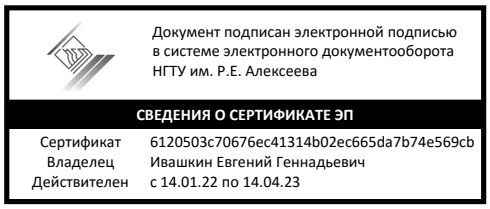
МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

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



УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“_____”_____2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.8_ Безопасность и защита информации
(индекс и наименование дисциплины по учебному плану)
для подготовки магистров

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность: Диагностические и информационно-поисковые системы

Форма обучения: очная

Год начала подготовки 2020,2021

Выпускающая кафедра ВСТ

Кафедра-разработчик ИСУ

Объем дисциплины 108/3
часов/з.е

Промежуточная аттестация экзамен

Разработчики: Мокляков В.А., к.т.н., доцент

Нижний Новгород

2021

Рецензент _____ Хранилов В.П. д.т.н., профессор кафедры КТПП

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 года № 918 на основании учебного плана принятого УМС НГТУ

протокол от __17.12.20__ № 5

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

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 10.06.2021_____№____1

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.04.01-д-8____
Начальник МО _____

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

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 4

1.1 Цель освоения дисциплины 4
1.2 Задачи освоения дисциплины (модуля) 4

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 4

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) 5

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам 7
4.2 Содержание дисциплины, структурированное по темам 8

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ. 11

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности 11
5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания 13

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 15

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 16

7.1 Перечень информационных справочных систем 16
7.2 Перечень свободно распространяемого программного обеспечения 16
7.3 Перечень современных профессиональных баз данных и информационных справочных систем 17

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ 17

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ 17

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 19

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии 19
10.2 Методические указания для занятий лекционного типа 20
10.3 Методические указания по освоению дисциплины на лабораторных работах 20
10.4 Методические указания по самостоятельной работе обучающихся 20

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ 21

11.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости 21
11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине: 21

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области безопасности систем обработки информации и управления и защиты информации в них.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Безопасность и защита информации» способствует подготовке студентов к решению следующих профессиональных задач:

1. Сбор, обработка, анализ и систематизация научно-технической информации по теме исследования, выбор методик и средств решения задачи обеспечения информационной безопасности.
2. Определение состава защищаемой информации и объектов защиты, выявление угроз, источников воздействия нарушителей, возможных потерь;
3. Разработка модели угроз безопасности, которая включает определение вероятностей угроз и способов их осуществления, оценка рисков, связанных с их осуществлением, а также проведение оценки возможного ущерба;
4. Построение модели нарушителя, определяемой на основе обследования ресурсов системы и способов их использования;
5. Определение требований безопасности, по результатам анализа угроз безопасности;
6. Осуществление выбора компонентов СЗИ и определение условий их функционирования;
7. Разработка мер обеспечения информационной безопасности организационного и программно-технического уровня, предпринимаемых для реализации СЗИ;
8. Организация системы управления и контроля функционирования СЗИ, оценка эффективности созданной СЗИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Безопасность и защита информации» Б1.Б.8 включена в обязательный перечень дисциплин в рамках базовой части Блока 1, установленного ФГОС ВО, и является обязательной для всех профилей направления подготовки 09.04.01 Информатика и вычислительная техника.

Дисциплина базируется на дисциплинах математического блока и блока программирования программы бакалавриата по направлению 09.03.01 «Информатика и вычислительная техника», в рамках учебного плана непосредственно базируется на дисциплине «Современные проблемы информатики и вычислительной техники».

Дисциплина «Безопасность и защита информации» является основополагающей для практики: преддипломная и выполнения выпускной квалификационной работы.

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

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»			
	1	*2*	*3*	*4*
ОПК-2 *Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач*				
Введение в искусственный интеллект				
Современные проблемы информатики и вычислительной техники				
Проектирование интеллектуальных систем				
Современные методы оптимизации и численные методы				
Параллельные методы и алгоритмы				
Ознакомительная практика				
Безопасность и защита информации				
Выполнение и защита ВКР				
ОПК-6 *Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования*				
Технология разработки программного обеспечения				
Безопасность и защита информации				
Архитектура параллельных вычислительных систем				
Параллельные методы и алгоритмы				
Основы проектирования САПР				
Выполнение и защита ВКР				

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
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	***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-6. Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ИОПК-6.1. Разрабатывает компоненты программно-аппаратных комплексов обработки информации	***Знать:*** основные криптографические протоколы.	***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		

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3зач.ед. 108 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

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

Вид учебной работы	Трудоёмкость в час	
	Всего час.	В т.ч. по семестрам
		3 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**40**	**40**
1.1 Аудиторная работа, в том числе:	**34**	**34**
занятия лекционного типа (Л)	17	17
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**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)	**32**	**32**
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.)	**32**	**32**
Подготовка к экзамену (контроль)	**36**	**36**

