Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В. А. Бондаренко»

Кафедра математики и цифровых технологий

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.32 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 2026

Рабочая программа дисциплины «*Б1.Д.Б.32 Криптографические методы защиты информации*» рассмотрена и утверждена на заседании кафедры

математики и цифровых технологий
наименование кафедры

протокол № 7 от "19" марта 2026 г.

Заведующий кафедрой
математики и цифровых технологий _____ А. Е. Шухман
наименование кафедры *подпись* *расшифровка подписи*

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

Старший преподаватель _____ А. В. Михляева
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
главный библиограф _____ Т. С. Гасайтис
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
_____ С. Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Благовисная А. Н.
Михляева А. В., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цели освоения дисциплины: сформировать у обучающихся базовые знания о криптографических методах защиты информации и навыки их практического применения.

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.16 Алгебра и теория чисел, Б1.Д.Б.18 Дискретная математика и математическая логика, Б1.Д.Б.22 Основы программирования*

Постреквизиты дисциплины: *Б1.Д.В.Э.3.1 Программирование WEB-приложений*

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. **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,	ОПК-4-В-1 Знает базовые основы современного математического аппарата, связанного с	**Знать:** основы построения и реализации современных шифров. **Уметь:** использовать современные

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	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	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);* *– решение типовых задач;* *– самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *– изучение разделов курса в системе электронного обучения;* *– подготовка к лабораторным занятиям;* *– подготовка к тестам, опросам;* *– подготовка к рубежному контролю;* *– подготовка к промежуточной аттестации)*	**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	

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в криптографические методы защиты информации	16	4			12
2	Основы теоретико-информационной стойкости	12	4			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. – Библиогр.: с. 422-428. – ISBN 978-5-86404-234-2. – Текст: электронный.

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. – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст: электронный.

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. – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст: электронный.

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. – Библиогр. с 46. – ISBN 978-5-7782-3411-6. – Текст: электронный.

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. – Библиогр.: с. 301. – ISBN 978-5-9275-3363-3. – Текст: электронный.

4. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст]: учебное пособие / П. Б. Хорев. – 4-е изд., стер. – М.: Академия, 2008. – 256 с.

5. Домашев, А. В. Программирование алгоритмов защиты информации: учебное пособие / А. В. Домашев, В. О. Попов, Д. И. Правиков и др. – 2-ое изд., испр. и доп. – М.: Нолидж, 2000. – 288 с. – ISBN: 5-89251-102-2.

5.3 Периодические издания

1. Информатика и системы управления: журнал. – М.: Агентство «Роспечать», 2018-2026.
2. Информационные технологии в проектировании и производстве: журнал. – М.: Агентство «Роспечать», 2018-2026.
3. Мир ПК: журнал. – М.: Агентство «Роспечать», 2018-2026.
4. Программные продукты и системы: журнал. – М.: Агентство «Роспечать», 2018-2026.
5. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2018-2026.
6. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2018-2026.

5.4 Интернет-ресурсы

1. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.
2. http://www.exponenta.ru – математический сайт с большим количеством методических материалов по высшей математике и математическим компьютерным пакетам.
3. http://www.intuit.ru – сайт института дистанционного обучения «ИНТУИТ».

4. https://eqworld.ipmnet.ru/indexr.htm – международный научно-образовательный сайт «Мир математических уравнений».

5. https://mathhelpplanet.com/static.php – математический форум с обсуждением и решением задач.

6. https://mccme.ru/ – Московский центр непрерывного математического образования.

7. https://math.ru/ – научно-популярный математический сайт.

8. http://www.techlibrary.ru/books.htm – книги по математике в электронном виде.

9. https://archive.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по математике и другим дисциплинам.

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. – URL: https://redos.red-soft.ru/

2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения. – URL: https://ru.libreoffice.org/

3. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО. – URL: https://yandex.ru/

4. Программная система для организации видео-конференц-связи DION. – URL: https://diongo.ru/

5. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle». – URL: http://moodle.osu.ru

6. Автоматизированная интерактивная система сетевого тестирования (АИССТ). – URL: https://aist.osu.ru/cgi-bin/auth.cgi

7. Университетская платформа для сопровождения процедуры проведения экзаменационных испытаний с использованием дистанционных образовательных технологий. – URL: https://exam.osu.ru/

8. Система автоматизированной проверки текстов на наличие заимствований «Антиплагиат.Структура 5.0», имеется лицензия на 1 год. – URL: https://osu.antiplagiat.ru/

9. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей. – URL: https://www.elibrary.ru/

10. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – URL: http://www.mathnet.ru/

11. Wolfram|Alpha [Электронный ресурс]: база знаний и справочная система, включающая множество вычислительных алгоритмов. – URL: https://www.wolframalpha.com/

12. Большая Российская энциклопедия [Электронный ресурс]: универсальная энциклопедия, содержит статьи по всем областям знаний, справочники по персоналиям, словари. – URL: https://bigenc.ru/

13. Система компьютерной алгебры Sage – свободное программное обеспечение с лицензией GNU GPL. – URL: https://doc.sagemath.org/html/ru/tutorial/index.html

14. Математическое ПО для решения широкого спектра научных и прикладных задач SciLab, свободно распространяемая. – URL: https://soft.mydiv.net/win/files-Scilab.html

15. Система программирования Python, свободно распространяемая по лицензии PSFL. – URL: https://www.python.org/

16. Математическая система GeoGebra, свободно распространяемая по лицензии GPL. – URL: https://www.geogebra.org/classic?lang=ru

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.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

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