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

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

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“_10_” __июня___2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.1 Криптографические методы в информационных технологиях
(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность: Вычислительные машины, комплексы, системы и сети

Форма обучения: очная, очно-заочная, заочная

Год начала подготовки 2020, 2021

Выпускающая кафедра ВСТ

Кафедра-разработчик ВСТ

Объем дисциплины 72 / 2
часов/з.е

Промежуточная аттестация зачет

Разработчик: Жаринов В.Ф., к.т.н., доцент

Нижний Новгород, 2021

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки09.03.01Информатика и вычислительная техника, утвержденного приказом МИНОБРНАУКИ РОССИИ от 19 сентября 2017 года № 929 на основании учебного плана принятого УМС НГТУ

протокол от __10.06.2021_ №__6__

Рабочая программа одобрена на заседании кафедры ВСТ протокол от __12.05.2021__ № _10__

Зав. кафедрой д.т.н, доцент, Жевнерчук Д.В. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от10.06.2021_ №__1

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.03.01-Ф-1

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. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПВО 6

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5.1 Распределение трудоёмкости дисциплины по видам работ по семестрам 6
5.2 Содержание дисциплины, структурированное по темам 9

6. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ. 24

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности 24
6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания 24

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 26

8. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 26

8.1 Перечень информационных справочных систем 27
8.2 Перечень свободно распространяемого программного обеспечения 27
8.3 Перечень современных профессиональных баз данных и информационных справочных систем 27

9. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ 27

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ 28

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 29

11.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии 29
11.2 Методические указания для занятий лекционного типа 30
11.3Методические указания по освоению дисциплины на лабораторных работах 30
11.4Методические указания по освоению дисциплины на курсовой работе 30
11.5 Методические указания по самостоятельной работе обучающихся 30

12. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ 31

12.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости 31

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области криптографических методов в информационных технологиях, освоение практических методов и средств решения задач криптографической защиты информации.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Криптографические методы в информационных технологиях» способствует подготовке студентов к решению следующих профессиональных задач:

1. Разработка программного обеспечения с элементами криптографии;
2. Анализ программного обеспечения на защищённость с точки зрения криптографии;
3. Разработка криптографических алгоритмов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Криптографические методы в информационных технологиях» ФТД.1 включена в список факультативных дисциплин. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП.

Дисциплина базируется на дисциплинах программы бакалавриата по направлению «Информатика и вычислительная техника» профиля «Вычислительные машины, комплексы, системы и сети». Предшествующими курсами, на которых непосредственно базируется дисциплина «Криптографические методы в информационных технологиях», являются:

- «Информатика»,
- «Программирование»,
- «Теоретические основы алгоритмизации»,
- «Алгоритмы и структуры данных»,
- «Дискретные структуры».

Дисциплина «Криптографические методы в информационных технологиях» является основополагающей для изучения следующих дисциплин: «Организация и проектирование информационных систем», а также для преддипломной практики и выполнения ВКР.

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

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»							
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
ПКС-1. Способен разрабатывать модели компонентов и алгоритмы функционирования вычислительной техники и автоматизированных систем								
Системный анализ и принятие решений					■			
Основы теории управления							■	
Системы автоматизации проектирования							■	
Программирование	■	■						
Методы и средства обработки сигналов					■			
Исследование операций					■			
Вычислительная математика				■				
Численные методы в АСО и У				■				
Теоретические основы алгоритмизации		■						
Математическая логика и теория алгоритмов		■						
Дискретные структуры	■							
Теория графов и дискретная математика	■							
Информационные модели построения АСО и У			■					
Машинное обучение				■				
Технологии программирования				■				
Параллельные вычисления					■			
Методы Data Mining							■	
Основы теории интеллектуальных вычислительных систем								■
Моделирование систем								■
Цифровые устройства и ПЛИС					■			
Криптографические методы в информационных технологиях						■		
Технологическая (проектно-технологическая) практика				■				
Практика по получению профессиональных умений и опыта профессиональной деятельности						■		
Преддипломная практика								■
Выполнение и защита ВКР								■

