Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.32 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 2022

Рабочая программа дисциплины «*Б1.Д.Б.32 Методы и средства криптографической защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "14" марта 2022 г.

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

Исполнители:
доцент — *должность* — *подпись* — Е.И. Ряполова *расшифровка подписи*

должность — *подпись* — *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность
код наименование — *личная подпись* — И.В. Влацкая *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись — Н.Н. Бигалиева *расшифровка подписи*

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

№ регистрации 139042

© Ряполова Е.И., 2022
© ОГУ, 2022

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: являются изучение студентами указанных методов и средств развитие навыков решения задач криптографии.

Задачи:

- освоение 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 и средств к решению прикладных задач защиты информации и шифрованию.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.7 Алгебра, Б1.Д.Б.16 Языки программирования, Б1.Д.Б.17 Методы программирования, Б1.Д.Б.34 Теоретико-числовые методы в криптографии*

Постреквизиты дисциплины: *Б1.Д.Б.33 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 Знает основные задачи, решаемые криптографическими методами ОПК-10-В-2 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами ОПК-10-В-3 Владеет навыками использования типовых криптографических алгоритмов	**Знать:** основные задачи, решаемые криптографическими методами **Уметь:** корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами **Владеть:** навыками использования типовых криптографических алгоритмов при решении задач шифрования

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 7 зачетных единиц (252 академических часа).

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
Общая трудоёмкость	**108**	**144**	**252**
Контактная работа:	**47,25**	**87,25**	**134,5**
Лекции (Л)	16	52	68
Лабораторные работы (ЛР)	30	34	64
Консультации	1	1	2
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
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;* *- подготовка к экзамену*	**60,75**	**56,75**	**117,5**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	**экзамен**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в предмет	4	2	0	-	2
2	Симметричное шифрование	54	8	0	16	30
3	Криптосистемы с открытым ключом	48	4	0	14	30
	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	Электронная цифровая подпись	39	14		10	15
5	Последовательности над конечным полем	37	14	0	8	15
6	Булевы функции в криптографии	34	12	0	8	14
7	Инфраструктура открытых ключей	34	12	0	8	14
	Итого:	144	52		34	58
	Всего:	252	68		64	120

4.2 Содержание разделов дисциплины

Раздел №1. Введение в предмет

Понятие защиты информации. Различные аспекты безопасности информации. Безопасность информации и криптология. Этапы развития криптологии и ее основные понятия и определения. Роль математики в развитии методов защиты информации. Смежные области криптографии. Основная классификация криптосистем.

Раздел №2. Симметричное шифрование

Исторические шифры. Основы теоретико-информационной стойкости: Энтропия, ее свойства; условная энтропия; совершенная секретность по Шеннону, шифр Вернама; ложные ключи и расстояние единственности. Симметричные шифры: блочные, поточные, Фейстеля, DES, ГОСТ 28147-89. Распределение симметричных ключей, протоколы Барроуза, Нидхейма-Шредера, Цербер. Задача разделения секрета

Раздел №3. Криптосистемы с открытым ключом

Криптография с открытым ключом. Односторонние функции. Алгоритм RSA.Криптосистема Эль-Гамаля. Криптосистема на основе задачи об “укладке рюкзака”.

Раздел №4. Электронная цифровая подпись

Электронная цифровая подпись. Понятие и свойства хэш-функции.Электронная подпись как модификация RSA. Система ЭЦП Эль-Гамаля. Стандарты цифровой подписи.

Раздел №5. Последовательности над конечным полем

Рекуррентные уравнения. Однородные и неоднородные линейные рекуррентные уравнения. Полиномиальное представление последовательностей. Характеристический многочлен. Аннулирующие многочлены. Минимальные многочлены. Цикловая структура ЛРП. ЛРП максимального периода. Критерий. Примеры.

Раздел №6. Булевы функции в криптографии

Числовые и метрические характеристики булевых функций. Криптографические свойства булевых функций. Генерация булевых функций с заданными свойствами. Булевы функции в криптографических конструкциях.

Раздел №7 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	2	Исторические шифры: Цезаря, Виженера. Их реализация и раскрытие. Шифрование перестановкой, раскрытие.	6
2	2	Алгоритм Евклида, расширенный алгоритм Евклида, решение линейного диофантова уравнения с двумя переменными.	6
3	2	Вычисление мультипликативного обратного элемента в конечном поле: 1) с помощью РАЕ; 2) возведением в степень бинарным алгоритмом. Решение линейного сравнения с одной неизвестной: 1) с помощью РАЕ; 2) умножением на мультипликативный обратный.	6
4	2	Решение системы линейных сравнений с одной переменной на основе греко-китайской теоремы об остатках.	6

5	2	Вычисление значения многочлена над конечным полем в точке по схеме Горнера. Разделение секрета по схеме Шамира: 1) получение долей; 2) восстановление ключа по допустимому количеству фрагментов: а) решением системы линейных уравнений по методы Гаусса; б) с помощью интерполяционной формулы Лагранжа.	6
6	2	Задача о безопасном хранении ключа (на основе греко-китайской теоремы): 1) получение долей; 2) восстановление ключа.	6
7	3	Вычисление значений символов Лежандра и Якоби. Вероятностные тесты простоты: 1) на основе малой теоремы Ферма; 2) Соловея-Штрассена; 3) Рабина-Миллера.	6
8	3	Генерация простых чисел. Возведение в степень. Алгоритм RSA.	6
9	6	НОД и расширенный алгоритм Евклида для многочленов. Алгебра многочленов. Генерация неприводимых многочленов. Порядок многочлена.	6
10	5	Решение линейного рекуррентного уравнения, вычисление периода последовательности. Реализация линейного регистра сдвига.	6
11	6	Проверка криптографических свойств булевых функций, генерация функций с заданными свойствами.	8
		Итого:	64

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Бабаш, А. В. Криптография. – М.: Солон-Пресс, 2007. – 512 с.

5.2 Дополнительная литература

1. Смарт, Н. Криптография. – М.: Техносфера, 2006. – 528 с.

5.3 Периодические издания

1 Информатика и системы управления: журнал. - М. : Агентство "Роспечать", 2022

2 Вестник компьютерных и информационных технологий: журнал. - М. : Агентство "Роспечать", 2022

3 Информационные технологии: журнал. - М. : Агентство "Роспечать", 2022

5.4 Интернет-ресурсы

1 https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii – «Coursera», МООК: Методы и средства защиты информации

2 Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Глосис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. - Электрон. дан. и прогр. - [Москва; Санкт-Петербург], [1999–2013]. – Загл. с экрана.

3 ProQuest Dissertations & Theses A&I [Электронный ресурс] : база данных диссертаций. – Режим доступа : https://search.proquest.com/.

4 Web of Science [Электронный ресурс]: реферативная база данных / компания Clarivate Analytics. – Режим доступа : http://apps.webofknowledge.com/. – Загл. с экрана.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows
2. Open Office/LibreOffice – свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. MicrosoftVisualStudio – среда разработки приложений.

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки модели Intel Celeron;
- системные блоки модели Intel Pentium Core 2 Duo;
- мониторы модели Samsung 793 DF.