

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра математических методов и моделей в экономике

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.27 Математические методы защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

01.03.04 Прикладная математика
(код и наименование направления подготовки)

Математическое и компьютерное моделирование
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2023

Рабочая программа дисциплины «Б1.Д.Б.27 Математические методы защиты информации» рассмотрена и утверждена на заседании кафедры

Кафедра математических методов и моделей в экономике
наименование кафедры

протокол № 8 от "6" 02 2023г.

И.о. заведующего кафедрой

Кафедра математических методов и моделей в экономике
наименование кафедры



Н.П.Фот

Исполнители:


должность


подпись

В.И.Васянина
расшифровка подписи

должность

подпись

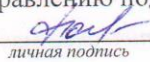
расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

01.03.04 Прикладная математика

код наименование


личная подпись


расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов


личная подпись

расшифровка подписи

Уполномоченный по качеству факультета


личная подпись

Н.А. Тычинина
расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование теоретических знаний о математических методах построения криптографических алгоритмов и практических навыков их применения для защиты информации.

Задачи:

- освоение основных понятий криптографии и математических методов защиты информации;
- ознакомление с наиболее распространенными типами;
- освоение математических методов построения криптографических протоколов идентификации и аутентификации;
- изучение математических методов построения алгоритмов электронной цифровой подписи;
- приобретение навыков шифрования, расшифрования информации;
- приобретение навыков реализации алгоритмов идентификации и аутентификации;
- приобретение навыков разработки собственного программного обеспечения для решения задач защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.13 Информационные технологии и программирование, Б1.Д.Б.15 Линейная алгебра и аналитическая геометрия, Б1.Д.Б.16 Дискретная математика и математическая логика, Б1.Д.Б.28 Программирование, Б1.Д.В.7 Технологии разработки программного обеспечения*

Постреквизиты дисциплины *Б2.П.В.П.3 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-1 Способен применять знание фундаментальной математики и естественно-научных дисциплин при решении задач в области естественных наук и инженерной практике	ОПК-1-В-6 Применяет фундаментальные разделы прикладной алгебры для реализации, анализа свойств и обоснованного выбора криптографических алгоритмов при решении задач защиты информации	Знать: разделы прикладной алгебры, применяемые для построения криптографических алгоритмов; алгоритмы криптографических методов защиты информации Уметь: применять разделы прикладной алгебры для реализации, анализа свойств и обоснованного выбора криптографических алгоритмов при решении задач защиты информации Владеть: навыками применения разделов прикладной алгебры для реализации, анализа свойств и обоснованного выбора криптографических алгоритмов при решении задач защиты информации
ОПК-2 Способен обоснованно выбирать,	ОПК-2-В-2 Применяет математический	Знать: разделы прикладной алгебры и алгоритмы криптографических методов

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надежность и качество функционирования систем	инструментарий для анализа и управления системами в различных отраслях	защиты информации, применяемые для анализа и управления системами защиты информации Уметь: применять знания разделов прикладной алгебры, криптографических алгоритмов защиты информации для анализа и управления системами защиты информации Владеть: навыками применения знаний разделов прикладной алгебры, криптографических алгоритмов защиты информации для анализа и управления системами защиты информации
ОПК-3 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-3-В-2 Использует принципы работы современных информационных технологий для разработки собственного программного обеспечения, формирования баз данных и управления ими, организации процедур защиты информации	Знать: программные средства и ИКТ, применяемые для решения задач криптографической защиты информации, криптографические методы, применяемые в программных средствах и ИКТ для защиты информации Уметь: применять программные средства и ИКТ для обработки информации, решения задач профессиональной деятельности с учетом требований к защите информации Владеть: навыками применения программных средств и ИКТ для обработки информации, решения задач профессиональной деятельности с учетом требований к защите информации
ОПК-4 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-4-В-2 Разрабатывает алгоритмы и создает на их основе собственные программные средства для решения прикладных задач обработки данных на ЭВМ	Знать: разделы прикладной алгебры, применяемые для построения криптографических алгоритмов; криптографические методы защиты информации Уметь: применять разделы прикладной алгебры для разработки алгоритмов и создания программных средств при решении практических задач с учетом требований защиты информации Владеть: навыками применения разделов прикладной алгебры для разработки алгоритмов и создания программных средств при решении практических задач с учетом требований защиты информации

