

Министерство науки и высшего образования РФ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.ДВ.07.02 Математические методы в  
информационной безопасности

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.03.04 Прикладная математика

Направленность (профиль)

01.03.04 Прикладная математика

Форма обучения

очная

Год набора

2019

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили \_\_\_\_\_

к.п.н., доцент, Кирко И.Н.

\_\_\_\_\_  
должность, инициалы, фамилия

## 1 Цели и задачи изучения дисциплины

### 1.1 Цель преподавания дисциплины

Дисциплина “Математические методы в информационной безопасности” знакомит студентов с основами защиты информации

### 1.2 Задачи изучения дисциплины

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- Знать основные понятия и определения, используемые при защите информации.
- Изучить возможные источники, риски и формы атак на информацию.
- Ознакомиться со стандартами безопасности. Знать основные особенности политики безопасности.
- Изучить теоретические основы криптографии. Знать и уметь применить основные алгоритмы шифрования.
- Иметь понятие об особенностях и требованиях к защите информации в сетях.

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

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
<b>ПК-1: Способен к постижению основ математических моделей реального объекта или процесса, готов применять моделирование для построения объектов и процессов, определения или предсказания их свойств.</b>	
ПК-1.1: Знать основы применения математических моделей при исследовании процессов и систем.	Знать основные понятия и определения, используемые при защите информации
ПК-1.2: Уметь использовать современный аппарат математического моделирования при решении прикладных научных и производственных задач	уметь применить основные алгоритмы шифрования
ПК-1.3: Владеть методами проверки на адекватность и проведения анализа результатов моделирования.	Владеть основами особенности политики безопасности.

### 1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

## 2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
<b>Контактная работа с преподавателем:</b>	<b>2 (72)</b>	
занятия лекционного типа	0,5 (18)	
практические занятия	1,5 (54)	
<b>Самостоятельная работа обучающихся:</b>	<b>2 (72)</b>	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
<b>Промежуточная аттестация (Экзамен)</b>	<b>1 (36)</b>	

### 3 Содержание дисциплины (модуля)

#### 3.1 Разделы дисциплины и виды занятий (тематический план занятий)

		Контактная работа, ак. час.							
№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
<b>1. Математические методы информационной безопасности</b>									

<p>1. Группы. Аксиомы и примеры. Теорема о единичном элементе и его обратном элементе. Произведение обратных элементов. Латинские квадраты. Абелевы группы. Кольца, определение, аксиомы и примеры. Коммутативные кольца и их свойства. Поля, определения, аксиомы и примеры. Простейшие поля. Простые числа и связанные с ними поля и их свойства. Поля Гауа. Мультипликативные группы полей Гауа. Порядок элементов. Идеалы, определение, свойства и примеры. Классы вычетов, свойства и примеры. Идеалы и классы вычетов целых чисел. Их свойства; соответствующие теоремы. Важные объекты теории чисел: простые числа, делители. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Теорема Ферма. Функция Эйлера. Нахождение обратного элемента по модулю. Подгруппы и смежные классы. Теорема Лагранжа. Расширенный алгоритм Евклида и соотношение Безу. Их применение.</p>	6							
<p>2. Модульные операции. Суммирование и умножение. Деление и возведение в степень</p>			18					
<p>3. Работа с литературой</p>							10	

4. Структура конечных групп, образованных остатками от деления для полиномов. Изоморфизм. Нормированные и двойственные полиномы. Алгоритм Евклида для полиномов. Алгебра классов вычетов многочленов. Теорема о примитивном элементе поля Гауа. Свойства корней полиномов. Неприводимые и примитивные многочлены. Идеалы многочленов и классы вычетов. Структуры конечных групп, образованных остатками от деления для составных чисел. Линейные переключательные схемы. Определение и примеры. Операции над полиномами. Деление полиномов.	4							
5. Алгоритм Евклида и расширенный алгоритм Евклида			12					
6. Работа с литературой							20	
7. Виды шифрования, их свойства. Пароли. Поточное, блочное, сверточное шифрование, их свойства. Виды шифрования: одностороннее (без расшифровки), симметричное и несимметричное (с открытым ключом). Модульное возведение в степень. Система шифрования RSA. Алгоритм и его обоснование. Достоинства и недостатки метода. Система шифрования по Эль-Гамалу. Алгоритм и его обоснование. Достоинства и недостатки метода. Открытое распределение ключей. Алгоритм Диффи-Хелмана. Понятие о методах криптоанализа. Факторизация. Парадокс дней рождений.	4							
8. Метод шифрования			12					
9. Работа с литературой							10	

<p>10. Определение и способы вычисления ко-дов CRC. Выбор “магического” поли-нома и его влияние на обнаружение ошибок при помощи CRC-кода. Генераторы случайных последовательностей на регистрах. Рекуррентные соотношения. Генераторы случайных последовательностей, использующие переключаемые схемы. Шифрование методом деления полино-мов. Длина периода гаммы. Шифрование при помощи генераторов случайных по-следовательностей. Свойства шифрова-ния при помощи гамма-последовательностей. Получение гамма-последовательностей с очень большим периодом. Поточковые шифры. Линейная сложность. Генератор Грегге, генератор с нелинейным фильтром. Сжимающий генератор. Псевдослучайные последова-тельности. Определение длины периода последовательности. Метод Флойда. Пе-риод и автокорреляция. Постулаты Го-ломба для псевдослучайных последова-тельствностей.</p>	2							
<p>11. Шифрование при помощи гамма-последовательности</p>			6					
<p>12. Работа с литературой</p>						10		



13. Источники, риски и формы атак на информацию. Информационная безопасность компьютерных систем. Дискреционное управление доступом. Безопасность повторного использования объектов. Метки безопасности. Мандатное управление доступом. Подотчетность. Аудит. Операционная и технологическая гарантированность вычислительных систем. Алгоритмы аутентификации пользователей. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Требования к системам защиты информации.	2							
14. Криптоанализ текста, зашифрованного методом гамма-последовательности			6					
15. Работа с литературой							22	
16.								
Всего	18		54				72	

## **4 Учебно-методическое обеспечение дисциплины**

### **4.1 Печатные и электронные издания:**

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии(Москва: Горячая линия-Телеком).
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие.; допущено УМО вузов по университетскому образованию(М.: ИНФРА-М).
3. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: учебное пособие.; рекомендовано УМО по образованию в области информационных технологий и систем(М.: ИНФРА-М).
4. Кирко. И.Н., Кушнир. В.П. Программно-аппаратные средства защиты информации: учеб-метод. материалы к изучению дисциплины для ... 10.05.01 - Компьютерная безопасность(Красноярск: СФУ).

### **4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):**

1. Методика проведения занятий допускает использование технических средств (про-екторы, интерактивные доски), обеспеченных соответствующим программным обеспечением, предлагается применение вычислительной техники и стандартных пакетов прикладных программ (MS Office, MathCad, MathLab и др.).
- 2.

### **4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:**

1. Справочная система "Консультант плюс"

## **5 Фонд оценочных средств**

Оценочные средства находятся в приложении к рабочим программам дисциплин.

## **6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)**

Методика проведения занятий допускает как использование технических средств (проекторы, интерактивные доски), так и классические аудиторные занятия, обеспечиваемые стандартными материально-техническими средствами