Минобрнауки России

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

Кафедра математики и цифровых технологий

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.4.2 Криптографические протоколы»

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 2024

Рабочая программа дисциплины «*Б1.Д.В.Э.4.2 Криптографические протоколы*» рассмотрена и утверждена на заседании кафедры

Кафедра математики и цифровых технологий
наименование кафедры

протокол № 6 от "19" февраля 2024 г.

Заведующий кафедрой
Кафедра математики и цифровых технологий — 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 — личная подпись — А.Е. Шухман
код наименование *личная подпись* *расшифровка подписи*

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

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

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

– формирование системы знаний о правилах, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах, развитие навыков решения задач, связанных с преобразованием и передачей информации.

Задачи:

– изучение базовых криптографических протоколов, используемых при исследовании и построении современных алгоритмов, методов и моделей преобразования и защиты информации;

– овладение основными методами анализа и реализации криптографических протоколов;

– приобретение навыков решения теоретических и практических задач защищенной передачи информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.34 Дополнительные разделы алгебры, Б1.Д.В.3 Теоретико-числовые методы в криптографии*

Постреквизиты дисциплины: *Отсутствуют*

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
ПК*-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	ПК*-1-В-1 Обладает базовыми знаниями, полученными в области математических и (или)естественных наук, программирования и информационных технологий ПК*-1-В-2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности, в математике и информатике ПК*-1-В-3 Имеет практический опыт научно-исследовательской деятельности в математике и информатике	**Знать:** - *математические основы построения правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах;* **Уметь:** - *решать задачи алгебры, математической логики, теории чисел, дискретной математики, возникающие при построении различных криптографических протоколов;* **Владеть:** - *навыками интерпретации математических моделей процессов передачи и преобразования информации.*
ПК*-2 Способен использовать современные методы разработки и реализации конкретных	ПК*-2-В-1 Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов	**Знать:** - *криптографические стандарты;* - *типовые криптографические протоколы и основные требования*

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
алгоритмов на основе математических моделей на базе языков программирования и пакетов прикладных программ моделирования	прикладных программ моделирования ПК*-2-В-2 Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования ПК*-2-В-3 Имеет практический опыт разработки и реализации алгоритмов на базе языков и пакетов прикладных программ моделирования	*к ним;* *- протоколы идентификации;* *- протоколы передачи и распределения ключей;* **Уметь:** *- использовать симметричные и асимметричные криптоалгоритмы для построения криптографических протоколов;* *- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;* **Владеть:** *- методами реализации криптографических протоколов.*

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:	**34,25**	**34,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- 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 рубежному контролю)*	**73,75**	**73,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Общие сведения о криптографических протоколах	26	6		0	20
2	Протоколы идентификации и аутентификации	36	6		6	24
3	Протоколы распределения ключей	46	6		10	30
	Итого:	108	18		16	74

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	Всего:	108	18		16	74

4.2 Содержание разделов дисциплины

№ 1 Общие сведения о криптографических протоколах

Понятие протокола и его основные характеристики. Понятие криптографического протокола. Виды криптографических протоколов. Свойства безопасных криптографических протоколов.

№ 2 Протоколы идентификации и аутентификации

Понятия идентификации и аутентификации. Слабая и сильная аутентификация. Слабая аутентификация на основе фиксированных паролей. Атаки на фиксированные пароли. Правила составления паролей. Методы хранения паролей в системах. Схемы использования паролей. Сильная аутентификация типа «запрос-ответ». «Запрос-ответ» на основе симметричных и асимметричных алгоритмов шифрования. Протоколы аутентификации, использующие цифровую подпись. Протоколы идентификации, использующие технику доказательства знания.

№ 3 Протоколы распределения ключей

Типы протоколов распределения ключей: протоколы обмена ключей, протоколы открытого распределения ключей и схемы предварительного распределения ключей.

Протоколы передачи ключей с использованием симметричного шифрования. Двусторонние протоколы передачи ключей с использованием симметричного шифрования. Протоколы типа «запрос-ответ» и его модификации. Использование односторонней функции. «Бесключевой» протокол Шамира и его модификации. Трехсторонние протоколы: виды и атаки. Протоколы широкоротой лягушки, Yahalom, Нидхейма-Шредера, Отвей-Риса, Kerberos и их модификации.

Использование асимметричного шифрования для передачи ключей симметричных криптосистем. Протоколы без использования цифровой подписи: одношаговый протокол, протокол NSPK, протокол Woo-Lam. Смешанные протоколы. Использование цифровой подписи. Сертификаты открытых ключей.

Открытое распределение ключей и его отличие от распределения открытых ключей. Понятие безопасного аутентификационного протокола обмена ключами. Протокол Диффи-Хеллмана, его достоинства и недостатки. Атака «человек посередине» и методы защиты от неё. Аутентифицированные протоколы.

Предварительное распределение ключей. Проблема предварительного распределения ключей. Свойства схем предварительного распределения ключей. Примеры схем предварительного распределения ключей между n *абонентами. Схемы разделения секрета*.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Протоколы идентификации, использующие пароли.	2
2	2	Протоколы сильной аутентификации.	2
3	2	Протоколы идентификации, использующие технику доказательства знания.	2
4	3	Протоколы передачи ключей с использованием симметричного шифрования.	4
5	3	Протоколы передачи ключей с использованием асимметричного шифрования.	4
6	3	Схемы предварительного распределения ключей.	2

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

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. «МойОфис Образование» – набор приложений для работы с текстом, таблицами и презентациями в образовательных организациях.

3. Программная система для организации видео-конференц-связи MTS Link

4. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.

5. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей – Режим доступа: https://www.elibrary.ru/, в локальной сети ОГУ.

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

7. 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.