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

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

Рабочая программа 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.

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

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.

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 (28.08.2018).
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 (28.08.2018).
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 (28.08.2018).

Дополнительная учебная литература:

1. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] : . — Электрон. дан. — М. : ДМК Пресс, 2008. — 448 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3027 (28.08.2018).
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 (28.08.2018).
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 (28.08.2018).

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

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ БашГУ и ООО «Знаниум»№ 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022
6	Соглашение о сотрудничестве между БашГу и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	http://comp-science.narod.ru	Дидактические материалы по информатике
2	http://www.iXBT.ru	Последние новости в компьютерном мире

6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.
Office Standart 2010 RUS OLP NL Acdmc / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021
Kaspersky Endpoint Security / 950 / ООО «Смартлайн»/ №44/013 от 06.12.2021
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО«Фермомобайл» / № 04182 от 03.12.2013
Visual Studio Community 2019 v.16.3 / OLP. Бессрочная / https://visualstudio.microsoft.com/ru/vs/community/

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Лаборатория информатики и вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.
Специально-оборудованный кабинет в области информатики, технологий и методов программирования. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.
Лаборатория аппаратных средств вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.
Читальный зал: помещение для самостоятельной работы	Учебная мебель, учебно-наглядные пособия, компьютеры
Лаборатория технической защиты	Компьютеры; учебно-наглядные пособия;

информации. Помещение для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций	специализированное оборудование по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок; технические средства контроля эффективности защиты информации от утечки по каналам.