УТВЕРЖДЕНО

решением Учёного совета факультета математики, информационных и авиационных технологий

от «21» мая 2024 г., протокол № 5/24

Председатель _____/ М.А. Волков

«21» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Криптография**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра телекоммуникационных технологий и сетей
Курс	3 - очная форма обучения; 3 - заочная форма обучения

Направление (специальность): 09.03.02 Информационные системы и технологии
Направленность (профиль/специализация): Разработка информационных систем
Форма обучения: очная, заочная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Липатова Светлана Валерьевна	Кафедра телекоммуникационных технологий и сетей	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

·приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;

·знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

·освоение основных методов выбора алгоритмов для различных применений и оценки их качества;

·дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;

·дать основы математических методов, используемых в криптоанализе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Криптография» относится к числу дисциплин блока Б1.В.1.ДВ.07, предназначенного для студентов, обучающихся по направлению: 09.03.02 Информационные системы и технологии.

В процессе изучения дисциплины формируются компетенции: ПК-10.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Инфокоммуникационные системы и сети, Операционные системы, Информационные технологии, Преддипломная практика, Проектная деятельность, Технологии дополненной реальности, Управление программно-аппаратными средствами информационных систем, Выполнение и защита выпускной квалификационной работы.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-10 Способен управлять программно-аппаратными средствами информационных систем	**знать**: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; **уметь**: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	числе с использованием компьютерных программ; **владеть**: навыками эффективного шифрования и программно-аппаратными средствами защиты информации.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		6
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	36	36
Аудиторные занятия:	36	36
Лекции	18	18
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	18	18
Самостоятельная работа	72	72
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт
Всего часов по дисциплине	108	108

Форма обучения: заочная

Вид учебной работы	**Количество часов (форма обучения заочная)**	
	Всего по плану	**В т.ч. по семестрам**
		8
1	**2**	**3**
Контактная работа обучающихся с преподавателем в соответствии с УП	12	12
Аудиторные занятия:	12	12
Лекции	6	6
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	6	6
Самостоятельная работа	92	92
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет (4)	Зачет
Всего часов по дисциплине	108	108

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	**Всего**	**Виды учебных занятий**					**Форма текущего контроля знаний**
		Аудиторные занятия			**Занятия в интерактивной форме**	**Самостоятельная работа**	
		Лекции	**Практические занятия, семинары**	**Лабораторные работы, практикумы**			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Раздел 1. Математическая модель шифров							
Тема 1.1. Шифры замены и перестановки	12	2	0	2	0	8	Тестирование
Тема 1.2. Математич	12	2	0	2	0	8	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
еские модели открытых текстов							
Раздел 2. Надежность шифров							
Тема 2.1. Совершенные шифры	12	2	0	2	0	8	Тестирование
Тема 2.2. Вопросы имитостойкости шифров	12	2	0	2	0	8	Тестирование
Тема 2.3. Шифры, не распространяющие искажений	12	2	0	2	0	8	Тестирование
Раздел 3. Схемы разделения секрета							
Тема 3.1. Пороговые схемы разделения секрета	12	2	0	2	0	8	Тестирование
Тема 3.2. Схемы разделения секрета с произвольной структурой доступа	12	2	0	2	0	8	Тестирование
Раздел 4. Блочные шифры							
Тема 4.1. Симметричные блочные шифры	12	2	0	2	0	8	Тестирование
Тема 4.2. Асимметричные шифры	12	2	0	2	0	8	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Итого подлежит изучению	108	18	0	18	0	72	

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: заочная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Математическая модель шифров							
Тема 1.1. Шифры замены и перестановки	12	1	0	1	0	10	Тестирование
Тема 1.2. Математические модели открытых текстов	12	1	0	1	0	10	Тестирование
Раздел 2. Надежность шифров							
Тема 2.1. Совершенные шифры	12	1	0	1	0	10	Тестирование
Тема 2.2. Вопросы имитостойкости шифров	12	1	0	1	0	10	Тестирование
Тема 2.3. Шифры, не распространяющие	12	1	0	1	0	10	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
искажений							
Раздел 3. Схемы разделения секрета							
Тема 3.1. Пороговые схемы разделения секрета	12	1	0	1	0	10	Тестирование
Тема 3.2. Схемы разделения секрета с произвольной структурой доступа	10	0	0	0	0	10	Тестирование
Раздел 4. Блочные шифры							
Тема 4.1. Симметричные блочные шифры	11	0	0	0	0	11	Тестирование
Тема 4.2. Асимметричные шифры	11	0	0	0	0	11	Тестирование
Итого подлежит изучению	104	6	0	6	0	92	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Математическая модель шифров

Тема 1.1. Шифры замены и перестановки

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров.

