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

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра цифровых технологий управления	**Кафедра цифровых технологий управления**
наименование кафедры	наименование кафедры
	А.А. Ступина
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Дисциплина Б1.В.ДВ.02.02 Криптографические методы защиты информации

Направление подготовки / специальность

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

090000 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

Направление подготовки /специальность (профиль/специализация)

09.04.03 Прикладная информатика программа магистратуры 09.04.03.07 Информационное обеспечение финансового мониторинга

Программу составили Казаковцев Л.А.

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Цель – изучение основных математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению современных криптографических алгоритмов. Дисциплина должна способствовать развитию творческих способностей магистрантов, умению использования математического аппарата для вывода свойств разрабатываемых методов, умению творчески применять и самостоятельно повышать свои знания в области криптографии и защиты информации вообще

1.2 Задачи изучения дисциплины

Задачами дисциплины «Криптографические методы защиты информации» являются:

- изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии (организации);
- ознакомление магистрантов с современными научными исследованиями в области криптографии и примыкающих к ней прикладных областях, способствовать формированию направлений собственных научных исследований
- формирование у студентов личностных и профессиональных качеств необходимых для участия в работе по совершенствованию уровня защты информации на предприятии или объекте;
- формирование у обучающихся практических умений и навыков, необходимых для самостоятельной работы

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

ОПК-6:Способен исследовать современные проблемы и методы прикладной информатики и развития информационного общества;	
Уровень 1	проблемы и тенденции развития в области информационной безопасности; состояние законодательной базы информационной безопасности; правила защиты информации
Уровень 1	использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в профессиональной деятельности
Уровень 1	основной терминологией области безопасности информации

ПК-3:Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы по финансовому мониторингу (Росфинмониторинг), Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Уровень 1	основные положения государственной системы правового обеспечения защиты информации в Российской Федерации; виды технических средств и программных продуктов по защите информации; способы и средства защиты информации
Уровень 1	определять источники и содержание угроз в информационной сфере; использовать технические средства и программные продукты по защите информации
Уровень 1	программно-аппаратными и техническими методами и средствами защиты информации; основными технологиями построения защищенных систем

1.4 Место дисциплины (модуля) в структуре образовательной программы

Информационная безопасность

Информационное обеспечение системы управления рисками

Правовое обеспечение информационной среды

Технологии специализированных баз данных и информационных систем

Информационно-аналитическая деятельность в сфере финансовой разведки

Правовое обеспечение информационной среды

1.5 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)	Семестр
		3
Общая трудоемкость дисциплины	**4 (144)**	**4 (144)**
Контактная работа с преподавателем:	**0,89 (32)**	**0,89 (32)**
занятия лекционного типа	0,22 (8)	0,22 (8)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,67 (24)	0,67 (24)
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:	**3,11 (112)**	**3,11 (112)**
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	Основы информационной безопасности	2	0	0	28	ОПК-6 ПК-3
2	Инструментальные средства и библиотеки для реализации криптографических алгоритмов	2	4	0	28	ОПК-6 ПК-3
3	Теоретико-числовые методы в криптографии. Вычисления в простых полях и кольцах целых чисел	2	12	0	28	ОПК-6 ПК-3
4	Теория секретных систем Шеннона и современные подходы к теоретико-информационной секретности	2	8	0	28	ОПК-6 ПК-3
Всего		8	24	0	112	

3.2 Занятия лекционного типа

№	№ раздела	Наименование занятий	Объем в акад.часах

п/п	дисциплины		Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Основы информационной безопасности Понятие национальной безопасности, Каналы утечки информации	2	0	0
2	2	Криптографическая библиотека Агава. Windows Crypto-API. Библиотека вычислений с большими числами GNU MP. Библиотека криптографических алгоритмов GNU Crypto.	2	0	0
3	3	Арифметика по модулю, понятия конечных целочисленных колец и полей. Эффективные алгоритмы вычисления мультипликативной инверсии и возведения в степень. Теоремы Ферма и Эйлера. Алгоритмические аспекты поиска больших простых чисел.	2	0	0
4	4	Совершенные, идеальные и строго идеальные шифры. Рандомизация. Связь между длиной ключа и избыточностью, роль рандомизации. Эффективные методы построения идеальных шифров	2	0	0
Всего			8	0	0

