МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине
по дисциплине «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов направления подготовки
10.03.01 Информационная безопасность
направленность (профиль) Безопасность компьютерных систем

Пятигорск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. Цель и задачи изучения дисциплины

Цель дисциплины: формирование набора универсальных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачи дисциплины: ознакомить студентов с современными системами шифрования на основе симметричных и асимметричных алгоритмов; научить выбирать параметры псевдослучайных последовательностей для генерирования криптостойких ключей; изучить стандарты систем шифрования; изучить криптографические протоколы.

2. Оборудование и материалы

Для проведения практических занятий необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам; интерактивная доска.

3. Наименование лабораторных работ

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
5 семестр			
1	Лабораторная работа 1. Программная реализация вычисления наибольшего общего делителя двух чисел.	1,5	
2	Лабораторная работа 2. Программная реализация расширенного алгоритма Евклида.	1,5	
3	Лабораторная работа 3. Применение расширенного алгоритма Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии.	1,5	
4	Лабораторная работа 4. Операции над матрицами вычетов.	1,5	
5-6	Лабораторная работа 5. Программная реализация генераторов простых чисел.	1,5	
7	Лабораторная работа 6. Разложение чисел на простые множители.	1,5	
8	Лабораторная работа 7. Решение систем уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.	1,5	
13	Лабораторная работа 8. Программная реализация классических шифров с симметричным ключом.	3	
	Итого за 5 семестр	**13,5**	
6 семестр			
10	Лабораторная работа 9. Программная реализация основных компонентов современных шифров с симметричным ключом.	1,5	

21	Лабораторная работа 10. Программная реализация шифра DES.	3	
24	Лабораторная работа 11. Подготовка к реализации шифра RSA.	1,5	
25	Лабораторная работа 12. Программная реализация шифра RSA.	3	
29-31	Лабораторная работа 13. Программная реализация ЭЦП.	1,5	
32-33	Лабораторная работа 14. Программная реализация криптографических протоколов.	1,5	
	Итого за 6 семестр	12	
	Итого	**25,5**	

4. Содержание лабораторных работ

5 семестр

Лабораторная работа 1. Программная реализация алгоритма Евклида для вычисления наибольшего общего делителя двух чисел.

Цель работы: .освоить применение алгоритма Евклида.

Задание к работе: используя алгоритм Евклида, создать программу, которая для чисел *a* и *b* определяет наибольший общий делитель. Подготовить отчет по работе. В отчете описать алгоритм Евклида, структуру представления данных в программе, входные и выходные параметры функции.

Контрольные вопросы

1. Дать определение простого и составного числа.
2. Сформулировать свойства делимости целых чисел.
3. Дать определение общего делителя и наибольшего общего делителя.
4. Сформулировать теорему о делении двух целых чисел.
5. Сформулировать алгоритм Евклида.

Лабораторная работа 2 Программная реализация расширенного алгоритма Евклида

Цель работы. Научиться программно реализовывать расширенный алгоритм Евклида

Задание к работе

Пусть число *d* - наибольший общий делитель для целых чисел *a* и b. Используя расширенный алгоритм Евклида, создать программу для определения таких двух чисел *x* и y, для которых выполняется равенство d = ax + by.

Подготовить отчет по работе. В отчете описать расширенный алгоритм Евклида, описать структуру представления данных в программе, основные функции программы, назначение функций, входные и выходные параметры функций.

Контрольные вопросы

1. Сформулировать цель расширенного алгоритма Евклида.
2. Для решения каких задач криптографии используется расширенный алгоритм Евклида?
3. Сформулировать основные шаги расширенного алгоритма Евклида.

Лабораторная работа 3 Применение расширенного алгоритма Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии

Цель работы. Научиться применять расширенный алгоритм Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии

Задание к работе

Используя расширенный алгоритм Эвклида, составить программу для решения задачи в соответствии с номером варианта.

Номера вариантов	Задача
1, 4, 7, 10, 13, 16	решение линейного диофантового уравнения (вывести первые десять решений)
2, 5, 8, 11, 14, 17	вычисление мультипликативной инверсии (с проверкой ее существования)
3, 6, 9, 12, 15, 18	решение уравнения сравнения

Контрольные вопросы

1. Покажите различие между Z и Z_n. Какое из этих множеств может содержать отрицательные целые числа? Как мы можем отобразить целое число из Z в целое число из Z_n?
2. Приведите пример целого числа с единственным делителем. Приведите пример целого числа только с двумя делителями. Приведите пример целого числа с более чем двумя делителями.
3. Определите наибольший общий делитель двух целых чисел. Какой алгоритм может эффективно найти наибольший общий делитель?
4. Что такое линейное диофантово уравнение двух переменных? Сколько решений может иметь такое уравнение? Как могут быть найдены решения?
5. Что такое оператор по модулю? Перечислите свойства операций по модулю.
6. Определите сравнение и перечислите его свойства.
7. Определите систему вычетов.
8. Дайте определение аддитивной инверсии и мультипликативной инверсии чисел a и b в Z_n.
9. Какова разница между множеством Z_n и множеством Z_n*? В каком множестве каждый элемент имеет аддитивную инверсию? В каком множестве каждый элемент имеет мультипликативную инверсию?
10. Какой алгоритм используется, чтобы найти мультипликативную инверсию целого числа b в Z_n? При выполнении какого условия такая инверсия существует?