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

Таблица 4.1- Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ПКС-1. Способен разрабатывать модели компонентов и алгоритмы функционирования вычислительной техники и автоматизированных систем	ИПКС-1.2. Разрабатывает алгоритмы функционирования вычислительной техники и автоматизированных систем	**Знать:** - типовые шифры замены и перестановки; - частотные характеристики языков и их использование в криптоанализе; - требования к шифрам и основные характеристики шифров; - принципы построения современных шифрсистем; - типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы.	**Уметь:** - выполнить постановку задач криптоанализа и указать подходы к их решению; - использовать основные математические методы, применяемые в анализе типовых криптографических алгоритмов; - применять полученные знания к различным предметным областям.	**Владеть:** - навыками использования основных типов шифров и криптографических алгоритмов; - методами криптоанализа простейших шифров; - навыками применения современной научно-технической литературы в области криптографической защиты.	Выполнение сквозного индивидуального задания – 20 вариантов	Вопросы для устного собеседования – 20 билетов

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 2 зач. ед. 72 часа, распределение часов по видам работ семестрам представлено в таблицах 5.1-5.3.

Таблица 5.1 - 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**
		6 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**72**	**72**
1. Контактная работа:	**38**	**38**
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	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		

текущий контроль, консультации по дисциплине		
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**34**	**34**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	26	26
Подготовка к экзамену (контроль)		
Подготовка к зачёту/ зачёту с оценкой (контроль)	8	8

Таблица 5.2 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очно-заочного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		9 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**72**	**72**
1. Контактная работа:	**22**	**22**
1.1 Аудиторная работа, в том числе:	**18**	**18**
занятия лекционного типа (Л)	9	9
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	9	9
1.2 Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине		
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**50**	**50**
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.)	40	40
Подготовка к экзамену (контроль)		
Подготовка к зачёту/ зачёту с оценкой (контроль)	10	10

Таблица 5.3 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов заочного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по курсам**
		3 курс
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**72**	**72**
1. Контактная работа:	**20**	**20**
1.1 Аудиторная работа, в том числе:	**16**	**16**
занятия лекционного типа (Л)	8	8
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	8	8
1.2 Внеаудиторная, в том числе	**4**	**4**

курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине		
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**48**	**48**
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.)	48	48
Подготовка к экзамену (контроль)		
Подготовка к зачёту/ зачёту с оценкой (контроль)	4	4

5.2Содержание дисциплины, структурированное по темам

Таблица 5.4 - Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Введение в криптографические методы										
ПКС-1- ИПКС-1.2.	**Тема 1.1** Основные определения. Задачи и современные приложения криптографии. Особенности применения криптографических методов в информационных технологиях. Классификация криптографических систем. Основные определения.	1				2	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 1.2 Определение криптографического алгоритма и протокола. Виды протоколов. Понятие нарушителя. Разновидности атак на протоколы. Условная и безусловная секретность. Криптографическая стойкость. Основные понятия теории передачи информации: энтропия и неопределенность, норма языка, абсолютная норма языка, энтропия криптосистемы, расстояние уникальности. Сложность криптоанали-	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	тической атаки									
	Тема лабораторной работы: “Симметричные криптосистемы”		6				Подготовка к лабораторной работе	Видеоконференция		
	Итого по 1 разделу	**3**	**6**		**2**	**5**				
Раздел 2. Типы криптографических систем										
ПКС-1- ИПКС-1.2.	**Тема 2.1** Определение и классификация симметричных криптоалгоритмов. Особенности построения криптосистем с секретным ключом. Подстановочные и перестановочные шифры. Определение поточных шифров. Поточные шифры на основе регистров сдвига. Достоинства и недостатки, области применения поточных шифров. Современные поточные шифры.	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 2.2 Определение блочных шифров. SP-сети. Сети Фейстеля. Режимы работы блочных шифров. Общая	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	схема симметричной криптосистемы. Безопасная длина ключа. Достоинства и недостатки, области применения блочных шифров. Современные блочные шифры. Система распределения ключей. Надежность современных одноключевых криптосистем									
	Тема 2.3 Особенности построения криптосистем с открытым ключом. Понятие односторонней функции. Вычислительно сложные задачи. Общая схема асимметричной криптосистемы. Система открытого распределения ключей. Современные асимметричные криптоалгоритмы. Обмен ключами по алгоритму Диффи-Хеллмана. Надежность современных двухключевых криптосистем. Гибридные криптосистемы.	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1] работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы:		6				Подготовка к лабораторной работе	Видео-конференция		

