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

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

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.О.28 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
2021 г.

Разработчик (составитель)
кандидат физико-математических наук, доцент
Перевалова С. Л.
ученая степень, должность, ФИО

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)
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1	Обучающийся должен знать: криптографические алгоритмы в современных программных комплексах и корректность их применения.
	ОПК-9.2	Обучающийся должен уметь: устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.
	ОПК-9.3	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 4 курсе в 7 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
	Очно-заочная обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	24
практических (семинарских)	40
другие формы контактной работы (ФКР)	0,2

Учебных часов на контроль (включая часы подготовки):	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	79,8

Формы контроля	Семестры
дифференцированный зачет	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	
3	**Алгоритмы ассиметричного шифрования**	**7**	**18**	**0**	**24**
3.3	Электронная цифровая подпись.	2	6	0	8
2.2	Алгоритмы симметричного шифрования ГОСТ и DES	4	9	0	14
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения	4	5	0	13,8
2	**Алгоритмы симметричного шифрования**	**8**	**14**	**0**	**27,8**
1.4	Комплексная система защиты информации	3	4	0	7
1.3	Методы защиты от несанкционированного доступа к информации	2	4	0	7
1.2	Угрозы информационной безопасности	2	0	0	7
1.1	Основные понятия информационной безопасности.	2	0	0	7
1	**Комплексная система защиты информации**	**9**	**8**	**0**	**28**
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	3	6	0	8
3.2	Хэш-функции.	2	6	0	8
	Итого	**24**	**40**	**0**	**79,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
3	**Алгоритмы ассиметричного шифрования**	

3.3	Электронная цифровая подпись.	Создание электронной цифровой подписи на основе RSA
2.2	Алгоритмы симметричного шифрования ГОСТ и DES	Работа с S-box, кодовой таблицей . Выполнение алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ.
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения	Изучение основных криптографических примитивов. Разработка соответствующих процедур
2	**Алгоритмы симметричного шифрования**	
1.4	Комплексная система защиты информации	Студентами готовятся доклады с презентацией по заявленным темам. Организационные-правовые методы и средства защиты информации. Инженерно-технические методы и средства защиты информации. Программные и программно-аппаратные методы и средства защиты информации. Требования к комплексной системы защиты информации
1.3	Методы защиты от несанкционированного доступа к информации	Студентами готовятся доклады с презентацией по заявленным темам: парольная аутентификация, модель "рукопожатия", по биометрическим характеристикам, клавиатурному почерку
1	**Комплексная система защиты информации**	
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

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
3	**Алгоритмы ассиметричного шифрования**	
3.3	Электронная цифровая подпись.	Электронная цифровая подпись. Требования к цифровой подписи. Прямая и арбитражная цифровые подписи. Схемы создания ЭЦП.
2.2	Алгоритмы симметричного шифрования ГОСТ и DES	Алгоритм DES. Алгоритм ГОСТ 28147.
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения	Алгоритмы симметричного шифрования. Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования.
2	**Алгоритмы симметричного шифрования**	
1.4	Комплексная система защиты информации	Организационные - правовые методы и средства защиты информации. Инженерно-технические методы и средства защиты информации. Программные и программно-аппаратные методы и средства защиты информации. Требования к комплексной системы защиты информации.
1.3	Методы защиты от несанкционированного доступа к информации	Методы защиты от несанкционированного доступа к информации: парольная аутентификация, модель "рукопожатия", по биометрическим характеристикам, клавиатурному почерку.
1.2	Угрозы информационной безопасности	Угрозы информационной безопасности. Основные определения и критерии классификации угроз.

		Наиболее распространенные угрозы доступности. Некоторые примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.
1.1	Основные понятия информационной безопасности.	Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.
1	**Комплексная система защиты информации**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Алгоритмы ассиметричного шифрования. Основные требования к алгоритмам ассиметричного шифрования. Алгоритм RSA.
3.2	Хэш-функции.	Хэш-функции. Требования к хэш-функциям. Простые и сильные хэш-функции.

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

№	Тема	Содержание СРС	Источники	Форма Выполнения СРС
1.	**Комплексная система защиты информации**			
1.1.	Основные понятия информационной безопасности.	Методы и сервисы безопасности	Осн.[2,3] Доп.[1,2]	Конспектирование
1.2.	Угрозы информационной безопасности	Классификация угроз Классификация атак	Осн.[2,3] Доп.[1,2]	Конспектирование
1.3	Методы защиты от несанкционированного доступа к информации	Подготовка докладов по темам	Осн.[1,2] Доп.[2]	Доклад
1.4.	Комплексная система защиты информации	Подготовка докладов по темам	Осн.[1,2] Доп.[1,2]	Доклад
2	Алгоритмы симметричного шифрования.			
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения	Анализ режимов выполнения алгоритмов симметричного шифрования. Области применения	Осн.[1,2] Доп.[1,4]	Конспектирование.
2.2	Алгоритмы симметричного шифрования	Алгоритм DES, двойной DES Криптоалализ	Осн.[2] Доп.[2,4]	Выполнение 1 раунда алгоритмы в тетрадях.
3	Алгоритмы асимметричного шифрования.			
3.1.	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Алгоритм SHA-1, SHA-2		Изучение, тестирование алгоритма сравнительный анализ.
3.2.	Хэш-функции.	Сильная хеш-функция MD5		Конспектирование.
3.3.	Электронная цифровая подпись.	Стандарт цифровой подписи DSS	Осн.[1,2] Доп.[2]	Генерация и проверка подписи

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Чечёта, С.И. Введение в дискретную теорию информации и кодирования : учебное пособие / С.И. Чечёта. - Москва : МЦНМО, 2011. - 224 с. : табл., схем. - ISBN 978-5-94057-701-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63307 [25.08.2018]
2. Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] : учебник. — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990. [25.08.2018]
3. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578. [25.08.2018]

Дополнительная учебная литература:

1. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] : . — Электрон. дан. — М. : ДМК Пресс, 2008. — 451 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3027 [25.08.2018]
2. Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко. - Изд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2006. - 208 с. - (Основы информационных технологий). - ISBN 5-9556-0052-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233063. [25.08.2018]
3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 [25.08.2018]

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов