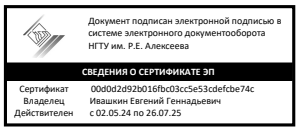
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

Передовая инженерная школа атомного машиностроения
и систем высокой плотности энергии (ПИШ)



УТВЕРЖДАЮ:
Директор ПИШ:
_____ А.В. Тумасов

“21” июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.11 Основы обеспечения информационной и компьютерной безопасности

(индекс и наименование дисциплины по учебному плану)

для подготовки магистров

Направление подготовки: 09.04.01 Информатика и вычислительная техника
(код и направление подготовки)

Направленность: Цифровые технологии управления технологическими процессами атомных станций нового поколения
(наименование программы магистратуры)

Форма обучения: очная

Год начала подготовки 2024

Выпускающая кафедра ВСТ

Кафедра-разработчик ИСУ

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация экзамен
экзамен, зачет с оценкой, зачет

Разработчик: Мокляков В.А., к.т.н.
(ФИО, ученая степень, ученое звание)

Нижний Новгород, 2024 год

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным
образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом МИНОБРНАУКИ РОССИИ

от 19 сентября 2017 № 918 на основании учебного плана принятого УМС НГТУ

протокол от _23.04.2024__ № 14

Рабочая программа одобрена на заседании кафедры разработчика программы протокол от _15.05.24_ № ____9____
Зав. кафедрой к.т.н, доцент, О.П.Тимофеева _____
(подпись)
Программа рекомендована к утверждению ученым советом института _ИРИТ__, где реализуется данная программа
протокол от _ 21.05.24__ № ____4___

Председатель УМС, директор института _____А.В. Мякиньков
(подпись)

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.04.01-ц-11__

Начальник МО _____ Н.Р. Булгакова
(подпись)

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

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью (целями) освоения дисциплины является развитие компетенций в области безопасности систем обработки информации и управления и защиты информации в них
1.2. Задачи освоения дисциплины (модуля):

Обеспечение надежности, безопасности и эффективности автоматизированных систем управления.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина Б1.Б.11 «Основы обеспечения информационной и компьютерной безопасности» включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля).Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 09.04.01 Информатика и вычислительная техника.

код направления подготовки

Дисциплина базируется на дисциплинах математического блока и блока программирования программы бакалавриата, в рамках учебного плана непосредственно базируется на дисциплине «Методы и системы принятия решений на основе искусственного интеллекта».

Дисциплина «Основы обеспечения информационной и компьютерной безопасности» является основополагающей для практики: преддипломная и выполнения выпускной квалификационной работы.

Рабочая программа дисциплины «Основы обеспечения информационной и компьютерной безопасности» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся, по их личному заявлению.

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

Таблица 1- Формирование компетенций дисциплинами

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки магистра			
	1	*2*	*3*	*4*
ОПК-2. *Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач*				
Методы и системы принятия решений на основе искусственного интеллекта				
Алгоритмы обработки сигналов в системах управления				
Основы обеспечения информационной и компьютерной безопасности				
Технологии разработки цифровых сервисов				
Абстрактная алгебра				
Ознакомительная практика				
Выполнение и защита ВКР				
ОПК-5. *Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем*				
Основы обеспечения информационной и компьютерной безопасности				
Аппаратное обеспечение АСУ ТП				
Технологии разработки цифровых сервисов				
Ознакомительная практика				
Выполнение и защита ВКР				
ОПК-8. *Способен осуществлять эффективное управление разработкой программных средств и проектов*				
Системы автоматизации проектирования цифровых систем управления				
Системы контроля и управления атомными станциями				
Основы обеспечения информационной и компьютерной безопасности				
Выполнение и защита ВКР				

