Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)	**Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)**
наименование кафедры	наименование кафедры
	А.А. Кытманов
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ КРИПТОГРАФИИ (THE BASICS OF CRYPTOGRAPHY)

Дисциплина Б1.В.ДВ.01.02 Основы криптографии (The Basics of Cryptography)

Направление подготовки / специальность 01.04.02 Прикладная математика и информатика, программа 01.04.02.09 Data Science and Mathematical Modeling 2020г

Направленность (профиль)

Форма обучения очная

Год набора 2020

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования с учетом профессиональных стандартов по укрупненной группе

010000 «МАТЕМАТИКА И МЕХАНИКА»

Направление подготовки /специальность (профиль/специализация)

Направление 01.04.02 Прикладная математика и информатика,
программа 01.04.02.09 Data Science and Mathematical Modeling 2020г.

Программу составили

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Ознакомление с теоретико-числовыми методами в криптографии

1.2 Задачи изучения дисциплины

1. Ознакомление с основами теории чисел.
2. Ознакомление с основными видами и формами угроз информационнйо безопасности
3. Изучение одной из криптографических систем с открытым ключом

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

ПК-3:Способен управлять разработкой продуктов, услуг и решений на основе данных.
ПК-3.1:Знает: состояние и перспективы развития информационных технологий, технологий данных в России и в мире; современные и перспективные методы сбора, хранения и передачи данных; источники данных, интенсивность генерации данных источниками; технические средства и среды сбора, хранения и обработки данных; современные и перспективные средства визуализации и интерпретации данных; исследование операций; машинное обучение; математическое моделирование; методы сравнительного анализа.
ПК-4:Способен разрабатывать и внедрять новые методы и технологии исследования данных.
ПК-4.1:Знает: состояние и перспективы развития информационных технологий, технологий данных в России и в мире; современные и перспективные методы сбора, хранения и передачи данных; источники данных, интенсивность генерации данных источниками; технические средства и среды сбора, хранения и обработки данных; современные и перспективные средства визуализации и интерпретации данных; исследование операций; машинное обучение; математическое моделирование; методы сравнительного анализа.

1.4 Место дисциплины (модуля) в структуре образовательной программы

Машинное обучение и криптография
Прикладные задачи анализа данных
выполнение и защита выпускной квалификационной работы
Машинное обучение и криптография (Applications of Machine Learning in Cryptography)

Прикладные задачи анализа данных (Applied Data Analysis)

Выполнение и защита выпускной квалификационной работы (Final certification)

1.5 Особенности реализации дисциплины

Язык реализации дисциплины Английский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		2
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1 (36)**	**1 (36)**
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,5 (18)	0,5 (18)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
Самостоятельная работа обучающихся:	**2 (72)**	**2 (72)**
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Зачёт)		

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад.час)	Занятия семинарского типа		Самостоятельная работа, (акад.час)	Формируемые компетенции
			Семинары и/или Практические занятия (акад.час)	Лабораторные работы и/или Практикумы (акад.час)		
1	2	3	4	5	6	7
1	Algorithms for primality testing and integer factorization	3	3	0	14	
2	Finite fields and polynomials	4	4	0	16	
3	Algorithms for discrete logarithms	3	3	0	16	
4	Public-key cryptography	8	8	0	26	
Всего		18	18	0	72	

3.2 Занятия лекционного типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	- Deterministic and probabilistic primality testing (pseudoprime numbers)	1	0	0
2	1	- Algorithms for generating of large primes	1	0	0
3	1	- Factorization of integers with exponential and sub-exponential complexity	1	0	0

4	2	- Irreducible polynomials and construction of finite fields	1	0	0
5	2	- Primitive polynomials over a finite field and their generating	1	0	0
6	2	- Factorization algorithms for polynomials over a finite field	1	0	0
7	2	- Algebraic equations over a finite field	1	0	0
8	3	- Deterministic algorithms for discrete logarithms	1	0	0
9	3	- Discrete logarithms in finite fields	2	0	0
10	4	- Asymmetric cryptosystems (RSA, etc.)	2	0	0
11	4	- El-Gamal cryptosystem	2	0	0
12	4	- Probabilistic encryption (as an example: Rabin cryptosystem)	2	0	0
13	4	- William’s cryptosystem vs. RSA	2	0	0
Всего			18	0	0

3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	- Deterministic and probabilistic primality testing (pseudoprime numbers)	1	0	0
2	1	- Algorithms for generating of large primes	1	0	0
3	1	- Factorization of integers with exponential and sub-exponential complexity	1	0	0

4	2	- Irreducible polynomials and construction of finite fields	1	0	0
5	2	- Primitive polynomials over a finite field and their generating	1	0	0
6	2	- Factorization algorithms for polynomials over a finite field	1	0	0
7	2	- Algebraic equations over a finite field	1	0	0
8	3	- Deterministic algorithms for discrete logarithms	1	0	0
9	3	- Discrete logarithms in finite fields	2	0	0
10	4	- Asymmetric cryptosystems (RSA, etc.)	2	0	0
11	4	- El-Gamal cryptosystem	2	0	0
12	4	- Probabilistic encryption (as an example: Rabin cryptosystem)	2	0	0
13	4	- William’s cryptosystem vs. RSA	2	0	0
Всего			18	0	0

3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
Всего					

4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год

Л1.1	Кириллова С. В.	Теоретико-числовые методы в криптографии. Криптографическая система RSA: учеб-метод. пособие для студентов спец. 090301.65 (090102.65) «Компьютерная безопасность» и направления 090900.62 «Информационная безопасность».	Красноярск: СФУ, 2012

5 Фонд оценочных средств для проведения промежуточной аттестации

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Кнауб Л. В., Новиков Е. А., Шитов Ю. А.	Теоретико-численные методы в криптографии: учеб. пособие для студентов вузов	Красноярск: ИПК СФУ, 2011
Л1.2	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учеб. пособие для студентов вузов, обуч. по спец. 090101 "Криптография"	Санкт-Петербург: Лань, 2011
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Коржик В. И., Яковлев В. А.	Основы криптографии: учебное пособие для обучающихся по направлениям подготовки бакалавров и магистров: "Информационная безопасность", "Сервис", "Инфокоммуникационные технологии и системы связи", а также по специальности "Защищенные системы связи"	Санкт-Петербург: Интермедия, 2016
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Кириллова С. В.	Теоретико-числовые методы в криптографии. Криптографическая система RSA: учеб-метод. пособие для студентов спец. 090301.65 (090102.65) «Компьютерная безопасность» и направления 090900.62 «Информационная безопасность».	Красноярск: СФУ, 2012

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Для получения допуска к зачету по дисциплине необходимо выполнить и защитить преподавателю в устной форме лабораторные работы.

В конце семестра в устной форме проводится зачет по дисциплине.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

9.1 Перечень необходимого программного обеспечения

9.1.1	Программа PGP (Свободное ПО)

9.2 Перечень необходимых информационных справочных систем

9.2.1	электронные информационно-справочные ресурсы научной библиотеки СФУ (http://bik.sfu-kras.ru)

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

Учебные лаборатории и классы, оснащенные современными компьютерами, объединенными в локальные вычислительные сети с выходом в Интернет, а также периферийным и проекционным оборудованием.