4.2Содержание дисциплины, структурированное по темам

Таблица 4.2-Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения:код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Основы защиты информации										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 1.1** Основные защиты информации в Российской Федерации, организация защиты информации на предприятии	1				2	Подготовка к лекциям [6.1.1, 6.1.2].			
	Тема 1.2 Основные термины и определения в области защиты информации. Основные нормативные документы в области защиты информации, структура нормативной базы	1				2	Подготовка к лекциям [6.1.1, 6.1.2].	Разбор конкретных ситуаций		
	Итого по 1 разделу	**2**				**4**				
Раздел 2. Основы организации технической защиты информации на предприятии										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 2.1** Основные нормативные документы в области защиты информации, структура нормативной базы.	2				2	Подготовка к лекциям [6.1.1, 6.1.2].	Мозговой штурм		
	Тема 2.2 Основы организации технической защиты информации на предприятии	2				5	Подготовка к лекциям [6.1.1, 6.1.2].			

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					
	Итого по 2 разделу	**4**				**7**				
Раздел 3. Технические каналы утечки информации, характеристика наиболее распространенных угроз безопасности.										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 3.1** Технические каналы утечки информации основные средства контроля и системы защиты информации	2				2	Подготовка к лекциям [6.1.1, 6.1.2].			
	Тема 3.2 Базовая модель угроз безопасности персональных данных	2			1	5	Подготовка к лекциям [6.1.1, 6.1.2].	Разбор конкретных ситуаций		
	Тема лабораторной работы: Определение исходной защищенности ТКС		5				Подготовка к лабораторной работе [6.1.10]	Мозговой штурм		
	Итого по 3 разделу	**4**	**5**		**1**	**7**				
Раздел 4. Этапы разработки системы защиты информации, построение модели угроз безопасности информации и модели нарушителя										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 4.** 1. Методика определения актуальных угроз безопасности и создания модели угроз для телекоммуникационных систем.	1,5				2	Подготовка к лекциям [6.1.1, 6.1.2].			
	Тема 4.2. Методика создания модели нарушителя, нормативные документы ФСБ России	1,5			1	4	Подготовка к лекциям [6.1.1, 6.1.2].	Мозговой штурм		
	Тема лабораторных работы: «Определение актуальных угроз безопасности для распределенной ТКС с		6				Подготовка к лабораторной работе [6.1.10]	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					
	выходом в сети общего пользования» «Определение типа нарушителя для распределенной ТКС»		6							
	Итого по 3 разделу	**3**	**12**		**1**	**6**				
Раздел 5. Основные требования по защите информации в телекоммуникационной системе										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 5.1.** Требования по защите информации в телекоммуникационной системе	1				3	Подготовка к лекциям [6.1.1, 6.1.2].			
	Тема 5.2. Сертификация и лицензирование в области обеспечения защиты информации	1			1	3	Подготовка к лекциям [6.1.1, 6.1.2].	Разбор конкретных ситуаций		
	Итого по 5 разделу	**2**			**1**	**6**				
Раздел 6. Критерии надежности и эффективности функционирования СЗИ										
ОПК-2 – ИОПК-2.1 ОПК-6 – ИОПК-6.1	**Тема 6.1** Понятие надежности сложных систем. Решения по повышению надежности СЗИ	2				**2**	Подготовка к лекциям [6.1.1, 6.1.2]			
	Итого по 6 разделу	**2**			**1**	**2**				
	Подготовка к экзамену (контроль)				**2**	**36**				
	Итого за семестр	**17**	**17**		**6**	**32**				

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

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

Для выполнения процедур оценивания составлен 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 угрозы безопасности 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.

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

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

При промежуточном контроле успеваемость 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 5.4–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	Подготовка недостаточная и требует дополнительного изучения материала, дает ошибочные ответы, как на теоретические вопросы, так и на дополнительные 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 нестандартных задачи
ОПК-6. Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ИОПК-6.1. Разрабатывает компоненты программно-аппаратных комплексов обработки информации	Наличие грубых ошибок в основном материале	Способность решения основных стандартных задач с существенными ошибками	Способность решения всех стандартных задач с незначительными погрешностями	Способность решения стандартных и некоторых нестандартных задач

Таблица 5.5 - Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.

6.1.2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. 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

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

6.1.4. Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

6.1.5. 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.

6.1.6. 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.

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

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

6.2.2. Байхельд Ф., Франкен П., Надежность и техническое обслуживание. Математический подход. – И.: Радио и связь, 1988.

6.2.3. Барсуков В. С., Водолазкий В. В. Современные технологии безопасности. Интегральный подход. М.: «Нолидж», 2000. - 496 с.