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 2

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПВО

Таблица 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**
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ИОПК-2.1. Разрабатывает оригинальные алгоритмы для решения профессиональных задач. ИОПК-2.2. Разрабатывает программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач.	***Знать:*** - алгоритмический аппарат, описывающий взаимодействие информационных процессов в криптосистемах. - социальные аспекты защиты информации, - организационные методы защиты информации.	***Уметь:*** - оценивать риски при проектировании автоматизированных систем в различных областях в части защиты информации, - обосновывать решения в области использовании конкретных криптографических протоколов; - строить защищенные программные комплексы с использованием современных криптографических систем и протоколов.	***Владеть:*** - методами социальной инженерии	Выполнение итогового тестирования и сдача 3 лабораторных работ.	Зачет - 58 вопросов для устного собеседования на экзамене
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ИОПК-5.1. Разрабатывает и модернизирует аппаратное обеспечение информационных и автоматизированных систем ИОПК-5.2.	***Знать:*** -угрозы информационной и компьютерной безопасности; - методы обеспечения целостности	***Уметь:*** - защищать информацию от компьютерных вирусов.	***Владеть:*** - криптографии-ческими методами защиты информации; - основами правовой защиты информации;		

	Разрабатывает и модернизирует программное обеспечение информационных и автоматизированных систем	данных; - модели информационной и компьютерной безопасности		- организационными методами защиты информации.		
ОПК-8. Способен осуществлять эффективное управление разработкой программных средств и проектов	ИОПК-8.1. Осуществляет эффективное управление разработкой программных средств, в том числе планирование, контроль, тестирование. ИОПК-8.2. Осуществляет эффективное управление разработкой проектов.	***Знать:*** - основные криптографические протоколы – правовые нормы в области защиты информации; – закон о защите персональных данных; – отечественный и зарубежный опыт законодательного регулирования информатизации.	***Уметь:*** строить защищенные программные комплексы с использованием современных криптографических систем и протоколов	***Владеть:*** - современными методами обеспечения контроля целостности информации, при её хранении, обработке и передаче – основами правовой защиты информации; – организационными методами защиты информации.		

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. 144 часа, распределение часов по видам работ семестрам представлено в таблице 3.

Таблица 3 - Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		3 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**57**	**57**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**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)	**51**	**51**
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.)	**51**	**51**
Подготовка к экзамену (контроль)	**36**	**36**

5.2. Содержание дисциплины, структурированное по темам

Таблица 4. -Содержание дисциплины, структурированное по темам

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. Основы защиты информации										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 1.1** Основные защиты информации в Российской Федерации, организация защиты информации на предприятии	2				4	Подготовка к лекциям [7.1.1, 7.1.2].			
	Тема 1.2 Основные термины и определения в области защиты информации. Основные нормативные документы в области защиты информации, структура нормативной базы	2				4	Подготовка к лекциям [7.1.1, 7.1.2].	Разбор конкретных ситуаций		
	Итого по 1 разделу	**4**				**8**				
Раздел 2. Основы организации технической защиты информации на предприятии										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 2.1** Основные нормативные документы в области защиты информации, структура нормативной базы.	4				4	Подготовка к лекциям [7.1.1, 7.1.2].	Мозговой штурм		
	Тема 2.2 Основы организации технической защиты информации на	4				5	Подготовка к лекциям [7.1.1, 7.1.2].			

Планируемые (контролируемые) результаты освоения:код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	предприятии									
	Итого по 2 разделу	**8**				**9**				
Раздел 3. Технические каналы утечки информации, характеристика наиболее распространенных угроз безопасности.										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 3.1** Технические каналы утечки информации основные средства контроля и системы защиты информации	4				3	Подготовка к лекциям [7.1.1, 7.1.2].			
	Тема 3.2 Базовая модель угроз безопасности персональных данных	4			1	5	Подготовка к лекциям [7.1.1, 7.1.2].	Разбор конкретных ситуаций		
	Тема лабораторной работы: Определение исходной защищенности ТКС		5			2	Подготовка к лабораторной работе [7.2.6]	Мозговой штурм		
	Итого по 3 разделу	**8**	**5**		**1**	**10**				
Раздел 4. Этапы разработки системы защиты информации, построение модели угроз безопасности информации и модели нарушителя										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 4.** 1. Методика определения актуальных угроз безопасности и создания модели угроз для телекоммуникационных систем.	3				4	Подготовка к лекциям [7.1.1, 7.1.2].			
	Тема 4.2. Методика создания модели нарушителя, нормативные документы ФСБ России	3			1	4	Подготовка к лекциям [7.1.1, 7.1.2].	Мозговой штурм		
	Тема лабораторных работы: «Определение актуальных		6			2	Подготовка к лабораторной работе [7.2.6]	Мозговой штурм		

