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.О.21 Методы и средства криптографической защиты информации***

обязательная часть

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-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)
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1. Понимать корректность криптографических алгоритмов в современных программных комплексах.	Обучающийся должен: Понимать корректность криптографических алгоритмов в современных программных комплексах.
	ОПК-9.2. Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.	Обучающийся способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.
	ОПК-9.3. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Обучающийся владеет 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 «Методы и средства защиты информации» является дисциплиной, дающей начальные представления и понятия в области информационной безопасности,4 определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.
Основной задачей преподавания дисциплины является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.
Уровень освоения содержания дисциплины предполагает: - Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности; Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности; - Принятие обоснованных решений по выбору политики

информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ. Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.
Дисциплина реализуется в рамках обязательной части.
Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: "Языки и методы программирования", "Теория информации", "Информационные технологии", "Основы информационной безопасности", "Основы безопасности систем баз данных".

Дисциплина изучается на 3, 4 курсах в 6, 7 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 6 зач. ед., 216 акад. ч.

Объем дисциплины	**Всего часов**
	Очно-заочная обучения
Общая трудоемкость дисциплины	216
Учебных часов на контактную работу с преподавателем:	
лекций	26
практических (семинарских)	28
лабораторных	26
другие формы контактной работы (ФКР)	1,4
Учебных часов на контроль (включая часы подготовки):	34,8
зачет	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	99,8

Формы контроля	**Семестры**
зачет	6
экзамен	7

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**	**8**	**6**	**8**	**29,8**
1.1	Донаучный период криптографии.	3	2	8	15

1.2	Основные криптографические примитивы.	5	4	0	14,8
2	**Алгоритмы симметричного шифрования**	**9**	**10**	**6**	**34**
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения	4	0	0	17
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	5	10	6	17
3	**Алгоритмы асимметричного шифрования.**	**9**	**12**	**12**	**36**
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	5	8	4	17
3.2	Хэш-функции	2	2	4	5
3.3	Электронная цифровая подпись.	2	2	4	14
	Итого	**26**	**28**	**26**	**99,8**

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 7 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 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.

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.