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

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра алгебры и математической логики (АиМЛ_ФМиИ)	**Кафедра алгебры и математической логики (АиМЛ_ФМиИ)**
наименование кафедры	наименование кафедры
	Левчук В.М.
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.07 Криптографические методы защиты информации

Направление подготовки / специальность 01.04.01 Математика Магистерская программа 01.04.01.02 Алгебра, логика и дискретная математика

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 01.04.01 Математика Магистерская программа 01.04.01.02 Алгебра, логика и дискретная математика

Программу составили	Кандидат физико-математических наук, Доцент, Жданов Олег Николаевич

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины «Криптографические методы защиты информации» является знакомство магистрантов с математическими основами криптографии. Рассматриваются исторические и современные криптосистемы и, в особенности, их криптоанализ и лежащие в его основе математические средства.

1.2 Задачи изучения дисциплины

Задачей изучения дисциплины является изучение основных понятий и истории развития криптографии, исторических шифров и их недостатков, современных блочных шифров и способов их криптоанализа, средств асимметричной криптографии и математического аппарата, обеспечивающего их построение и криптоанализ, приложений криптоалгоритмов при построении криптографических протоколов и систем защиты информации.

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

ПК-1:Способен применять в научно-исследовательской деятельности знания математических и естественных наук, основ программирования и информационных технологий	
Уровень 1	Какие исследовательские вопросы стоят в рамках данной дисциплины знания.
Уровень 1	Самостоятельно освоить темы дисциплины, углубляющие и детализирующие содержание лекционных и семинарских занятий.
Уровень 1	Алгоритмическими методами решения задач и проблем, входящими в рамки данной дисциплины.

1.4 Место дисциплины (модуля) в структуре образовательной программы

При изучении дисциплины достаточно владеть основными понятиями стандартного курса алгебры: кольца классов вычетов целых чисел, конечные поля, подстановки, полная линейная группа.

Данная дисциплина может быть полезна при освоении курсов информатики, теории баз данных, интернет-технологий.

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
		1
Общая трудоемкость дисциплины	**2 (72)**	**2 (72)**
Контактная работа с преподавателем:	**1,06 (38)**	**1,06 (38)**
занятия лекционного типа	0,53 (19)	0,53 (19)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,53 (19)	0,53 (19)
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:	**0,94 (34)**	**0,94 (34)**
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	Основные понятия и история криптографии.	2	2	0	6	ПК-1
2	Симметричная криптография.	8	5	0	10	ПК-1
3	Асимметричная криптография.	6	6	0	14	ПК-1
4	Криптографические протоколы.	3	6	0	4	ПК-1
Всего		19	19	0	34	

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	Основные понятия криптографии 1.1.Постановка задачи. Виды информации, подлежащей закрытию. Три метода защиты информациот несанкционированного доступа. Отличие криптографического решения от иных. Краткий исторический очерк развития криптографии. 1.2. Открытые сообщения и их характеристики. Модели и свойства информации. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. 1.3. Основные понятия криптографии. Модели шифров. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к щифрам.	2	0	0

2	2	Основные классы шифров и их свойства. 2.1. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. 2.2 Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. 2.3. Поточные цифры Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	2	0	0

3	2	Надёжность шифров 3.1.Теория К. Шеннона. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Характеризация совершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости.Избыточность языка и расстояние единственности. 3.2 Имитостойкость шифров Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. 3.3 Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	2	0	0

4	2	Симметричные алгоритмы шифрования. 4.1.Принципы построения блочных шифров. 4.2. Алгоритмы DES и ГОСТ 28147-89, алгоритмы ``Магма`` и ``Кузнечик``. 4.3. Алгоритм AES. 4.4. Алгоритм IDEA. 4.5.Требования, предъявляемые к блочным симметричным шифрам. 4.6.Режимы работы блочных шифров.	2	0	0

5	2	Основные способы реализации криптографических алгоритмов 5.1. Различия между программными и аппаратными реализациями. Программные реализации шифров. 5.2.Современные криптографические интерфейсы. Криптографические стандарты. 5.3. Вопросы синтеза генераторов случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный контурный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях. 5.3.Методы усложнения последовательностей псевдослучайных чисел.Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнения последовательностей.	2	0	0

6	3	Алгоритмы асимметричные 6.1.Понятие односторонней функции и односторонней функции с «лазейкой». 6.2. Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. 6.3. Шифрование на основе эллиптических кривых. 6.4.Криптосистемы на основе задачи об укладке рюкзака.Достоинства и недостатки асимметричных систем шифрования.	2	0	0
7	3	Методы анализа криптографических алгоритмов. 7.1.Понятие криптоатаки. Классификация криптоатак.Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уровней шифрования, бесключевые методы. 7.2. Особенности линейного криптоанализа. 7.3. Особенности дифференциального криптоанализа.	2	0	0

