СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

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

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.В.07 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
2019 г.

Стерлитамак 2022

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	Обучающийся должен знать: современные приемы, методы и технологии обучения предмету; приемы , методы и средства диагностики образовательных результатов данного обучения; методы психологической и педагогической диагностики для решения различных задач профессиональной педагогической деятельности.
	ПК-3.2	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.
	ПК-3.3	Обучающийся должен владеть: опытом реализации приемов, методов, технологий обучения и диагностики результатов обучения предмету с учетом различных условий обучения, по различным образовательным программам; диагностиками учебно-воспитательного процесса образовательной организации.

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

Цели изучения дисциплины:
Дисциплина реализуется в рамках части, формируемой участниками образовательных отношений.
Дисциплина изучается на 3-4 курсе в 6-7 семестре.
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 4, 5 курсах в 8, 9 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 7 зач. ед., 252 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	252
Учебных часов на контактную работу с преподавателем:	
лекций	32
практических (семинарских)	48
лабораторных	32
другие формы контактной работы (ФКР)	0,4
Учебных часов на контроль (включая часы подготовки):	
зачет	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	139,6

Формы контроля	**Семестры**
зачет	8
дифференцированный зачет	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**	
7.1	Криптография с использованием эллиптических кривых.	2	2	2	0
4.1	Алгоритмы асимметрического шифрования.	2	6	6	12
1	**Основные криптографические примитивы.**	**1**	**2**	**2**	**4**

7	**Криптография с использованием эллиптических кривых.**	**2**	**2**	**2**	**0**
6.1	Электронная цифровая подпись. Виды цифровой подписи.	4	0	0	10
5.2	Хэш-функция MD5.	2	1	1	0
1.1	Основные криптографические примитивы.	1	2	2	4
2	**Криптография донаучного периода.**	**1**	**2**	**2**	**2**
2.1	Донаучный период криптографии.	1	2	2	2
3	**Алгоритмы симметричного шифрования.**	**2**	**4**	**4**	**12**
3.1	Разработка алгоритмов симметричного шифрования.	1	4	4	12
3.2	Выполнение алгоритмов симметричного шифрования.	1	0	0	0
4	**Алгоритмы асимметричного шифрования.**	**4**	**6**	**6**	**12**
4.2	Алгоритм RSA.	2	0	0	0
5	**Хэш-функции.**	**4**	**2**	**2**	**14**
5.1	Основные хэш-функции.	2	1	1	14
6	**Электронная цифровая подпись.**	**4**	**0**	**0**	**10**
	Итого	**18**	**18**	**18**	**54**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
7.1	Криптография с использованием эллиптических кривых.	
4.1	Алгоритмы асимметрического шифрования.	Алгоритмы асимметричного шифрования. Программирование алгоритма RSA.
1	**Основные криптографические примитивы.**	
7	**Криптография с использованием эллиптических кривых.**	
5.2	Хэш-функция MD5.	Программирование дешифрования алгоритма ГОСТ.
1.1	Основные криптографические примитивы.	Программирование алгоритма Гронсфельда.
2	**Криптография донаучного периода.**	
2.1	Донаучный период криптографии.	Программирование основных криптографических операций.
3	**Алгоритмы симметричного шифрования.**	
3.1	Разработка алгоритмов симметричного шифрования.	Программирование алгоритма ГОСТ.
4	**Алгоритмы асимметричного шифрования.**	

5	**Хэш-функции.**	
5.1	Основные хэш-функции.	Программирование шифрования алгоритма ГОСТ.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
7.1	Криптография с использованием эллиптических кривых.	
4.1	Алгоритмы асимметрического шифрования.	Алгоритмы асимметричного шифрования. Программирование алгоритма RSA.
1	**Основные криптографические примитивы.**	
7	**Криптография с использованием эллиптических кривых.**	
5.2	Хэш-функция MD5.	Программирование дешифрования алгоритма ГОСТ.
1.1	Основные криптографические примитивы.	Программирование алгоритма Гронсфельда.
2	**Криптография донаучного периода.**	
2.1	Донаучный период криптографии.	Программирование основных криптографических операций.
3	**Алгоритмы симметричного шифрования.**	
3.1	Разработка алгоритмов симметричного шифрования.	Программирование алгоритма ГОСТ.
4	**Алгоритмы асимметричного шифрования.**	
5	**Хэш-функции.**	
5.1	Основные хэш-функции.	Программирование шифрования алгоритма ГОСТ.

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
7.1	Криптография с использованием эллиптических кривых.	Математические понятия. Аналог алгоритма Диффи-Хеллмана обмена ключами. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA. Шифрование и дешифрование с использованием эллиптических кривых. Применение криптографических методов и алгоритмов в комплексной защите вычислительных систем.
4.1	Алгоритмы асимметрического шифрования.	Основные требования к алгоритмам ассиметричного шифрования.
1	**Основные криптографические примитивы.**	
7	**Криптография с использованием эллиптических кривых.**	
6.1	Электронная цифровая подпись. Виды цифровой подписи.	Требования к цифровой подписи. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS и ГОСТ 3410.
5.2	Хэш-функция MD5.	Хэш-функция MD5.
1.1	Основные	Подстановки. Перестановки. Гаммирование.

	криптографические примитивы.	Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
2	**Криптография донаучного периода.**	
2.1	Донаучный период криптографии.	Прикладные направления шифрования и их развитие. Закладка фундаментальных ориентиров учеными.
3	**Алгоритмы симметричного шифрования.**	
3.1	Разработка алгоритмов симметричного шифрования.	Прикладные направления шифрования и их развитие. Закладка фундаментальных ориентиров учеными.
3.2	Выполнение алгоритмов симметричного шифрования.	Алгоритм DES. Алгоритм ГОСТ 28147. Режимы выполнения алгоритмов симметричного шифрования. Создание случайных чисел.
4	**Алгоритмы асимметричного шифрования.**	
4.2	Алгоритм RSA.	Алгоритм RSA.
5	**Хэш-функции.**	
5.1	Основные хэш-функции.	Требования к хэш-функциям. Простые хэш-функции.
6	**Электронная цифровая подпись.**	