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					
	"Асимметричные криптосистемы"									
	Итого по 2 разделу	**6**	**6**		**1**	**9**				
Раздел 3. Криптографические методы в сетях ЭВМ										
ПКС-1- ИПКС-1.2.	**Тема 3.1.** Хэш-функции на основе блочных шифров. Бесключевые шифры. Требования к хэш-функциям. Принципы построения и области применения хэш-функций. Современные криптографические хэш-функции.	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.2. Цифровая электронная подпись. Процедура выработки и проверки ЭЦП. Виды нападений на цифровую подпись. Современные системы ЭЦП. Цифровые сертификаты. Перспективы развития криптографических систем.	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.3. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи									
	Тема 3.4. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым	2				3	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы: “Алгоритмы ЭЦП”		5				Подготовка к лабораторной работе	Видеоконференция		
	Итого по 3 разделу	**8**	**5**		**1**	**12**				
	Подготовка к зачёту/ зачёту с оценкой (контроль)					**8**				
	Итого за семестр	**17**	**17**		**4**	**34**				

Таблица 5.5 - Содержание дисциплины, структурированное по темам для студентов очно-заочного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Введение в криптографические методы										
ПКС-1- ИПКС-1.2.	**Тема 1.1** Основные определения. Задачи и современные приложения криптографии. Особенности применения криптографических методов в информационных технологиях. Классификация криптографических систем. Основные определения.	1				2	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 1.2 Определение криптографического алгоритма и протокола. Виды протоколов. Понятие нарушителя. Разновидности атак на протоколы. Условная и безусловная секретность. Криптографическая стойкость. Основные понятия теории передачи информации: энтропия и неопределенность, норма языка, абсолютная норма языка, энтропия криптосистемы, расстояние уникальности. Сложность криптоанали-	1				4	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	тической атаки									
	Тема лабораторной работы: "Симметричные криптосистемы"		3				Подготовка к лабораторной работе	Видеоконференция		
	Итого по 1 разделу	**2**	**3**		**2**	**6**				
Раздел 2. Типы криптографических систем										
ПКС-1- ИПКС-1.2.	**Тема 2.1** Определение и классификация симметричных криптоалгоритмов. Особенности построения криптосистем с секретным ключом. Подстановочные и перестановочные шифры. Определение поточных шифров. Поточные шифры на основе регистров сдвига. Достоинства и недостатки, области применения поточных шифров. Современные поточные шифры.	1				4	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 2.2 Определение блочных шифров. SP-сети. Сети Фейстеля. Режимы работы блочных шифров. Общая	1				4	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	схема симметричной криптосистемы. Безопасная длина ключа. Достоинства и недостатки, области применения блочных шифров. Современные блочные шифры. Система распределения ключей. Надежность современных одноключевых криптосистем									
	Тема 2.3 Особенности построения криптосистем с открытым ключом. Понятие односторонней функции. Вычислительно сложные задачи. Общая схема асимметричной криптосистемы. Система открытого распределения ключей. Современные асимметричные криптоалгоритмы. Обмен ключами по алгоритму Диффи-Хеллмана. Надежность современных двухключевых криптосистем. Гибридные криптосистемы.	1				4	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1] работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы:		3				Подготовка к лабораторной работе	Видео-конференция		