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					
	угроз безопасности для распределенной ТКС с выходом в сети общего пользования» «Определение типа нарушителя для распределенной ТКС»		6							
	Итого по 3 разделу	**6**	**12**		**1**	**10**				
Раздел 5. Основные требования по защите информации в телекоммуникационной системе										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 5.1.** Требования по защите информации в телекоммуникационной системе	2				4	Подготовка к лекциям [7.1.1, 7.1.2].			
	Тема 5.2. Сертификация и лицензирование в области обеспечения защиты информации	2			1	5	Подготовка к лекциям [7.1.1, 7.1.2].	Разбор конкретных ситуаций		
	Итого по 5 разделу	**4**			**1**	**9**				
Раздел 6. Критерии надежности и эффективности функционирования СЗИ										
ОПК-2 – ИОПК-2.1, 2.2 ОПК-5 – ИОПК-5.1, 5.2 ОПК-8 – ИОПК-8.1, 8.2	**Тема 6.1** Понятие надежности сложных систем. Решения по повышению надежности СЗИ	4			**1**	**5**	Подготовка к лекциям [7.1.1, 7.1.2]			
	Итого по 6 разделу	**4**			**1**	**5**				
	Подготовка к экзамену (контроль)				**2**	**36**				
	Итого за семестр	**34**	**17**		**6**	**51+ 36**				

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

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

Текущий контроль осуществляется для всех форм текущего контроля учебного процесса:

– контроль по темам лекционных занятий,
– отчет по лабораторным занятиям:
– итоговое тестирование по темам лекций.

Для выполнения процедур оценивания составлен фонд оценочных средств, содержащий материалы для оценивания знаний, умений и навыков студентов для текущей и промежуточной аттестации.

1. Вопросы к лабораторной работе №1

1. Типовые объекты информатизации.
2. Понятие угрозы безопасности информации.
3. Состав возможных уязвимых звеньев.
4. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.
5. Порядок разработки модели угроз безопасности, основные этапы.
6. Как определяется исходный уровень защищенности ТКС.

2. Вопросы к лабораторной работе №2

1. Понятие угрозы безопасности информации.
2. Состав возможных уязвимых звеньев.
3. Основные документы, содержащие нормы, требования и рекомендации по разработке модели угроз.
4. Порядок разработки модели угроз безопасности, основные этапы.
5. Определение характерных угроз безопасности для распределенной ТКС.
6. Порядок определения актуальных угроз безопасности для распределенной ТКС.
7. Порядок оформления модели угроз безопасности

3. Вопросы к лабораторной работе №3

1. Понятие угрозы безопасности информации.
2. Состав возможных уязвимых звеньев и возможных атак.
3. Основные документы, содержащие нормы, требования и рекомендации разработке модели нарушителя.
4. Порядок разработки модели нарушителя, основные этапы.
5. Определение типов нарушителя для распределенной ТКС.
6. Порядок определения итогового типа нарушителя для распределенной ТКС.
7. Порядок оформления модели нарушителя

4. Примерный перечень вопросов для экзамена:

1. Основные нормативно-правовые акты по защите конфиденциальной информации.
2. Понятия защищаемая информация, защита информации от утечки.
3. Понятия Защита информации от несанкционированного доступа (НСД), Защита информации от технической разведки, Техническая защита конфиденциальной информации (ТЗКИ).

