Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра геометрии и компьютерных наук

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.31 Криптографические методы защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Цифровые технологии
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины *«Б1.Д.Б.31 Криптографические методы защиты информации»* рассмотрена и утверждена на заседании кафедры

Кафедра геометрии и компьютерных наук
наименование кафедры

протокол № 6 от "17" февраля 2023 г.

Заведующий кафедрой
Кафедра геометрии и компьютерных наук — подпись — А.Е. Шухман
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Старший преподаватель — подпись — А.Н. Благовисная
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки — А.Е. Шухман
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

– формирование у обучающихся представлений о роли математики в развитии методов защиты информации, развитие навыков решения задач криптографии.

Задачи:

– освоение терминологического аппарата теории защиты информации и фундаментальных математических понятий криптологии;

– освоение базовых математических алгоритмов и методов, лежащих в основе методов защиты информации;

– изучение подходов к созданию современных криптосистем;

– приобретение навыков применения математических методов к решению прикладных задач защиты информации.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.3 Иностранный язык, Б1.Д.Б.18 Алгебра и теория чисел, Б1.Д.Б.20 Дискретная математика и математическая логика, Б1.Д.Б.27 Языки и технологии программирования*

Постреквизиты дисциплины: *Б1.Д.В.Э.3.1 Программирование WEB-приложений, ФДТ.2 Информационные технологии в экономике и управлении*

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-2 Способен проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности	ОПК-2-В-1 Владеет навыками научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке ОПК-2-В-2 Умеет решать научные задачи в связи с поставленной целью и в соответствии с выбранной методикой ОПК-2-В-3 Имеет практический опыт исследований в конкретной области профессиональной деятельности	**Знать:** - *основные источники (учебники, монографии, периодические издания, интернет-ресурсы и т.п.), отражающие современное состояние развития криптографических методов защиты информации;* **Уметь:** - *собирать, обрабатывать и анализировать публикации, содержащие теоретические сведения и практические результаты в области криптографии;*

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		Владеть: - *навыками анализа проблем в области криптографических методов защиты информации.*
ОПК-3 Способен самостоятельно представлять научные результаты, составлять научные документы и отчеты	ОПК-3-В-1 Знает принципы построения научной работы, современные методы сбора и анализа полученного материала, способы аргументации ОПК-3-В-2 Умеет представлять научные результаты, составлять научные документы и отчеты ОПК-3-В-3 Имеет практический опыт выступлений и научной аргументации в профессиональной деятельности	**Знать:** - *формулировки научных проблем в области криптографии;* **Уметь:** - *составлять описание результатов исследования криптографических конструкций;* **Владеть:** - *навыками интерпретации результатов исследования криптографических конструкций.*
ОПК-4 Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	ОПК-4-В-1 Знает базовые основы современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности ОПК-4-В-2 Умеет использовать математический аппарат в профессиональной деятельности ОПК-4-В-3 Имеет практический опыт применения современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	**Знать:** - *основы построения и реализации современных шифров;* **Уметь:** - *использовать современные языки программирования для реализации криптографических конструкций;* **Владеть:** - *методами реализации криптографических конструкций.*

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов

	7 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**35,25**	**35,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**72,75**	**72,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в криптографические методы защиты информации	16	4		0	12
2	Основы теоретико-информационной стойкости	12	4		0	8
3	Симметричное шифрование	30	4		6	20
4	Асимметричное шифрование	30	4		6	20
5	Электронная цифровая подпись	20	2		4	14
	Итого:	108	18		16	74
	Всего:	108	18		16	74

4.2 Содержание разделов дисциплины

№ 1 Введение в криптографические методы защиты информации

Предмет и объект защиты информации. Конфиденциальность, аутентичность, целостность. Криптология, криптография, криптоанализ. Исторические этапы развития криптологии и их характеристика. Примеры исторических шифров. Шенноновское описание традиционной криптосистемы. Классификация криптосистем. Группы методов атак на шифры.