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					
	“Асимметричные криптосистемы”									
	Итого по 2 разделу	**3**	**3**		**1**	**12**				
Раздел 3. Криптографические методы в сетях ЭВМ										
ПКС-1- ИПКС-1.2.	**Тема 3.1**Хэш-функции на основе блочных шифров. Бесключевые шифры. Требования к хэш-функциям. Принципы построения и области применения хэш-функций. Современные криптографические хэш-функции.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.2.Цифровая электронная подпись. Процедура выработки и проверки ЭЦП. Виды нападений на цифровую подпись. Современные системы ЭЦП. Цифровые сертификаты. Перспективы развития криптографических систем.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.3.Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой	1				6	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи									
	Тема 3.4.Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым	1				6	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы: “Алгоритмы ЭЦП ”		3				Подготовка к лабораторной работе	Видеоконференция		
	Итого по 3 разделу	**4**	**3**		**1**	**22**				
	Подготовка к зачёту/ зачёту с оценкой (контроль)					**10**				
	Итого за семестр	**9**	**9**		**4**	**40**				

Таблица 5.6 - Содержание дисциплины, структурированное по темам для студентов заочного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Введение в криптографические методы										
ПКС-1- ИПКС-1.2.	**Тема 1.1** Основные определения. Задачи и современные приложения криптографии. Особенности применения криптографических методов в информационных технологиях. Классификация криптографических систем. Основные определения.	0.5				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 1.2 Определение криптографического алгоритма и протокола. Виды протоколов. Понятие нарушителя. Разновидности атак на протоколы. Условная и безусловная секретность. Криптографическая стойкость. Основные понятия теории передачи информации: энтропия и неопределенность, норма языка, абсолютная норма языка, энтропия криптосистемы, расстояние уникальности.	0.5				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	Сложность криптоаналитической атаки									
	Тема лабораторной работы: “Симметричные криптосистемы”		2				Подготовка к лабораторной работе	Видеоконференция		
	Итого по 1 разделу	**1**	**2**		**2**	**10**				
Раздел 2. Типы криптографических систем										
ПКС-1- ИПКС-1.2.	**Тема 2.1** Определение и классификация симметричных криптоалгоритмов. Особенности построения криптосистем с секретным ключом. Подстановочные и перестановочные шифры. Определение поточных шифров. Поточные шифры на основе регистров сдвига. Достоинства и недостатки, области применения поточных шифров. Современные поточные шифры.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 2.2 Определение блочных шифров. SP-сети. Сети Фейстеля. Режимы работы блочных шифров. Общая	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	схема симметричной криптосистемы. Безопасная длина ключа. Достоинства и недостатки, области применения блочных шифров. Современные блочные шифры. Система распределения ключей. Надежность современных одноключевых криптосистем									
	Тема 2.3 Особенности построения криптосистем с открытым ключом. Понятие односторонней функции. Вычислительно сложные задачи. Общая схема асимметричной криптосистемы. Система открытого распределения ключей. Современные асимметричные криптоалгоритмы. Обмен ключами по алгоритму Диффи-Хеллмана. Надежность современных двухключевых криптосистем. Гибридные криптосистемы.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1] работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы:		3				Подготовка к лабораторной работе	Видео-конференция		

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					
	“Асимметричные криптосистемы”									
	Итого по 2 разделу	**3**	**3**		**1**	**15**				
Раздел 3. Криптографические методы в сетях ЭВМ										
ПКС-1- ИПКС-1.2.	**Тема 3.1**Хэш-функции на основе блочных шифров. Бесключевые шифры. Требования к хэш-функциям. Принципы построения и области применения хэш-функций. Современные криптографические хэш-функции.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.2.Цифровая электронная подпись. Процедура выработки и проверки ЭЦП. Виды нападений на цифровую подпись. Современные системы ЭЦП. Цифровые сертификаты. Перспективы развития криптографических систем.	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема 3.3.Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической сис-	1				5	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		

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					
	темы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи									
	Тема 3.4.Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым	1				8	Подготовка к лекциям [7.1.1 – 7.1.4, 7.2.1, 7.2.2], работа над сквозным индивидуальным заданием	Видео-лекция. Лекция-консультация.		
	Тема лабораторной работы: “Алгоритмы ЭЦП”		3				Подготовка к лабораторной работе	Видео-конференция		
	Итого по 3 разделу	**4**	**3**		**1**	**23**				
	Подготовка к зачёту/ зачёту с оценкой (контроль)					**4**				
	Итого за семестр	**8**	**8**		**4**	**48**				

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

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Вычислительные системы и технологии».