4. Внешние и внутренние источники угроз безопасности информации.
5. Понятие классификации объектов информатизации.
6. Типовые объекты информатизации.
7. Понятие угрозы безопасности информации.
8. Состав возможных уязвимых звеньев.
9. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.
10. Принципы разграничения доступа.
11. Дайте определение технического канала утечки информации.
12. В чем отличие основных технических средств (ОТСС) от вспомогательных технических средств и систем (ВТСС)?
13. Дайте определение контролируемой зоны (КЗ).
14. Определения аттестации объектов информатизации по требованиям безопасности информации и сертификации, что общего, в чем различие.
15. Понятие объекта информатизации и автоматизированной системы.
16. Понятия - информация, документ, безопасность информации.
17. Понятия – техническая защита конфиденциальной информации, защита информации от НСД.
18. Понятия классификации и типизации, основные составляющие.
19. Признаки классификации.
20. Принципы организации ТЗИ.
21. Общий алгоритм организации ТЗИ на объекте информатизации.
22. Порядок организации ТЗИ на этапе оценки обстановки.
23. Объекты защиты на объекте информатизации.
24. Понятие инвентаризации и категорирования, основные задачи инвентаризации.
25. Понятие инвентаризации и категорирования.
26. Источники угроз безопасности информации.
27. Дать понятие актуальной угрозыбезопасности информации.
28. Уязвимости, используемые в атаках.
29. Классификация угроз безопасности информации.
30. Понятия цели и задачи защиты информации.
31. Понятие программного (программно-математического) воздействия, группы угроз ПМВ.
32. Классы защиты информации в СВТ.
33. Классы защиты информации в АС.
34. Порядок организации ТЗИ на этапе определения замысла защиты.
35. Стратегии защиты информации в компьютерной сети.
36. Принципы разграничения доступа.
37. Общая классификация способов, мер и средств защиты от НСД.
38. Технологии (способы) создания доверенной среды.
39. Содержание замысла защиты информации.
40. Содержание концепции защиты информации.
41. Меры и средства защиты от физического доступа.
42. Меры и средства защиты информации от утечки по ПЭМИН.
43. Меры и средства защиты от НСД с применением программных и программно-аппаратных средств.
44. Меры и средства защиты от ПМВ.
45. Меры и средства защиты информации от техногенных угроз.
46. Порядок выбора целесообразных мер и средств защиты.
47. Понятие системы защиты информации на объекте информатизации.
48. Документы по организации ТЗИ на объекте информатизации.

49. На основании каких документов разрабатывается Модель угроз безопасности информации.
50. Порядок разработки модели угроз безопасности, основные этапы.
51. Как определяется исходный уровень защищенности ИСПДн.
52. Порядок разработки модели нарушителя, основные этапы.
53. Нормативные документы ФСБ России по защите персональных данных и разработке модели нарушителя.
54. Нормативные документы по разработке ТЗ на создание АС в защищенном исполнении.
55. Понятие надежности, отказа, критериев отказа.
56. Дерево отказов, его назначение.
57. Нормирование показателей надежности.
58. Виды показателей надежности и безотказности.
59. Виды показателей долговечности и ремонтопригодности.
60. Классификация объектов по показателям и методам оценки надежности.

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

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

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

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

Таблица 6. – 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
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ИОПК-2.1. Разрабатывает оригинальные алгоритмы для решения профессиональных задач. ИОПК-2.2. Разрабатывает программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач.	Подготовка недостаточная, требует дополнительного изучения материала, дает ошибочные ответы, как на теоретические вопросы, так и на практические вопросы.	Знает основной материал с рядом заметных погрешностей.Владеет фрагментарными знаниями методики разработки интеллектуальных методов для решения задач информационной безопасности, допускает существенные ошибки в выполнении лабораторных работ, которые исправляет при помощи преподавателя, затрудняется формулировать практические результаты.	Знает основной материал с незначительными погрешностями, способен системно излагать методологию разработки интеллектуальных методов для решения задач информационной безопасности, при этом допускает единичные ошибки в адаптации алгоритмов к новым областям знаний.	Знает основной и дополнительный материал, без ошибок и погрешностей, способен решать стандартные задачи и разрабатывать оригинальные алгоритмы и программные средствадля обеспечения информационной безопасности
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ИОПК-5.1. Разрабатывает и модернизирует аппаратное обеспечение информационных и автоматизированных систем. ИОПК-5.2. РМодернизирует программное	Наличие грубых ошибок в основном материале, неумение проводить разработку и модернизацию аппаратного обеспечения информационных и автоматизированных систем	Способностьрешения основных стандартных задач с существенными ошибками, слабое владение методами разработки и неумение проводить модернизацию аппаратного обеспечения информационных и автоматизированных систем	Способность решения всех стандартных задач с незначительными погрешностями, владение методами разработки и способностью проводить модернизацию аппаратного	Способность решения стандартных и некоторых нестандартных задач, в том числе новые подходы к разработке и модернизации аппаратного обеспечения информационных и автоматизированных