№ 2 Основы теоретико-информационной стойкости

Понятие стойкости криптосистемы. Подходы к определению стойкости. Энтропия, ее свойства. Условная энтропия. Совершенная секретность по Шеннону, шифр Вернама. Ложные ключи и расстояние единственности.

№ 3 Симметричное шифрование

Традиционные шифры с симметричным ключом. Шифры подстановки и шифры перестановки. Блочные, поточные шифры. Синтез симметричных шифров. Требования, предъявляемые к созданию поточных шифров. Режимы использования поточных шифров: линейное (канальное) шифрование, предварительное шифрование, передача информации об используемом ключе. Синхронизация поточных шифров. Построение последовательностей с большим периодом в поточных шифрах. Требования, предъявляемые к созданию блочных шифров. Режимы использования блочных шифров. Слабости блочных шифров. Криптосистемы Фейстеля, DES, ГОСТ 28147-89, алгоритмы AES, ГОСТ 34.12-2018 и математический аппарат, используемый в них.

Управление ключами в симметричных криптоалгоритмах. Проблемы распределения ключей и методы их решения.

№ 4 Асимметричное шифрование

Идеи криптографии с открытым ключом. Односторонние функции. Математические задачи и проблемы, лежащие в основе асимметричной криптографии. Схема асимметричного шифрования. Распределение ключей. Алгоритм Диффи-Хеллмана. Алгоритм RSA. Схема шифрования Эль Гамаля. Схема шифрования Рабина.

№ 5 Электронная цифровая подпись

Понятие электронной подписи. Схема процедуры постановки и проверки электронной подписи. Понятие и свойства хэш-функции. Примеры схем ЭЦП. ЭЦП на основе сложности факторизации. ЭЦП на основе сложности дискретного логарифмирования

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Реализация исторических шифров подстановки и перестановки.	2
2	3	Реализация регистров сдвига.	2
3	3	Реализация S-блоков блочных шифров.	2
4	4	Реализация схемы Диффи-Хеллмана распределения ключей.	2
5	4	Реализация схем асимметричного шифрования.	4
6	4	Реализация схем ЭЦП.	4
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

2. Фомичев, В. М. Методы дискретной математики в криптологии: учебное пособие: [16+] / В. М. Фомичев. – Москва: Диалог-МИФИ, 2010. – 436 с: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=447668

3. Фороузан, Б. А. Математика криптографии и теория шифрования: учебное пособие: [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с.: ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428998

.

5.2 Дополнительная литература

1. Гультяева, Т. А. Основы защиты информации: учебное пособие: [16+] / Т. А. Гультяева. – Новосибирск: Новосибирский государственный технический университет, 2018. – 83 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730

2. Котов, Ю. А. Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: учебное пособие: [16+] / Ю. А. Котов. – Новосибирск: Новосибирский государственный технический университет, 2017. – 67 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574782

3. Пилиди, В. С. Математические основы защиты информации: учебное пособие: [16+] / В. С. Пилиди; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2019. – 309 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577894

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2022.

2. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2022.

5.4 Интернет-ресурсы

1. http://eqworld.ipmnet.ru/indexr.htm – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).

2. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.

3. «Введение в информационную безопасность» [Электронный ресурс]: онлайн-курс на платформе https://www.lektorium.tv/mooc – «Лекториум» / Разработчик курса: Московский государственный университет, режим доступа: https://www.lektorium.tv/course/23019.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС для рабочих станций, имеется лицензия, входит в реестр отечественного ПО.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Система управления учебным процессом Moodle, свободно распространяемая.
4. Программная система для организации видео-конференц-связи Webinar.ru, имеется лицензия, входит в реестр отечественного ПО.
5. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.
6. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей – Режим доступа: https://www.elibrary.ru/, в локальной сети ОГУ.
7. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа http://www.mathnet.ru/.
8. Система программирования Python, свободно распространяемая по лицензии PSFL.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного 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.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.