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Таблица 6.1 - При текущем контроле (контрольные недели) и оценка выполнения лабораторных работ

Шкала оценивания	**Экзамен**
40<R<=50	Отлично
30<R<=40	Хорошо
20<R<=30	Удовлетворительно
O<R<=20	Неудовлетворительно

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

Таблица 6.2 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо»** / «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично»** / «зачтено» 90-100% от max рейтинговой оценки контроля
ПКС-1. Способен разрабатывать модели компонентов и алгоритмы функционирования вычислительной техники и автоматизированных систем	ИПКС-1.2. Разрабатывает алгоритмы функционирования вычислительной техники и автоматизированных систем	Не знает типовые шифры замены и перестановки; Не знает частотные характеристики языков и их использование в криптоанализе; Не знает требования к шифрам и основные характеристики шифров; принципы построения современных шифр систем; Не знает типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические прото-	Частично знает типовые шифры замены и перестановки; частично знает частотные характеристики языков и их использование в криптоанализе; Не знает требования к шифрам и основные характеристики шифров; принципы построения современных шифр систем; Не знает типовые поточные и блочные шифры, системы шифрования с открытыми ключами,	Знает типовые шифры замены и перестановки; частично знает частотные характеристики языков и их использование в криптоанализе; Частично знает требования к шифрам и основные характеристики шифров; принципы построения современных шифр систем; Знает типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптогра-	Знает типовые шифры замены и перестановки; частично знает частотные характеристики языков и их использование в криптоанализе; Знает требования к шифрам и основные характеристики шифров; принципы построения современных шифр систем; Знает типовые поточные и блочные шифры, системы шифрования с откры-

		колы. Не умеет выполнить постановку задач криптоанализа и указать подходы к их решению; Не умеет использовать основные математические методы, применяемые в анализе типовых криптографических алгоритмов; Не умеет применять полученные знания к различным предметным областям Не владеет навыками использования основных типов шифров и криптографических алгоритмов; Не владеет методами криптоанализа простейших шифров; Не владеет навыками применения современной научно-технической литературы в области криптографической защиты.	криптографические протоколы. Частично умеет выполнить постановку задач криптоанализа и указать подходы к их решению; Частичноумеет использовать основные математические методы, применяемые в анализе типовых криптографических алгоритмов; Не умеет применять полученные знания к различным предметным областям Частично владеет навыками использования основных типов шифров и криптографических алгоритмов; Не владеет методами криптоанализа простейших шифров; Не владеет навыками применения современной научно-технической литературы в области криптографической защиты	фические протоколы. Умеет выполнить постановку задач криптоанализа и указать подходы к их решению; Умеет использовать основные математические методы, применяемые в анализе типовых криптографических алгоритмов; Частично умеет применять полученные знания к различным предметным областям Владеет навыками использования основных типов шифров и криптографических алгоритмов; Частично владеет методами криптоанализа простейших шифров; Частично владеет навыками применения современной научно-технической литературы в области криптографической защиты	тыми ключами, криптографические протоколы. Умеет выполнить постановку задач криптоанализа и указать подходы к их решению; Умеет использовать основные математические методы, применяемые в анализе типовых криптографических алгоритмов; Умеет применять полученные знания к различным предметным областям Владеет навыками использования основных типов шифров и криптографических алгоритмов; Владеет методами криптоанализа простейших шифров; Владеет навыками применения современной научно-технической литературы в области криптографической защиты

Таблица 6.3 - 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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

7.1.1. Гвоздева Т.В., Баллод Б.А. Проектирование информационных систем: Учебное пособие. Ростов н/Д: Феникс, 2009 ISBN: 978-5-222-14075-8, Гриф УМО вузовРФ по образованию в обл. прикл. Информ.