	обеспечение информационных и автоматизированных систем.			обеспечения	систем
ОПК-8. Способен осуществлять эффективное управление разработкой программных средств и проектов	ИОПК-8.1. Осуществляет эффективное управление разработкой программных средств, в том числе планирование, контроль, тестирование. ИОПК-8.2. Осуществляет эффективное управление разработкой проектов.	Наличие грубых ошибок в основном материале, неумение руководить разработкой программных средств и проектов	Способностьрешения основных стандартных задач с существенными ошибками, низкая способность руководить разработкой программных средств и проектов	Способность решения всех стандартных задач с незначительными погрешностями, неуверенное руководство разработкой программных средств и проектов	Способность решения стандартных и некоторых нестандартных задач, умение руководить разработкой программных средств и проектов

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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература,печатные издания библиотечного фонда

7.1.1. 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.
7.1.2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тум-бинская, 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
7.1.3. 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.
7.1.4. Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.
7.1.5. Алексеев Е.Б., Гордиенко В.Н., Крухмалев В.В., Моченов А.Д., Тверецкий М.С. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей. Под ред. В Гордиенко В.Н. и Тверецкого М.С. - М.: Горячая линия – Телеком, 2008. – 392 с.
7.1.6. Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

7.2. Справочно-библиографическая литература

7.2.1. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика. – М.: Радио и связь, 2001. – 504 с.

7.2.2. Байхельд Ф., Франкен П., Надежность и техническое обслуживание. Математический подход. – И.: Радио и связь, 1988.
7.2.3. Барсуков В. С., Водолазкий В. В. Современные технологии безопасности. Интегральный подход. М.: «Нолидж», 2000. - 496 с.
7.2.4. Ксенофонтов С.Н., Портнов Э.Л. Направляющие системы электросвязи. Сборник задач: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. - 268 с.
7.2.5. Колинько Т.А. Измерения в цифровых системах связи. Практическое руководство. – К.: ВЕК+, К.: НТИ 2002. - 320 с.
7.2.6. Малюк А.А., Пазинин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.
7.2.7. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. Пер. с англ. / Под ред. В.И. Журавлева. – М.: Радио и связь, 2000. – 520 с.
7.2.8. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.

7.3 Методические указания, рекомендации и другие материалы к занятиям

7.3.1. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность и защита информации» для студентов направления подготовки 09.04.01 «Информатика и вычислительная техника» дневной формы обучения / НГТУ; Сост.: Мокляков В.А., Н.Новгород, 2021, 21 с.

8. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Таблица 7. Перечень ресурсов сети Интернет

№	Наименование ЭБС	Ссылка к ЭБС
1	Polpred.com. Обзор СМИ. Полнотекстовая, многоотраслевая база данных (БД)	http://polpred.com/
2	Электронно-библиотечная система Znanium.com	http://znanium.com/

8.2. Перечень программного обеспечения и информационных справочных систем (при необходимости)

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

Таблица 8. – 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/)

Таблица 9 - Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка, по которой осуществляется доступ к ЭБС
1	2	3
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://urait.ru/
4	КонсультантПлюс [Электронный ресурс]: Справочная правовая система. -	http://www.consultant.ru/
5	TNT-ebook	https://www.tnt-ebook.ru/

