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 ***Криптографические методы защиты информации***

Блок Б1, базовая часть, Б1.Б.30
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

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

Программа

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

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

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

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Обучающийся должен знать: понятие составляющие и проблемы информационной безопасности; объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства нормативно-правовые, экономические и технологические методы обеспечения информационной безопасности.
	2 этап: Умения	Обучающийся должен уметь: обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов обеспечения информационной безопасности; применять криптографические и информационно-аналитические системы, информационные ресурсы и информационные технологии; сформулировать основные криптографические методы и методы стеганографии.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методом дискретного логарифмирования в конечных циклических группах; методом применения основных

		криптосистем и систем стенографирования; методом применения алгоритмов проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Обучающийся должен знать: источники угроз безопасности информации, методы оценки уязвимости информации; методы пресечения разглашения конфиденциальной информации.
	2 этап: Умения	Обучающийся должен уметь: отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства; применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками сопровождения и управления системами защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

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 6 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 3 зач. ед., 108 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	

лекций	12
практических (семинарских)	18
лабораторных	18
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

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	**Криптография донаучного периода.**	**3**	**2**	**4**	**19,8**
1.1	Донаучный период криптографии.	1	1	4	15
1.2	Основные криптографические примитивы.	2	1	0	4,8
2	**Алгоритмы симметричного шифрования.**	**4**	**10**	**6**	**24**
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	2	0	0	7
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	2	10	6	17
3	**Алгоритмы асимметричного шифрования.**	**5**	**6**	**8**	**16**
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	2	2	4	7
3.2	Хэш-функции.	2	2	2	5
3.3	Электронная цифровая подпись.	1	2	2	4
	Итого	**12**	**18**	**18**	**59,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	**Наименование раздела / темы дисциплины**	**Содержание**
1	**Криптография донаучного периода.**	
1.1	Донаучный период	Алгоритмы шифрования письма донаучного

	криптографии.	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 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	Работа с S-box, кодовой таблицей. Выполнение

	шифрования ГОСТ и DES.	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.

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

Внеаудиторными формами и инструментами самостоятельной работы студентов по дисциплине являются: работа с конспектом лекций, изучение дополнительного теоретического материала, чтение рекомендуемой литературы, подготовка к практическим занятиям, тестированию, контрольной работе и пр. Подробный перечень тем, выносимых на самостоятельное изучение, с указанием рекомендуемой учебно-методической литературой представлен ниже.

Наименование тем на самостоятельное изучение:

№	Тема	Содержание СРС	Источники	Форма выполнения СРС
1	**Криптография донаучного периода.**			
1.1	Донаучный период криптографии.	Изучение решеток Кардано. Криптографические машины 1 и 2 мировых войн	Осн.[2,3] Доп.[1,2]	Изучение и тестирование алгоритма.
1.2	Основные криптографические примитивы.	Криптография с использованием эллиптических кривых.	Осн.[2,3]	Конспектирование.
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.[1,3]	Конспектирование.
2.2	Алгоритмы симметричного шифрования.	Алгоритм IDEA	Осн.[2] Доп.[2,3]	Выполнение 1 раунда алгоритмы в тетрадях.
3	**Алгоритмы асимметричного шифрования.**			
3.1.	Требования к алгоритмам асимметрического шифрования. Алгоритм RSA.	Алгоритм SHA-1, SHA-2.	Осн.[2] Доп.[2,3]	Изучение, тестирование алгоритма и сравнительный анализ.
3.2.	Хэш-функции.	Хэш-функции.	Осн.[2] Доп.[2,3]	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

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. 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).
3. 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).

Дополнительная учебная литература:

1. 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).
2. 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).
3. 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).

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://www.iXBT.ru	Последние новости в компьютерном мире
2	http://comp-science.narod.ru	Дидактические материалы по информатике

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

Наименование программного обеспечения
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО«Фермомобайл» / № 04182 от 03.12.2013
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
Visual Studio Community 2019 v.16.3 / OLP. Бессрочная / https://visualstudio.microsoft.com/ru/vs/community/
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.

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

Тип учебной аудитории	Оснащенность учебной аудитории
Лаборатория технической защиты информации. Помещение для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций	Компьютеры; учебно-наглядные пособия; 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.
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	Доска, проектор, экран, учебная мебель, компьютеры, учебно- наглядные пособия.

работ)	
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.
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, учебная мебель, проектор, экран, 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, учебная мебель, компьютеры, проектор, экран, учебно-наглядные пособия.
Читальный зал: помещение для самостоятельной работы	учебная мебель, учебно-наглядные пособия, компьютеры
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.