8	3	Криптографические хеш -функции и электронная подпись. 8.1.Характеристики и алгоритмы выработки хэш-функций.Примеры. 8.2. Хеш-функция по стандарту РФ. 8.3.ЭЦП: определение, отличия от собственноручной подписи. 8.4. ЭЦП на основе группы точек эллиптической кривой над конечным полем.	2	0	0

9	4	Криптографические протоколы. 9.1. Модели криптографического протокола.Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. 9.2. Протоколы аутентификации. Парольные системы и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и цифровой подписи. 9.3. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификация. Вопросы организации сетей засекреченной связи. 9.4. Протоколы с нулевым знанием.Доказательство с нулевым знанием. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым знанием на основе NP-сложных задач.	2	0	0

10	4	Заключение.Проблемы и перспективы исследований в области современной криптографии. Нерешенные задачи. Итоги изучения курса.	1	0	0
Всего			19	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	Криптоанализ классических шифров: простой замены, перестановки, шифра Виженера.	2	0	0
2	2	Линейный и дифференциальный криптоанализ S- DES.	2	0	0
3	2	Шифрование по алгоритму ГОСТ 28147-89.	3	0	0
4	3	Шифрование по алгоритму AES.	2	0	0
5	3	Шифрование по алгоритму IDEA.	2	0	0
6	3	Тестирование чисел на простоту.	2	0	0
7	4	Криптоанализ системы шифрования RSA при неправильном выборе параметров.	3	0	0
8	4	Генерация и проверка ЭЦП на основе стандарта Российской Федерации.	3	0	0
Всего			19	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	Шеннон К. Э., Добрушин Р. Л., Лупанов О. Б., Колмогоров А. Н.	Работы по теории информации и кибернетике: [сборник]	Москва: Издательство иностранной литературы, 1963

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	Ященко В. В.	Введение в криптографию: учеб. пособие	Москва: МЦНМО-ЧеРо, 1999
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Жданов О. Н.	Методика выбора ключевой информации для алгоритма блочного шифрования: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2013
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Шеннон К. Э., Добрушин Р. Л., Лупанов О. Б., Колмогоров А. Н.	Работы по теории информации и кибернетике: [сборник]	Москва: Издательство иностранной литературы, 1963

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

Э1	Клод Шеннон. Работы по теории информации и кибернетике.	http://pv.bstu.ru/crypto/shannon.pdf

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Самостоятельная работа предусматривает два вида деятельности магистранта: изучение теоретического курса и решение задач. Изучение теоретического курса предполагает подготовку реферата по источникам, представленным в списке литературы.

Комплекты задач выдаются преподавателем, ведущим практические занятия.

Проверяются во время последующих практических занятий в рамках контроля самостоятельных работ.

Форма промежуточной аттестации: устный зачет. Необходимо подготовить ответ на вопросы лектора.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации в зависимости от нозологии:

Для лиц с нарушениями зрения:

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

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

9.1 Перечень необходимого программного обеспечения

9.1.1	Программные комплексы.
9.1.2	1.Программный комплекс Classic.
9.1.3	Программный комплекс предназначен для решения задач криптоанализа шифров столбцовой перестановки, двойной перестановки, простой замены и шифра Виженера.
9.1.4	2.Программа DES.

9.1.5	Программа предназначена для зашифрования и расшифрования по алгоритму DES.При этом показываются результаты всех раундов.Программа позволяет также изучить лавинный эффект.
9.1.6	3.Программа Gost.exe.
9.1.7	Программа предназначена для зашифрования и расшифрования по алгоритму ГОСТ 28147-89. Пользователь может выбирать ключ и таблицы замен.
9.1.8	4.Программный комплекс Crypto.exe включает программы:
9.1.9	7.Целочисленный калькулятор,
9.1.10	8.Алгоритм Евклида,
9.1.11	9.Генератор BBS,
9.1.12	10.Программа проверки числа на простоту,
9.1.13	11.Программа факторизации,
9.1.14	12.Операции с точками эллиптической кривой.
9.1.15	5. Программа генерации и тестирования ключа для алгоритма блочного шифрования. Реализованы тесты Чезаро и Пирсона.
9.1.16	Программные комплексы подготовлены и используются.
9.1.17	
9.1.18	Пакет Microsoft Office, ОС Windows XP/7/8/10, браузер Google Chrome/Opera/Mozilla Firefox,
9.1.19	информационные справочные системы: google.com, yandex.ru и т.д.

9.2 Перечень необходимых информационных справочных систем

9.2.1	Не требуется.

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

Для проведения занятий требуется оборудованная доской аудитория и персональные компьютеры.