7.1.2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: Учеб. Пособие.: М.: Академия, 2009 ISBN: 978-5-7695-5748-4,Гриф УМО по образованию в обл. информ. безопасности

7.1.3. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник.– 4-е изд. СПб.: Питер, 2010 Учебник. Гриф М-ва образов. и науки РФ

7.1.4. Райкин И.Л. Информационная безопасность и защита информации: Комплекс учебно-метод. материалов // Изд-во НГТУ, 2008

7.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

7.2.1 Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный

7.2.2 Онлайн-книга Вострецова, Е.В. В78 Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с. https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

7.3 Перечень журналов по профилю дисциплины:

7.3.1 Научно-технический и научно-производственный журнал Информационные технологии Журнал "Информационные технологии" (novtex.ru).

7.3.2 Информационные ресурсы России. Российская ассоциация электронных библиотек. Информационные Ресурсы России — Российская ассоциация электронных библиотек (aselibrary.ru).

7.3.3 Журнал «Информационные технологии и вычислительные системы». Журнал «Информационные технологии и вычислительные системы» - Aboutjournal (jitcs.ru)

7.4 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению лабораторных работ по дисциплине «Криптографические методы в информационных технологиях» в электронном варианте находятся на кафедре «Вычислительные системы и технологии», в библиотеке НГТУ им. Р.Е. Алексеева. Электронные варианты методических указаний по выполнению лабораторных работ отправляются на электронные адреса групп.

8. 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).

8.1 Перечень информационных справочных систем

Таблица 8.1 -Перечень электронных библиотечных систем

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

8.2 Перечень свободно распространяемого программного обеспечения

Таблица 8.2 – 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/
	Редактор блок-схем (https://app.diagrams.net/)

Таблица 8.3 - Программное обеспечение, используемое студентами очно-заочного, заочного 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/
	git (https://git-scm.com/), github (https://github.com/)
	Редактор блок-схем (https://app.diagrams.net/)

8.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 8.4 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 8.4 – 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

9. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 9.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации»https://www.nntu.ru/sveden/accenv/

Таблица 9.1 - 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

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

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

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

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

1. Компьютерные классы НГТУ им. Р.Е.Алексеева (6 корпус НГТУ, аудитории 6342, 6339), оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов(12 рабочих мест), оборудованных компьютерами:

- процессор: CPU IntelCore i3-2120 3.3 GHz;
- материнская плата: Asusp8h61-MLX2;
- оперативная память: 4 Gb (2*2Gb) DDR 3;
- жесткий диск: 500 Gb.

с пакетами ПО общего назначения:

- Windows 7;
- Linux;
- OpenOffice.

Перечень материально-технического обеспечения, необходимого для реализации программы бакалавриата и проведения лабораторных работ для студентов очного, очно-заочного и заочного обучения, включает в себя компьютерные классы

1. Ауд. 5412 кафедры «Вычислительные системы и технологии»,

Компьютеры оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов. 6 рабочих мест, включающих моноблоки Lenovo S710 Intel Core i3-3240/4 Gb RAM, в составе локальной вычислительной сети, с подключением к сети Интернет.

Пакеты ПО (лицензионное): Лицензия WindowsOEM (входила в поставку моноблоков)

Пакеты ПО (распространяемое по свободной лицензии):

- 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/)
- Maven (https://maven.apache.org/)

2. Ауд. 5422 кафедры «Вычислительные системы и технологии»,

Компьютеры оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов. 5 рабочих мест, включающих персональные компьютеры Intel Core i5-9400/8 Gb RAM (5 шт.), в составе локальной вычислительной сети, с подключением к сети Интернет.

Пакеты ПО (распространяемое по свободной лицензии):

- 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/)

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

- аудитория 6543;
- аудитория 6545 (Проектор Accer – 1шт;ПК на базе IntelCoreDuo 2.93 ГГц, 2 Гб ОЗУ, 320 Гб HDD, монитор Samsung19` – 11 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета).

