

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.38 Методы и средства криптографической защиты информации»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.01 Компьютерная безопасность

(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»

(наименование направленности (профиля)/специализации образовательной программы)

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год набора 2026

Рабочая программа дисциплины «Б1.Д.Б.38 Методы и средства криптографической защиты информации» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от "20" марта 2026 г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры  И.В. Влацкая
подпись расшифровка подписи

Исполнители:

Старший преподаватель
должность  А.Н. Благовисная
подпись расшифровка подписи

должность подпись расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по специальности

10.05.01 Компьютерная безопасность
код наименование  И.В. Влацкая
личная подпись расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

 С.А. Биктимирова
личная подпись расшифровка подписи

Уполномоченный по качеству института

 С.Н. Морозова
личная подпись расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

– формирование у обучающихся знаний и навыков в области применения методов и средств криптографии для защиты информации.

Задачи:

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

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

– изучение подходов к созданию современных криптосистем;

– приобретение навыков применения криптографических алгоритмов 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.14 Алгебра, Б1.Д.Б.22 Языки программирования, Б1.Д.Б.23 Методы программирования, Б1.Д.Б.40 Теоретико-числовые методы в криптографии

Постреквизиты дисциплины: Б1.Д.Б.39 Криптографические протоколы

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-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10-В-1 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами ОПК-10-В-2 Владеет навыками использования типовых криптографических алгоритмов	<u>Знать:</u> – математические методы, применяемые в криптографии; – теоретические основы построения и программной реализации современных шифров; – современные симметричные и асимметричные криптографические системы и криптографические стандарты их описывающие. <u>Уметь:</u> – применять и разрабатывать программные реализации криптографических

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		алгоритмов. Владеть: – навыками практического применения симметричных и асимметричных алгоритмов шифрования для защиты информации; – навыками использования электронной цифровой подписи (ЭЦП).

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
Общая трудоёмкость	108	108	216
Контактная работа:	46,25	53,25	99,5
Лекции (Л)	16	18	34
Лабораторные работы (ЛР)	30	34	64
Консультации		1	1
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); - изучение разделов курса в системе электронного обучения; - подготовка к лабораторным работам; - подготовка к тестам, опросам).	61,75	54,75	116,5
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	экзамен	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в криптографические методы защиты информации	24	4		6	14

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
2	Основы теоретико-информационной стойкости	26	4		6	16
3	Симметричное шифрование	58	8		18	32
	Итого:	108	16		30	62

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
4	Асимметричное шифрование	42	6		18	18
5	Электронная цифровая подпись	66	12		16	38
	Итого:	108	18		34	56
	Всего:	216	34		64	118

4.2 Содержание разделов дисциплины

№ 1 Введение в криптографические методы защиты информации

Понятие защиты информации. Предмет и объект защиты информации. Понятия конфиденциальности, аутентичности, целостности. Понятия криптологии, криптографии и криптоанализа. Смежные области криптографии. 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, основанные на схеме Фейстеля и подстановочно-перестановочных сетях, математический аппарат, используемый в них. Стандарт ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

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 Гамала. Схема шифрования Рабина.

№ 5 Электронная цифровая подпись

Понятие электронной подписи. Схема процедуры постановки и проверки электронной подписи. Понятие и свойства хэш-функции. Примеры хэш-функций. Стандарт ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». Примеры схем ЭЦП. ЭЦП на основе сложности факторизации. ЭЦП на основе сложности дискретного логарифмирования. Стандарт ГОСТ 34.10-2018. Информационная технология.

Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и основы теории эллиптических кривых.

Инфраструктура открытых ключей. Проблема аутентификации открытого ключа. Цифровой сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (СОС), приостановление действия сертификата. Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Исторические шифры сдвига, простой замены и Виженера.	2
2	1	Методы раскрытия исторических шифров.	4
3	2	Основы теоретико-информационной стойкости. Исследование учебных шифров на основе вероятностного подхода.	6
4	3	Поточные алгоритмы шифрования. Линейный регистр сдвига.	4
5	3	Схема Фейстеля. Учебный шифр на основе схемы Фейстеля.	4
6	3	Подстановочно-перестановочные сети (SP-сети). Учебный шифр на основе SP-сети.	4
7	3	Изучение стандарта ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».	2
8	3	Задача о безопасном хранении ключа и методы её решения.	4
9	4	Основные алгоритмы теории чисел, применяемые в асимметричной криптографии.	12
10	4	Алгоритм Диффи-Хеллмана.	2
11	4	Алгоритм RSA.	2
12	4	Алгоритм Эль-Гамала.	2
13	5	Изучение стандарта ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». Учебная хэш-функция.	2
14	5	ЭЦП RSA с извлечением сообщения и с использованием хэш-функции.	3
15	5	ЭЦП Эль-Гамала с извлечением сообщения и с использованием хэш-функции.	3
16	5	Основные алгоритмы теории эллиптических кривых, необходимые для программной реализации ЭЦП: задание эллиптической кривой над конечным полем, определение порядка группы точек эллиптической кривой, сложение точек эллиптической кривой, умножение точки эллиптической кривой на скаляр, определение порядка точки эллиптической кривой, поиск базовой точки кривой.	5
17	5	Изучение стандарта ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». ЭЦП Эль-Гамала на эллиптических кривых.	3
		Итого:	64

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. 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>
2. 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>
4. Сمارт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2024.
2. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2024.

5.4 Интернет-ресурсы

1. <https://znanierussia.ru/> – сайт Российского общества «Знание», который содержит интеллектуальный контент о достижениях в области науки, культуры и искусства и других сферах жизни.
2. <https://www.gost.ru/portal/gost/> – портал Федерального агентства по техническому регулированию и метрологии».

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет – веб-браузер Яндекс <https://yandex.ru/>.
4. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа – <http://aist.osu.ru>.
5. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе

обучения Moodle». – Режим доступа: <http://moodle.osu.ru>

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

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

9. 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.