Тема 1.2. Математические модели открытых текстов

Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе запретных m-грамм.

Раздел 2. Надежность шифров

Тема 2.1. Совершенные шифры

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Тема 2.2. Вопросы имитостойкости шифров

Подмена шифрованного сообщения. Имитация шифрованного сообщения. Имитостойкость шифра. Нижние оценки вероятности имитации и подмены сообщения. Примеры совершенных имитостойких шифров.

Тема 2.3. Шифры, не распространяющие искажений

Шифры, не распространяющие искажений типа замены знаков. Метрика Хэмминга на открытых и шифрованных текстах. Определение шифра, не распространяющего искажений типа замены знаков. Эквивалентные условия шифра, не распространяющего искажений типа замены знаков. Понятие изометрии. Теорема А.А.Маркова.

Раздел 3. Схемы разделения секрета

Тема 3.1. Пороговые схемы разделения секрета

Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая

схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n- разрядных равновесных двоичных кодов.

Тема 3.2. Схемы разделения секрета с произвольной структурой доступа

Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера. Схема Ито-Саито-Нишизеки.

Раздел 4. Блочные шифры

Тема 4.1. Симметричные блочные шифры

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES. Режимы использования блочных шифров. Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов.

Тема 4.2. Асимметричные шифры

Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамаля. Ограничения на параметры системы. Модификация шифра Эль-Гамаля на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Электронная подпись. Общие положения. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем. Примеры электронных подписей. Подпись Фиата-Шамира. Подпись Эль-Гамаля. Подпись RSA. Подпись Шнорра. Одноразовые электронные подписи.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами
Цели: Приобретение навыков шифрования информации с использованием простейших методов шифрования.
Содержание: 1. Разработать алгоритм и составить программу, позволяющую закодировать любой текст одним из вышеизложенных методов и выполнить обратное преобразование. Метод, которым

необходимо зашифровать исходную информацию, выбирается в соответствии с вариантом из таблиц 1.1, 1.2, 1.3. Язык программирования выбирается произвольно. 2. Осуществить вывод на экран или принтер полученной криптограммы. 3. Провести дешифрование данной криптограммы, в результате должен быть получен исходный текст. 4. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Шифр гаммирования
Цели: Освоение принципов шифрования гаммированием, изучение свойств генератора псевдослучайных чисел, программная реализация метода гаммирования
Содержание: 1. Выбрать в таблице 2.1 параметры генератора ПСЧ: A, C, T0, b в соответствии с вариантом. 2. Разработать программу шифрования и дешифрования текста. 3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом. Рекомендуется для представления символов исходного текста использовать стандартную кодировку символов. 4. Произвести изменение одного или несколько параметров генератора случайных чисел, осуществить получение шифрограммы и сравнение ее с предыдущим вариантом. 5. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Сеть Фейштеля
Цели: изучить принципы работы сети Фейштеля, научиться шифровать информацию посредством использования блочного криптоалгоритма
Содержание: 1. Выбрать из таблицы 3.1 параметры сети Фейштеля в соответствии с вариантом. 2. Разработать программу шифрования и дешифрования текста блоками, В программе предусмотреть ввод криптографического ключа, вычисление образующей функции, зависящей от материала ключа и части блока. 3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом. 4. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Изучение алгоритма RSA
Цели: Освоить механизм шифрования и дешифрования данных в криптографической системе с открытыми ключами RSA.
Содержание: 1. Разработать программу, осуществляющую шифрование и дешифрование сообщения алгоритмом RSA. Ключи генерируются на основе чисел p и q, значения которых 16 выбирается из таблицы 4.1 в соответствии с вариантом. При выборе числа e использовать минимально возможное 2. Исходное сообщение M может состоять из символов. как русского, так и любого другого алфавита. 3. Обеспечить вывод ключей и зашифрованного текста. 4. В программе предусмотреть проверку, являются ли два числа взаимно простыми. 5. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Создание электронной подписи в документе
Цели: разработка процедур выработки и проверки электронной цифровой подписи (ЭЦП) сообщений на базе асимметричного криптографического алгоритма с применением функции хеширования.
Содержание: 1. Выбрать из таблицы 5.1 в соответствии с вариантом алгоритм вычисления хэш-функции (контрольной суммы). 2. Реализовать программную реализацию алгоритма создания и проверки электронно-цифровой подписи. 3. Подписать текстовое сообщение 4. Проверить