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов		
	7 семестр	8 семестр	всего
Общая трудоёмкость	108	108	216
Контактная работа:	26,25	40,25	66,5
Лекции (Л)	14	20	34
Практические занятия (ПЗ)		20	20
Лабораторные работы (ЛР)	12		12
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к лабораторным занятиям; - подготовка к практическим занятиям; - подготовка к контрольным)	81,75	67,75	149,5
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	диф. зач.	диф. зач.	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Теория делимости	22	2		4	16
2	Сравнения, решение сравнений	34	4		4	26
3	Многочлены над конечными полями	32	4		2	26
4	Симметричные системы шифрования	20	4		2	14
	Итого:	108	14		12	82

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
5	Криптографические протоколы	20	4	4		12
6	Асимметричные криптосистемы	26	6	6		14
7	Электронная цифровая подпись	24	4	6		14
8	Надежность криптосистем	20	2	2		16
9	Цифровые сертификаты и инфраструктура открытых ключей	18	4	2		12
	Итого:	108	20	20		68

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	Всего:	216	34	20	12	150

4.2 Содержание разделов дисциплины

№ 1 Теория делимости Элементы теории делимости. Наибольший общий делитель, алгоритм Евклида. Непрерывные дроби, подходящие дроби. Наименьшее общее кратное. Простые числа, алгоритм Эратосфена получения простых чисел не превосходящих N . Каноническое разложение составного числа. Функция Эйлера. Сравнимые по модулю m числа. Тесты на простоту: пробное деление, тест Ферма, тест Миллера-Рабина.

№ 2 Сравнения, решение сравнений Сравнения, свойства сравнений, вычеты, полная система вычетов, приведенная система вычетов, теоремы Эйлера и Ферма.

Символ Лежанда, Якоби. Квадратичные вычеты.

Сравнения первой степени с одним неизвестным. Система сравнений первой степени. Китайская теорема об остатках.

Сравнения любой степени по простому и составному модулю. Сравнения второй степени.

№ 3 Многочлены над конечными полями Моноиды, группы, кольца, идеалы, поля, полиномиальные кольца над полями, полиномиальные коды, регистры сдвига. Примитивные элементы, базисы, представления конечных полей, первообразные корни, индексы и дискретные логарифмы. Рекуррентные последовательности. Характеристические функции кодовых последовательностей. Примитивные многочлены, неприводимые многочлены и их построение.

№ 4 Симметричные системы шифрования Простейшие системы шифрования (шифр замены, перестановки, шифры Вернама, Вижинера, гаммирование). Современные симметричные криптосистемы. Блочные и поточные шифры. Шифр DES, режимы работы DES, AES, ГОСТ 28147-89. Поточные шифры: РСЛОС, RC4. Стойкость криптографических систем и алгоритмов Энтропия, теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость. Вычислительная и временная сложность алгоритма.

№ 5 Криптографические протоколы Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Протоколы с нулевой передачей знаний. Схемы обязательств. Распределение ключей Выбор ключа, время жизни ключа, разделение секрета. Схемы обмена секретными ключами: Шамира, Диффи-Хеллмана.

Понятие эллиптической кривой (ЭК). Уравнение Вейерштрасса. Порядок ЭК. Сингулярные кривые. Эллиптические кривые и их свойства. Точки эллиптической кривой. Сложение точек. Протоколы основанные на эллиптических кривых.

№ 6 Асимметричные криптосистемы Общая схема функционирования систем с открытыми ключами, основанными на односторонних функциях. Криптосистема RSA и ее модификации. Криптосистема Эль Гамала (El Gamal). Криптосистема Рабина.

№ 7 Электронная цифровая подпись Целостность данных и аутентификация сообщений. Хэш-функции (MD4, SHA). Алгоритмы ЭЦП, основанные на односторонних функциях: RSA, Эль Гамала, Шнорра, Нибберга-Руппеля.

№ 8 Надежность криптосистем. Виды атак. Понятие и виды стойкости систем шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула Стойкость актуальных алгоритмов шифрования.