Таблица 10 - 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.gost.ru/portal/gost//home/standarts
2	Электронная база избранных статей по философии	http://www.philosophy.ru/
3	Единый архив экономических и социологических данных	http://sophist.hse.ru/data_access.shtml
4	Базы данных Национального совета по оценочной деятельности	http://www.ncva.ru
5	Справочная правовая система «КонсультантПлюс»	доступ из локальной сети
6	Информационно-справочная система «Техксперт»	доступ из локальной сети

9. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 11 указанперечень 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/

Таблица 11 - 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	**2**	**3**
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

Адаптированные образовательные программы (АОП) в образовательной организации не реализуются в связи с отсутствием в контингенте обучающихся лиц с ограниченными возможностями здоровья (ОВЗ), желающих обучаться по АОП. Согласно Федеральному Закону об образовании 273-ФЗ от 29.12.2012 г. ст. 79, п.8 "Профессиональное обучение и профессиональное образование обучающихся с ограниченными возможностями здоровья осуществляются на основе образовательных программ, адаптированных при необходимости для обучения указанных обучающихся". АОП разрабатывается по каждой направленности при наличии заявлений от обучающихся, являющихся инвалидами или лицами с ОВЗ и изъявивших желание об обучении по данному типу образовательных программ.

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

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения, состав которых определен в данном разделе.

В таблице 12 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;

-помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

Таблица 12 - Оснащенность аудиторий и помещений для проведения учебных занятий и самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для проведения учебных занятий и самостоятельной работы	Оснащенностьаудиторий помещений и помещений	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	№6567 аудитория для проведения лекционных и практических занятий, г. Нижний Новгород, Казанское шоссе, д.12	ПК на базе процессора Intel – 12 шт. Терминалы «Эльбрус 801-miniPC» ТВГИ.466256.011 – 2 шт. Источники бесперебойного питания IpponBackBasic 1500 – 2 шт. Высокопроизводительный сервер.	UbuntuLinux(свободное ПО) VirtualBox(свободное ПО) Комплект разработчика для ЗОСРВ «Нейтрино» (КПДА.96901-01, заводской номер 22027) Комплект разработчика для ЗОСРВ «Нейтрино-Э» (КПДА.10965-01, заводской номер 22007) ЗОСРВ «Нейтрино» (КПДА.10964-01, заводской номер 22178) ЗОСРВ «Нейтрино-Э» (КПДА.96904-01, заводской номер 22002)

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

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

При преподавании дисциплины «Основы обеспечения информационной и компьютерной 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, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

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

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

Для оценки знаний, умений, навыков и уровня сформированностикомпетенции применяетсятрадиционнаясистема контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме экзаменас 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.

11.2 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 (Таблица 4). 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.

В ходе лекционных занятий рекомендуется вести конспектирование учебного материала.

11.3 Методические указания по освоению дисциплины на лабораторных работах

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

При оценивании лабораторных работ учитывается следующее:

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

11.4. 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.

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 (указано в таблице 12). В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

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

12. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

12.1 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 защиту лабораторных работ.

Типовые задания для лабораторных работ

Типовые задания для лабораторных работ приведены в учебно-методических указаниях по проведению лабораторных работ.

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

Перечень вопросов и заданий для подготовки и проведения экзамена, для оценки сформированности компетенций (ОПК-2, ИОПК-2.1, 2.2):

1. Объекты защиты на объекте информатизации.
2. Понятие инвентаризации и категорирования, основные задачи инвентаризации.
3. Понятие инвентаризации и категорирования.
4. Источники угроз безопасности информации.

