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

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.В.06 Методы и средства защиты информации***

часть, формируемая участниками образовательных отношений

Направление

44.03.05 ***Педагогическое образование (с двумя профилями подготовки)***
код наименование направления

Программа

Математика, Информатика

Форма обучения

Очная

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 использовать базовые знания математики и информатики для реализации учебных программ по профильным предметам	ПК-3.1. Использует знания современных приемы, методов и технологии обучения предмету; приемов, методов и средств диагностики образовательных результатов данного обучения; методов психологической и педагогической диагностики для решения различных задач профессиональной педагогической деятельности	Обучающийся должен знать: современные приемы, методы и технологии обучения предмету; приемы, методы и средства диагностики образовательных результатов данного обучения с учетом обеспечения информационной безопасности
	ПК-3.2. Применяет в образовательном процессе методы, приѐмы, средства обучения предмету, результативные технологии в соответствии с целями обучения, учебного содержания и типа урока; осуществлять диагностику образовательных результатов обучения математике/информатике; использовать современные методы и технологии обучения и диагностики для анализа учебно-воспитательного процесса образовательной организации	Обучающийся должен уметь: выбирать оптимальное сочетание методов, приемов, средств обучения; применять в образовательном процессе методы, приемы, средства обучения предмету, результативные технологии в соответствии с целями обучения, учебного содержания и типа урока; осуществлять диагностику образовательных результатов обучения математике/информатике; использовать современные методы и технологии обучения и диагностики для анализа учебно-воспитательного процесса образовательной организации с учетом обеспечения информационной безопасности.
	ПК-3.3. Реализует приемы, методы, технологий обучения и диагностики результатов обучения	Обучающийся должен владеть: опытом реализации приемов, методов, технологий обучения и диагностики результатов обучения предмету с учетом различных условий обучения,

	предмету с учетом различных условий обучения, по различным образовательным программам	по различным образовательным программам; диагностиками учебно-воспитательного процесса образовательной организации с учетом обеспечения информационной безопасности.

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

Цели изучения дисциплины:
Дисциплина реализуется в рамках части, формируемой участниками образовательных отношений.
Основной целью курса является формирование у студентов основ знаний об информационной безопасности, роли и внедрении информации в современном обществе.
Задачи изучения дисциплины:
– формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;
– формирование практических навыков применения средств защиты информации при решении профессиональных задач.

Дисциплина изучается на 5 курсе в 9 семестре

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 4 зач. ед., 144 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических (семинарских)	16
лабораторных	16
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	60

Формы контроля	**Семестры**
экзамен	9

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	**Криптография донаучного периода.**	**4**	**2**	**4**	**20**
1.1	Донаучный период криптографии.	2	1	4	15
1.2	Основные криптографические примитивы.	2	1	0	5
2	**Алгоритмы симметричного шифрования.**	**4**	**8**	**6**	**24**
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	2	0	0	7
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	2	8	6	17
3	**Алгоритмы асимметричного шифрования.**	**8**	**6**	**6**	**16**
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	2	2	2	7
3.2	Хэш-функции.	2	2	2	5
3.3	Электронная цифровая подпись.	4	2	2	4
	Итого	**16**	**16**	**16**	**60**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.1	Донаучный период криптографии.	Алгоритмы шифрования письма донаучного периода. Первые шифровальные машины.
1.2	Основные криптографические примитивы.	Подстановки. Перестановки. Гаммирование. Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
2	**Алгоритмы симметричного шифрования.**	
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования. 4 режима выполнения.
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Алгоритм DES. Алгоритм генерации ключей. Алгоритм ГОСТ 2814. Сравнительный анализ ГОСТ и DES. Создание случайных чисел.
3	**Алгоритмы асимметричного шифрования.**	

3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Основные требования к алгоритмам ассиметричного шифрования. Математический аппарат алгоритма RSA.
3.2	Хэш-функции.	Требования к хэш-функциям. Простые хэш-функции. Сильные хэш- функции
3.3	Электронная цифровая подпись.	Требования к цифровой подписи. Прямая и арбитражная цифровые подписи.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.1	Донаучный период криптографии.	Разбор алгоритмов шифрования Цезаря, Гронефельда, Трипемиуса, Бодо. Шифрование биграммами.
1.2	Основные криптографические примитивы.	Частотные характеристики открытых сообщений. Определение частотных характеристик криптограммы. Определение вероятностных характеристик алфавита.
2	**Алгоритмы симметричного шифрования.**	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Работа с S-box, кодовой таблицей. Выполнение алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ. Разработка соответствующих процедур.
3	**Алгоритмы асимметричного шифрования.**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Генерация открытого и закрытого ключей RSA. Шифрование и дешифрование.
3.2	Хэш-функции.	Изучение сильных хэш-функций MD4, MD5.
3.3	Электронная цифровая подпись.	Изучение стандарта цифровой подписи DSS и ГОСТ 3410.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.1	Донаучный период криптографии.	Программирование алгоритма Гронсфельда.
2	**Алгоритмы симметричного шифрования.**	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Разработка приложения алгоритма ГОСТ (шифрование/дешифрование).
3	**Алгоритмы асимметричного шифрования.**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Программирование алгоритма RSA.
3.2	Хэш-функции.	Создание хеш-образа сообщения с помощью хеш-функции цепочки зашифрованных блоков.
3.3	Электронная цифровая подпись.	Создание электронной цифровой подписи на основе RSA.