правильность ЭЦП. 5. Внести изменения в сделанную подпись. Убедится, что подпись не является подлинной. 6. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Защита графического файла с помощью цифрового водяного знака
Цели: Изучение стеганографических методов защиты информации. Реализация программы с использованием стеганографических принципов защиты информации
Содержание: 1. Написать программу внедрения и извлечения скрытой информации в BMP-файлы с использованием стеганографических (LSB) алгоритмов. В качестве контейнера использовать графический формат BMP. В алгоритме LSB для четных вариантов число используемых младших бит - 2 бита, использовать метод LSB-R, для нечетных вариантов число используемых младших бит - 1 бит, использовать метод LSB-M. 2. Результаты работы оформить в виде отчета.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Парольная защита
Цели: изучение принципов организации парольной защиты программ, ознакомление с видами паролей, реализация парольной защиты
Содержание: 1. Изучить существующие методы парольной защиты 2. Выбрать метод парольной защиты в соответствии с заданным вариантом. 3.Разработать алгоритм и программную реализацию выбранного метода парольной защиты с использованием демонстрационных возможностей выбранного языка программирования. 4. Оформить отчет.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
Реализация протокола Диффи- Хеллмана на эллиптических кривых
Цели: изучение особенностей реализации криптографических протоколов распределения ключей, асимметричной криптографии на эллиптических кривых, разработка системы распределения криптографических ключей
Содержание: 1. Выбрать коэффициенты a,b и модуль p эллиптической кривой, координаты x, y точки G, а также секретные значения k1, k2 абонентов из таблицы 8.1 в соответствии с вариантом. 3.Разработать программную реализацию метода Диффи-Хеллмана. Предусмотреть проверку эллиптической кривой по формуле (8.2). Исходными данными являются параметры кривой, координаты точки и секретные значения каждого участника обмена. Результат работы программы – координаты произведения точки G на число, которые должны совпасть у каждого из участников. 4. Оформить отчет.
Результаты: Код, отчет
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/1344

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных

шифров.

2. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.

3. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.

4. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.

5. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.

6. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

7. Детерминированная модель открытого текста.

8. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

9. Алгебраическая и вероятностная модели шифров.

10. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр, шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

11. Понятие опорного шифра, степени опорного шифра. Случайный и детерминированный генераторы ключевого потока. Примеры генераторов.

12. Критерий для шифров, не распространяющеих искажений типа пропуска знаков, в классе эндоморфных шифров.

13. Понятие имитации сообщений. Определение вероятности Рим. Нижняя оценка для вероятности имитации сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой имитации сообщений.

14. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом.

15. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом.

16. Схема Диффи-Хеллмана.

17. Алгоритм быстрого возведения в степень. Задачи, приводящие к криптографии с открытым ключом и их решение.

18. Совершенные имитостойкие шифры замены с неограниченным ключом.

19. Понятие подмены сообщений. Определение вероятности Рподм. Нижняя оценка для вероятности подмены сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой подмены сообщений.

20. Шифры, не распространяющие искажений типа вставки знаков

21. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия.

22. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков.

23. Понятие изометрии. Свойства изометрий.

24. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия.

25. Методы взлома шифров, основанных на дискретном логарифмировании: Метод исчисления порядка.

26. Методы взлома шифров, основанных на дискретном логарифмировании: Полный перебор, метод «Шаг младенца, шаг великана».