5. Дать понятие актуальной угрозы безопасности информации.
6. Уязвимости, используемые в атаках.
7. Классификация угроз безопасности информации.
8. Понятия цели и задачи защиты информации.
9. Понятие программного (программно-математического) воздействия, группы угроз ПМВ.
10. Классы защиты информации в СВТ.
11. Классы защиты информации в АС.
12. Порядок организации ТЗИ на этапе определения замысла защиты.
13. Стратегии защиты информации в компьютерной сети.
14. Принципы разграничения доступа.
15. Общая классификация способов, мер и средств защиты от НСД.
16. Технологии (способы) создания доверенной среды.
17. Содержание замысла защиты информации.
18. Содержание концепции защиты информации.
19. Меры и средства защиты от физического доступа.
20. Меры и средства защиты информации от утечки по ПЭМИН.
21. Меры и средства защиты от НСД с применением программных и программно-аппаратных средств.

Перечень вопросов и заданий для подготовки и проведения экзамена, для оценки сформированности компетенций (ОПК-5, ИОПК-5.1, 5.2):

1. Понятие угрозы безопасности информации.
2. Состав возможных уязвимых звеньев.
3. Основные документы, содержащие нормы, требования и рекомендации по ТЗИ.
4. Принципы разграничения доступа.
5. Дайте определение технического канала утечки информации.
6. В чем отличие основных технических средств (ОТСС) от вспомогательных технических средств и систем (ВТСС)?
7. Дайте определение контролируемой зоны (КЗ).
8. Определения аттестации объектов информатизации по требованиям безопасности информации и сертификации, что общего, в чем различие.
9. Понятие объекта информатизации и автоматизированной системы.
10. Понятия - информация, документ, безопасность информации.
11. На основании каких документов разрабатывается Модель угроз безопасности информации.
12. Порядок разработки модели угроз безопасности, основные этапы.
13. Как определяется исходный уровень защищенности ИСПДн.
14. Порядок разработки модели нарушителя, основные этапы.
15. Нормативные документы ФСБ России по защите персональных данных и разработке модели нарушителя.
16. Нормативные документы по разработке ТЗ на создание АС в защищенном исполнении.

Перечень вопросов и заданий для подготовки и проведения экзамена, для оценки сформированности компетенций (ОПК-8, ИОПК-8.1, 8.2):

1. Основные нормативно-правовые акты по защите конфиденциальной информации.
2. Понятия защищаемая информация, защита информации от утечки.

3. Понятия Защита информации от несанкционированного доступа (НСД), Защита информации от технической разведки, Техническая защита конфиденциальной информации (ТЗКИ).
4. Внешние и внутренние источники угроз безопасности информации.
5. Понятие классификации объектов информатизации. Понятия – техническая защита конфиденциальной информации, защита информации от НСД.
6. Понятия классификации и типизации, основные составляющие.
7. Признаки классификации.
8. Принципы организации ТЗИ.
9. Общий алгоритм организации ТЗИ на объекте информатизации.
10. Порядок организации ТЗИ на этапе оценки обстановки.
11. Понятие надежности, отказа, критериев отказа.
12. Дерево отказов, его назначение.
13. Нормирование показателей надежности.
14. Виды показателей надежности и безотказности.
15. Виды показателей долговечности и ремонтопригодности
16. Классификация объектов по показателям и методам оценки надежности.
17. Меры и средства защиты от ПМВ.
18. Меры и средства защиты информации от техногенных угроз.
19. Порядок выбора целесообразных мер и средств защиты.
20. Понятие системы защиты информации на объекте информатизации.
21. Документы по организации ТЗИ на объекте информатизации.
22. Типовые объекты информатизации.

Форма проведения промежуточной аттестации по дисциплине: экзамен.

Пример оформления экзаменационного билета:

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. Р.Е.Алексеева

Кафедра ИСУ

Дисциплина Основы обеспечения информационной и компьютерной безопасности

Э К З А М Е Н А Ц И О Н Н Ы Й Б И Л Е Т № 1

1. Понятие инвентаризации и категорирования, основные задачи инвентаризации.
2. Нормативные документы ФСБ России по защите персональных данных и разработке модели нарушителя.
3. Меры и средства защиты информации от техногенных угроз.

Зав.кафедрой ИСУЭкзаменатор

“ ..... “ .....202_ г.

Весь комплект экзаменационных билетов по дисциплине хранится на кафедре