Н.П. Ямпурин, Ю.А. Гуськова.; НГТУ им. Р.Е. Алексеева, Арзамасский филиал ННГУ.-Н.Новгород-Арзамас: НГТУ-Арзамасский филиал ННГУ ,2016. -79 с.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая электронные библиотечные и информационно-справочные системы

7.1.1 Электронно-библиотечная система издательства «IPRbooks». Режим доступа: www.iprbookshop.ru.

7.1.2 Электронно-библиотечная система издательства «Лань». Режим доступа: https://e.lanbook.com

7.1.3 Электронная библиотека научных публикаций «eLIBRARY.RU». Режим доступа: http://elibrary.ru.

7.1.4 Научная электронная библиотека «КиберЛенинка». Режим доступа: https://cyberleninka.ru/.

7.1.5 Информационный портал «INGENERYI.INFO». Режим доступа: https://ingeneryi.info.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства необходимого для освоения дисциплины

7.2.1 MATLab Simulink R2011b

7.2.2 MS Office: Excel

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования.

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
ЭБС «IPRbooks»	Специальное мобильное приложение **IPR BOOKS WV-Reader**
ЭБС «Лань»	Синтезатор речи, который воспроизводит тексты книг и меню навигации

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

Учебные аудитории для проведения занятий по дисциплине (модулю), оснащены оборудованием и техническими средствами обучения.

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду АПИ НГТУ.

Таблица 9.1 – Оснащенность аудиторий и помещений для проведения занятий и самостоятельной работы студентов по дисциплине

Наименование аудиторий и помещений для проведения занятий и самостоятельной работы	Оснащенность аудиторий и помещений для проведения занятий и самостоятельной работы
317 - Компьютерный класс г. Арзамас, ул. Калинина, дом 19	Персональный компьютер (Intel Core i3-4130/8 Gb RAM/NVIDIA GeForce GT 730/HDD 1000) с подключением к интернету (11 шт.); Персональный компьютер Экран - (1 шт.); 4. Доска маркерная (1 шт.); 5. Стол компьют. с нишей (11 шт.); 6. Стол для препод. (1 шт.); 7. Стул (23) Посадочных мест - 22.
316 - Кабинет самоподготовки студентов г. Арзамас, ул. Калинина, дом 19	рабочих мест студента – 26 шт; ПК, с выходом на телевизор LG - 1 шт. ПК с подключением к интернету -5шт.

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

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.

Контактная работа проводится в аудиторной и внеаудиторной форме, а также в электронной информационно-образовательной среде института (далее – ЭИОС). В случае проведения части контактной работы по дисциплине в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При преподавании дисциплины, 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, а также материалы для практических занятий находятся в свободном доступе в СДО MOODLE на странице курса и могут быть проработаны студентами до чтения лекций в ходе самостоятельной работы. Это дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала.

На лекциях и практических занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, дискуссионные технологии, технологии 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, как встреч со студентами, так и современных информационных технологий, таких как форум, чат, внутренняя электронная почта СДО MOODLE.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента.

Для оценки знаний, умений и уровня сформированности компетенции в процессе текущего контроля применяется система контроля и оценки успеваемости студентов, представленная в табл. 5.1. Промежуточная аттестация проводится с использованием системы контроля и оценки успеваемости студентов, представленной в табл. 5.2.

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 . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложных и важных положениях изучаемого материала. Материалы лекций являются основой для подготовки обучающихся к практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на занятиях семинарского типа

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Практические (семинарские) занятия обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- развитие умений и навыков в рамках материалу дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению работ, требования к их оформлению, порядок сдачи.

10.4 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.

В процессе самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение основной учебной и справочно-библиографической литературы, представленной в разделе 6.

Для выполнения самостоятельной работы при изучении дисциплины студенты могут использовать специализированные аудитории (см. табл. 9.1), оборудование которых обеспечивает доступ через «Интернет» к электронной информационно-образовательной среде института и электронной библиотечной системе, где располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

10.5 Методические указания по обеспечению образовательного процесса

1. Методические рекомендации по организации аудиторной работы. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/metod_rekom_auditorii.PDF.

2. Методические рекомендации по организации и планированию самостоятельной работы студентов по дисциплине. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/metod_rekom_srs.PDF.

3. Учебное пособие «Проведение занятий с применением интерактивных форм и методов обучения», Ермакова Т.И., Ивашкин Е.Г., 2013 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/provedenie-zanyatij-s-primeneniem-interakt.pdf.

4. Учебное пособие «Организация аудиторной работы в образовательных организациях высшего образования», Ивашкин Е.Г., Жукова Л.П., 2014 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/organizaciya-auditornoj-raboty.pdf.

Дополнения и изменения в рабочей программе дисциплины
на 20____/20____ уч. г.

УТВЕРЖДАЮ:
Директор института:
_____ Глебов В.В.
«____»_____ 20___ г.

В рабочую программу вносятся следующие изменения:

1)

2)

или делается отметка о нецелесообразности внесения каких-либо изменений на данный учебный год

Рабочая программа пересмотрена на заседании кафедры, протокол от _____№ ____

Заведующий кафедрой _____ _____
(подпись) *(ФИО)*

Утверждено УМК АПИ НГТУ, протокол от _____№ _____

Зам. директора по УР _____Шурыгин А.Ю.
(подпись)

Согласовано:

Начальник УО _____Мельникова О.Ю.
(подпись)

(в случае, если изменения касаются литературы):

Заведующая отделом библиотеки _____Старостина О.Н.
(подпись)