СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Прикладной информатики и программирования***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.В.ДВ.01.01 Основные криптографические алгоритмы***

часть, формируемая участниками образовательных отношений

Направление

09.03.03	***Прикладная информатика***
код	наименование направления

Программа

Мобильные и сетевые технологии

Форма обучения

Заочная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ПК-3. Способен проводить описание прикладных процессов и информационного обеспечения решения прикладных задач	ПК-3.1. Знания	Обучающийся должен: знать криптографические алгоритмы в современных программных комплексах и корректность их применения.
	ПК-3.2. Умения	Обучающийся должен: уметь устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.
	ПК-3.3. Владения/навыки	Обучающийся должен: владеть навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:
Дисциплина реализуется в рамках базовой части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Информатика и программирование», «Архитектура компьютера», «Алгебра», «Теория вероятностей и математическая статистика».

Дисциплина изучается на 3 курсе в 5, 6 семестрах

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 180 акад. ч.

Объем дисциплины	Всего часов
	Заочная форма обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	4

практических (семинарских)	8
лабораторных	4
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	3,8
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	160

Формы контроля	Семестры
дифференцированный зачет	6

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	**Алгоритмы симметричного шифрования.**	**2**	**4**	**2**	**60**
1.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	1	2	0	30
1.2	Алгоритмы симметричного шифрования ГОСТ и DES.	1	2	2	30
2	**Алгоритмы асимметричного шифрования.**	**2**	**4**	**2**	**100**
2.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	1	2	0	30
2.2	Хэш-функции.	0,5	1	1	35
2.3	Электронная цифровая подпись.	0,5	1	1	35
	Итого	**4**	**8**	**4**	**160**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Алгоритмы симметричного шифрования.**	
1.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования. 4 режима выполнения.
1.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Алгоритм DES. Алгоритм генерации ключей. Алгоритм ГОСТ 2814. Сравнительный анализ ГОСТ и DES. Создание случайных чисел.

2	**Алгоритмы асимметричного шифрования.**	
2.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Основные требования к алгоритмам ассиметричного шифрования. Математический аппарат алгоритма RSA.
2.2	Хэш-функции.	Требования к хэш-функциям. Простые хэш-функции. Сильные хэш- функции
2.3	Электронная цифровая подпись.	Требования к цифровой подписи. Прямая и арбитражная цифровые подписи.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Алгоритмы симметричного шифрования.**	
1.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Разработка приложения алгоритма ГОСТ (шифрование/дешифрование).
2	**Алгоритмы асимметричного шифрования.**	
2.2	Хэш-функции.	Создание хеш-образа сообщения с помощью хеш-функции цепочки зашифрованных блоков.
2.3	Электронная цифровая подпись.	Создание электронной цифровой подписи на основе RSA.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Алгоритмы симметричного шифрования.**	
1.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования. 4 режима выполнения.
1.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Работа с S-box, кодовой таблицей. Выполнение алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ. Разработка соответствующих процедур.
2	**Алгоритмы асимметричного шифрования.**	
2.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Генерация открытого и закрытого ключей RSA. Шифрование и дешифрование.
2.2	Хэш-функции.	Изучение сильных хэш-функций MD4, MD5.
2.3	Электронная цифровая подпись.	Изучение стандарта цифровой подписи DSS и ГОСТ 3410.