6.2.4. Ксенофонтов С.Н., Портнов Э.Л. Направляющие системы электросвязи. Сборник задач: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. - 268 с.

6.2.5. Колинько Т.А. Измерения в цифровых системах связи. Практическое руководство. – К.: ВЕК+, К.: НТИ 2002. - 320 с.

6.2.6. Малюк А.А., Пазинин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с

6.3 Перечень журналов по профилю дисциплины:

6.3.1. 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.

6.3.2. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.

6.4 Методические указания, рекомендации и другие материалы к занятиям

6.3.3. Метод. 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.: Д.В. Мокляков В.А., Н.Новгород, 2021, 21 с.

Методические указания по выполнению лабораторных работ по дисциплине «Безопасность и защита информации» в электронном варианте отправляются на электронные адреса групп.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

7.1 Перечень информационных справочных систем

Таблица 7.1 -Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Лань	https://e.lanbook.com/
2	Юрайт	https://biblio-online.ru/

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
-	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html)
	Linux (https://www.linux.com/)
	OpenOffice (FreeWare) https://www.openoffice.org/ru/
	JDK 8 и выше (https://adoptopenjdk.net/)
	Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework)
	Eclipse (https://www.eclipse.org/) Intellij Idea (https://www.jetbrains.com/ru-ru/idea/)
	git (https://git-scm.com/), github (https://github.com/)
	Maven (https://maven.apache.org/), Gradle (https://gradle.org/)

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
	Редактор блок-схем (https://app.diagrams.net/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4– Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	2	3
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/accenv/

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

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

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);

- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы магистратуры и проведения лабораторных работ для студентов очного обучения, включает в себя:

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

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

мультимедийный проектор BenQ PB6240,

ноутбук Lenovo V130-151KB,

стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.

Пакеты ПО (лицензионное):

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

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Linux Ubuntu 20.04 (https://releases.ubuntu.com/20.04/)
- JDK 8 и выше (https://adoptopenjdk.net/);
- Фреймворк Java Spring 5(https://spring.io/projects/spring-framework)
- Intellij Idea (https://www.jetbrains.com/ru-ru/idea/)
- git (https://git-scm.com/)
- Maven (https://maven.apache.org/)
- Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/)

Также, для самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенностьаудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	**6421** учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 12	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе AMD Athlon 2.8Ггц, 4 Гб ОЗУ, 250 ГБ HDD, монитор 19” – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• Microsoft Windows7 (подписка DreamSpark Premium, договор №Tr113003 от 25.09.14) • Gimp 2.8 (свободное ПО, лицензия GNU GPLv3); • Microsoft Office Professional Plus 2007 (лицензия № 42470655); • OpenOffice 4.1.1 (свободное ПО, лицензия ApacheLicense 2.0) • AdobeAcrobatReader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNU LGPL); Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021).

	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	• Проектор Accer – 1шт; • ПК на базе IntelCoreDuo 2.93 ГГц, 2 Гб ОЗУ, 320 Гб HDD, монитор Samsung 19` – 11 шт.. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14); • Microsoft Office (лицензия № 43178972); • Adobe Design Premium CS 5.5.5 (лицензия № 65112135); • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNULGPL); • Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021) • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018); Gimp 2.8 (свободное ПО, лицензия GNUGPLv3)

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

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

При преподавании дисциплины «Безопасность и защита информации», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

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

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

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется традиционная система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с заданиями, вопросами, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной

программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

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

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

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 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 подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

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

10.4 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных вРазделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Для текущего контроля знаний студентов по дисциплине проводится комплексная оценка знаний, включающая защиту лабораторных работ.

11.1.1. Типовые задания для лабораторных работ

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

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

11.2.1.Типовые вопросы для промежуточной аттестации в форме 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 угрозы безопасности 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.

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

УТВЕРЖДАЮ:
Директор института ИРИТ

_____
“____”_____2021 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.8 Безопасность и защита информации**»**
индекс по учебному плану, наименование

для подготовки бакалавров/ специалистов/ **магистров**
Направление: {шифр – название } 09.04.01 Информатика и вычислительная техника
Направленность: Диагностические и информационно-поисковые системы
Форма обучения очная
Год начала подготовки:2021

Курс 2
Семестр 3
В рабочую программу не вносятся изменения. Программа актуализирована для 2021 г. начала подготовки.

Разработчик (и): __к.т.н. Мокляков В.А._____
(ФИО, ученая степень, ученое звание)
«__»_____20_ _г.
Рабочая программа пересмотрена и одобрена на заседании кафедры ВСТ
_____ протокол № _____ от «__» _____20__г.

Заведующий кафедрой _____

Лист актуализации принят на хранение:

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

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