3.3 Занятия семинарского типа

			Объем в акад.часах

			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	2	Работа с функциями и типами данных библиотек вычислений с большими числами GNU MP и криптографических алгоритмов GNU Crypto	2	0	0
2	2	Арифметические операции в простых полях и кольцах целых чисел, вычисления вручную и с помощью компьютера. Использование библиотечных средств для поиска случайных простых чисел.	2	0	0
3	3	Алгоритмы построения систем с открытым ключом: система Диффи-Хеллмана, шифры Шамира, Эль-Гамаля.	4	0	0
4	3	Операция извлечения корней в конечном кольце. Система RSA, шифр Рабина. Стойкость систем RSA и Рабина. Использование односторонних функций при построении криптографических протоколов.	4	0	0
5	3	Доказательства с нулевым разглашением Построение протоколов аутентификации Построение протоколов электронных денег	4	0	0
6	4	Омофонные коды, оптимальный омофонный код. Эффективный метод построения идеального шифра с помощью нумерации сочетаний.	4	0	0

7	4	Универсальное омофонное кодирование. Проблемы обобщения схем на марковские источники.	4	0	0
Всего			24	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					

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	Бабаш А.В.	Криптографические методы защиты информации: Учебно-методическое пособие: Том 1#205:	Москва: Издательский Центр РИО□, 2019
Л1.2		Криптографические методы защиты информации: лабораторный практикум	Ставрополь: СКФУ, 2015
Л1.3	Вайнштейн В.И.	Криптографические методы защиты информации: [учеб-метод. материалы к изучению дисциплины для ...10.03.01.01 Безопасность компьютерных систем]	Красноярск: СФУ, 2018
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Фот Ю. Д.	Методы защиты информации: учебное пособие для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.02 фундаментальная информатика и информационные технологии	Оренбург: ОГУ, 2019
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год

Л3.1	Корпачева Л.Н.	Перспективные направления прикладной информатики: [учеб-метод. материалы к изучению дисциплины для ...09.04.03.02 - Реинжиниринг бизнес-процессов]	Красноярск: СФУ, 2017

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Э1	Научная электронная библиотека	http://elibrary.ru
Э2	Федеральный образовательный портал	http://www.edu.ru
Э3	Библиотечно-издательский комплекс	http://bik.sfu-kras.ru
Э4	Информационная безопасность. Защита информации	http://all-ib.ru
Э5	Ресурсы базы знаний «Цифровая экономика»	https://data-economy.ru
Э6		

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Для успешного освоения дисциплины и формирования необходимых компетенций предусмотрены следующие формы проведения аудиторных занятий:

- лекции с применением презентационного материала;
- интерактивные аудиторные занятия;
- практические занятия с рассмотрением конкретных заданий, способствующих развитию профессиональных компетенций.

Все виды аудиторных занятий сочетают образовательную, воспитательную, практическую и методическую функции.

Лекционные занятия включают:

- вводную лекцию, на которой до сведения обучающего доводятся основные сведения о дисциплине, обосновывается ее роль в соответствующей области знаний, определяется значение дисциплины для формирования общих и профессиональных компетенций;
- модульные лекции, предназначенные для овладения обучающимися знаниями в рамках материала модуля ООП;

На практических занятиях со студентами предполагается:

- выполнение практических работ по теме предстоящего занятия, на основе изученного теоретического материала
- студенты самостоятельно обдумывают ответы на предложенные по каждой теме практических занятий «вопросы к обсуждению». Перечень вопросов, которые будут обсуждены на занятии, может быть определены как студентами, так и преподавателем. Обсуждение в группе или дискуссия по контрольным вопросам способствует закреплению изученного теоретического материала и выявлению недостатков его усвоения, приращению объема знаний уже на самом занятии.

Итоговая оценка по учебной дисциплине складывается из следующих элементов:

- выполнение заданий (отчеты о выполненной практической работе);
- зачет.

В ходе самостоятельной работы студентами используется теоретический материал, рекомендуемая литература, а также информационные ресурсы.

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

9.1 Перечень необходимого программного обеспечения

9.1.1	Стандартные программные приложения MS OFFICE (MS Excel, MS Word, MS PowerPoint), MS Visio

9.2 Перечень необходимых информационных справочных систем

9.2.1	1. Электронно-библиотечная система СФУ
9.2.2	2. Электронно-библиотечная система ИЗДАТЕЛЬСКОГО ДОМА "ИНФРА-М"
9.2.3	3. Правовая система Гарант
9.2.4	4. Справочно-правовая система Консультант+

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

1. Образовательная сеть Университета
2. Устройство беспроцессорное терминальное
3. Проектор
4. Панель сенсорная интерактивная
5. Компьютерный планшет
6. Wi-Fi беспроводная точка доступа