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 «Криптографические методы в информационных технологиях», 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 может сопровождаться 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 кон-

сультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

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

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

Промежуточная аттестация проводится в форме зачёта с учетом текущей успеваемости.

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

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

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

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 (таблицы 5.4, 5.5, 5.6) . 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.

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 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.

11.4 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом

11.5 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, представ-

ленной в Разделе 7.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 10. 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 выполнение и защита лабораторных работ **для студентов всех форм обучения**. Зачет для студентов очной формы обучения в 6 семестре, для студентов очно-заочной в 9 семестре и заочной форм обучения на 3 курсе.

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

Курсовая работа не предусмотрена учебным планом

Типовые вопросы для промежуточной аттестации в форме зачета **для студентов всех форм обучения:**

1. Основные определения. Задачи и современные приложения криптографии
2. Особенности применения криптографических методов в информационных технологиях
3. Классификация криптографических систем.
4. Определение криптографического алгоритма и протокола. Виды протоколов.
5. Понятие нарушителя. Разновидности атак на протоколы. Условная и безусловная секретность. Криптографическая стойкость.
6. Основные понятия теории передачи информации: энтропия и неопределенность, норма языка, абсолютная норма языка, энтропия криптосистемы, расстояние уникальности.
7. Сложность криптоаналитической атаки.
8. Определение и классификация симметричных криптоалгоритмов. Особенности построения криптосистем с секретным ключом.
9. Подстановочные и перестановочные шифры. Определение поточных шифров. Поточные шифры на основе регистров сдвига.
10. Достоинства и недостатки, области применения поточных шифров. Современные поточные шифры.
11. Определение блочных шифров. SP-сети. Сети Фейстеля.
12. Режимы работы блочных шифров. Общая схема симметричной криптосистемы. Безопасная длина ключа.
13. Достоинства и недостатки, области применения блочных шифров. Современные блочные шифры..
14. Система распределения ключей. Надежность современных одноключевых криптосистем.
15. Особенности построения криптосистем с открытым ключом. Понятие односторонней функции. Вычислительно сложные задачи.
16. Общая схема асимметричной криптосистемы. Система открытого распределения ключей.
17. Современные асимметричные криптоалгоритмы.
18. Обмен ключами по алгоритму Диффи-Хеллмана.
19. Надежность современных двухключевых криптосистем. Гибридные криптосистемы.

20. Хэш-функции на основе блочных шифров. Бесключевые шифры.
21. Требования к хэш-функциям. Принципы построения и области применения хэш-функций.
22. Современные криптографические хэш-функции.
23. Цифровая электронная подпись. Процедура выработки и проверки ЭЦП.
24. Виды нападений на цифровую подпись. Современные системы ЭЦП.
25. Цифровые сертификаты.
26. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы.
27. Классификация криптографических протоколов.
28. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи.
29. Протоколы сертификации ключей.
30. Протоколы предварительного распределения ключей.
31. Протоколы выработки сеансовых ключей.
32. Открытое распределение ключей Диффи-Хеллмана и его модификации.
33. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением.
34. Разделение секрета. Протоколы подбрасывания монеты.
35. Построение протоколов с нулевым разглашением на основе NP-сложных задач.
36. Перспективы развития криптографических систем.

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

УТВЕРЖДАЮ:
Директор института ИРИТ

_____
“____”_____2021 г.

Лист актуализации рабочей программы дисциплины
«ФТД.1 Криптографические методы в информационных технологиях**»**
индекс по учебному плану, наименование

для подготовки **бакалавров**/ специалистов/ магистров
Направление: {шифр – название} 09.03.01 Информатика и вычислительная техника
Направленность: Вычислительные машины, комплексы, системы и сети
Форма обучения очная, очно-заочная, заочная
Год начала подготовки: 2020, 2021

Курс 3,5
Семестр 6,9
В рабочую программу не вносятся изменения. Программа актуализирована для 2021 г. начала подготовки.

Разработчик (и): __Жаринов В.Ф., к.т.н., доцент_____
(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 ВСТ _____«__» _____ 20__г.

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

_____