№ 9 Цифровые сертификаты и инфраструктура открытых ключей: Системы перераспределения доверия: PGP, SSL, X509 (PKIX), SPKI. Неявные сертификаты.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
------	--------------	---------------------------------	-----------------

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Подходящие дроби	2
2	1	Функция Эйлера	2
3	2	Решение линейных сравнений, систем линейных сравнений	4
4	3	Рекуррентные последовательности	2
5	4	Простейшие системы шифрования	2
		Итого:	12

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	5	Схемы обмена секретными ключами	2
2	5	Протоколы на эллиптических кривых	2
3	6	Асимметричные криптосистемы RSA	2
4	6	Асимметричные криптосистемы El Gamal	2
5	6	Криптосистема Рабина	2
6	7	Хэш-функции	2
7	7	Электронная цифровая подпись на основе RSA	2
8	7	Электронная цифровая подпись на основе El Gamal	2
9	8	Стойкость актуальных алгоритмов шифрования	2
10	9	Цифровые сертификаты X509	2
		Итого:	20

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2004, 2009.
2. Новиков, Ф. А. Дискретная математика для программистов [Текст] : учеб. для вузов / Ф. А. Новиков. - СПб. : Питер, 2009 - 384 с.
3. Вычислительно сложные задачи теории чисел [Текст] : учебное пособие / Е. А. Гречников [и др.]; Мос. гос. ун-т им. М. В. Ломоносова. - Москва : Изд-во Моск. ун-та, 2012. - 312 с
4. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 528 с.

5.2 Дополнительная литература

1. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст] : пер. с англ. / Г. Биркгоф, Т.К. Барти.- 2-е изд., стер. - СПб. : Лань, 2005. - 400 с.

Методические материалы

1. Василего, И. П. Теория чисел в криптографии [Текст] : методические указания / И. П. Василего; М-во образования Рос. Федерации, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. приклад. математики. - Оренбург : ГОУ ОГУ, 2004. - 20 с.
2. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Электронный ресурс] : методические указания к лабораторному практикуму / Т. Н. Шалкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 0.42 Мб). - Оренбург : ОГУ, 2006. - 44 с. - Загл. с тит. экрана. -Adobe Acrobat Reader 6.0

3. Сердюк, А. И. Криптография. Разработка приложений для шифрования информации [Электронный ресурс] : методические указания для студентов, обучающихся по программам высшего профессионального образования по специальности 090104.65 Комплексная защита объектов информатизации, 230101.65 Вычислительные машины, комплексы, системы и сети, направлению подготовки 090900.62 Информационная безопасность, профиль "Комплексная защита объектов информатизации" / А. И. Сердюк, О. Н. Яркова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 1.62 Мб). - Оренбург : ОГУ, 2012. - 98 с.

5.3 Периодические издания

Вестник компьютерных и информационных технологий : журнал. - М. : Агентство "Роспечать", 2023

Информационные технологии : журнал. - М. : Агентство "Роспечать", 2023

5.4 Интернет-ресурсы

- <http://www.securitylab.ru/> информационный портал по ИТ безопасности
- <http://www.citforum.ru/> форум по информационным технологиям, методам защиты информации
- <http://www.itlab.unn.ru/?dir=104> Лаборатория информационные технологии
- <http://window.edu.ru/> Единое окно доступа к образовательным ресурсам по теме «Криптографические методы защиты информации»
- http://window.edu.ru/catalog/resources?p_str=криптографические+методы
- <https://openedu.ru/course/hse/DATPRO/> он-лайн курс «защита информации»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС
2. Пакет офисных приложений LibreOffice
3. Программная система для организации видео-конференц-связи Webinar.ru

Профессиональные базы данных, Информационные справочные системы

1. Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Гло-сис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. – Электрон. дан. и прогр. – [Москва; Санкт-Петербург]. – Режим доступа осуществляется в локальной сети ОГУ.
2. SCOPUS [Электронный ресурс] : реферативная база данных / компания Elsevier. – Режим доступа: <https://www.scopus.com/>, в локальной сети ОГУ.
3. Web of Science [Электронный ресурс]: реферативная база данных / компания Clarivate Analytics. – Режим доступа : <http://apps.webofknowledge.com/>, в локальной сети ОГУ.
4. Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : <http://pravo.fso.gov.ru/ips/>, в локальной сети ОГУ.
5. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2023]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe
6. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2023]. – Режим доступа к системе в сети ОГУ для установки системы: [\\fileserver1!\CONSULT\cons.exe](http://fileserver1!\CONSULT\cons.exe)

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.