27. Рюкзачные криптосистемы.

28. Шифр RSA.

29. Вероятностный шифр Эль-Гамаля.

30. Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ.

31. Схема разделения секрета Шамира.

32. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

33. Схема разделения секрета на основе китайской теоремы об остатках.

34. Криптоанализ симметричных блочных шифров.

35. Шифр “Магма” из ГОСТ Р 34.12-2015.

36. Режимы использования симметричных блочных шифров.

37. Слабые ключи итеративного блочного шифра.

38. Построение цикловой функции. Входное и выходное отображения.

39. Шифры Фейстеля и их обратимость.

40. Итеративные блочные шифры. Обратимость итеративного блочного шифра.

41. Электронная подпись Шнорра.

42. Электронная подпись с доверенным посредником на основе симметричной криптосистемы.

43. Электронная подпись Эль-Гамаля.

44. Электронная подпись Фиата-Шамира.

45. Электронные деньги на основе RSA.

46. Электронная подпись RSA.

47. Криптографические хеш-функции. Способы построения криптографических хеш- функций.

48. Хеш-функции. Требования, предъявляемые к хеш-функциям.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Математическая модель шифров			
Тема 1.1. Шифры замены и перестановки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 1.2. Математические	Проработка учебного материала с	8	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
модели открытых текстов	использованием ресурсов учебно-методического и информационного обеспечения дисциплины.		
Раздел 2. Надежность шифров			
Тема 2.1. Совершенные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 2.2. Вопросы имитостойкости шифров	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 2.3. Шифры, не распространяющие искажений	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Раздел 3. Схемы разделения секрета			
Тема 3.1. Пороговые схемы разделения секрета	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 3.2. Схемы разделения секрета с произвольной структурой доступа	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Раздел 4. Блочные шифры			
Тема 4.1. Симметричные блочные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 4.2. Асимметричные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование

Форма обучения: заочная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Математическая модель шифров			
Тема 1.1. Шифры замены и перестановки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Тема 1.2. Математические модели открытых текстов	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Раздел 2. Надежность шифров			
Тема 2.1. Совершенные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Тема 2.2. Вопросы имитостойкости шифров	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Тема 2.3. Шифры, не распространяющие искажений	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Раздел 3. Схемы разделения секрета			
Тема 3.1. Пороговые схемы разделения секрета	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Тема 3.2. Схемы разделения секрета с произвольной структурой доступа	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 4. Блочные шифры			
Тема 4.1. Симметричные блочные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	11	Тестирование
Тема 4.2. Асимметричные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	11	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рацеев Сергей Михайлович. Математические методы защиты информации : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 543 с. - (Высшее образование). - ISBN 978-5-8114-8589-5 (в пер.). / .— ISBN 1_258181

2. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 1 / А. М. Иванцов, В. Г. Козловский ; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 776 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1396. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_36065

дополнительная

1. Жарков А. В. Криптографические протоколы : учеб.-метод. рекомендации по выполнению лаб. работ / А. В. Жарков ; УлГУ, ФМиИТ, Каф. прикл. математики. - Ульяновск : УлГУ, 2011. - ил. - Загл. с экрана. - Имеется печ. аналог. - Электрон. текстовые дан. (1 файл : 1,99 Мб). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_1388

2. Рацеев С. М. Лабораторный практикум по криптографическим протоколам / С. М. Рацеев ; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - 2019. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 173 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1344. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_35988

3. Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А. П. Кирпичников, З. М. Хайбуллина ; А. П. Кирпичников, З. М. Хайбуллина. - Казань : Казанский национальный исследовательский технологический университет, 2016. - 100 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Гарантированный срок размещения в ЭБС до 18.01.2022 (автопролонгация). - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/79313.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-7882-2052-9. / .— ISBN 0_145623

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптография» для студентов направления подготовки 09.03.02«Информационные системы и технологии» / С. М. Рацеев. - 2022. - 9 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13326. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_475949.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Alt Linux
- LibreOffice

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ

ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент Кандидат технических наук, Доцент	Липатова Светлана Валерьевна
	Должность, ученая степень, звание	ФИО