11. Какой алгоритм может использоваться, чтобы решить линейное сравнение?

Лабораторная работа 4. Операции над матрицами вычетов

Цель работы. Изучить основные операции над матрицами вычетов

Задание к работе

Программно реализовать операции сложения и умножения матриц по модулю, а также нахождение мультипликативной инверсии матрицы о заданному модулю.

Лабораторная работа 5. Программная реализация генераторов простых чисел

Цель работы. Научиться генерировать простые числа

Задание к работе

Написать подпрограмму генерации простого числа в заданном диапазоне, используя алгоритм, определяемый номером варианта.

Вариант задания определяется порядковым номером студента в списке группы.

№ варианта	Используемый алгоритм
1	Решено Эратосфена
2	Комбинация теории делимости и теста Миллера-Рабина
3	Тест Миллера-Рабина
4	Испытание квадратным корнем
5	Комбинация теории делимости и теста Миллера-Рабина
6	Тест Ферма
7	Решено Эратосфена
8	Испытание квадратным корнем
9	Детерменированный алгоритм – испытание на делимость (с использованием массива известных простых чисел от 1 до 100)
10	Тест Миллера-Рабина
11	Тест Ферма
12	Решено Эратосфена
13	Тест Ферма
14	Испытание квадратным корнем

Контрольные вопросы

1. В чем разница между детерменированными и вероятностными алгоритмами проверки чисел на простоту?
2. Какую задачу решает решето Эратосфена? В чем суть данного алгоритма?
3. Что задает число $\varphi(n)$? По каким правилам оно вычисляется? Чему равно $\varphi(101)$, $\varphi(121)$?
4. Сформулируйте малую теорему Ферма. Каковы приложения этой теоремы?
5. Сформулируйте теорему Эйлера. Каковы приложения этой теоремы?
6. Какие простые числа называются простые числа Мерсенны и Ферма?
7. Приведите примеры детерменированных алгоритмов проверки чисел на простоту.

8. Приведите примеры вероятностных алгоритмов проверки чисел на простоту.
9. Как повысить вероятность правильного ответа при использовании теста Ферма?
10. На каком свойстве базируется испытание числа на простоту квадратным корнем?
11. Какие алгоритмы проверки чисел на простоту являются эффективными, а какие нет?

Лабораторная работа 6. Разложение чисел на простые множители

Цель работы – изучение методов разложения чисел на простые множители, алгоритмов возведения в степень по модулю.

Задание к работе: написать программу для решения задачи теории чисел в соответствии с номером варианта.

Вариант задания определяется порядковым номером студента в списке группы.

№ варианта	Используемый алгоритм
1	Разложение числа на простые множители методом проверки делением.
2	Метод Ферма разложения числа на нетривиальные множители.
3	PO (Rho) – метод Полларда разложения числа на множители.
4	Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
5	Нахождение мультипликативной инверсии заданного числа по заданному простому модулю с использованием малой теоремы Ферма.
6	Разложение числа на простые множители методом проверки делением.
7	Метод Ферма разложения числа на нетривиальные множители.
8	Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
9	PO (Rho) – метод Полларда разложения числа на множители.
10	Нахождение мультипликативной инверсии заданного числа по заданному простому модулю с использованием малой теоремы Ферма.
11	Разложение числа на простые множители методом проверки делением.
12	Метод Ферма разложения числа на нетривиальные множители.

Контрольные вопросы

1. Сформулируйте основную теорему арифметики.
2. Перечислите методы разложения на множители. Какой из методов раскладывает число на простые множители?
3. Объясните суть алгоритма разложения на множители проверкой делением.
4. На каком факте основан метод Ферма разложения на множители?
5. Объясните основные шаги алгоритма разложения на множители методом Ферма.
6. На каком положении базируется PO (Rho) – метод Полларда?
7. Какова [illegible] метода Полларда?

Лабораторная работа 7. Решение систем уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках

Цель работы – изучение методов решения систем уравнений сравнения с одной неизвестной и различными модулями.

Задание к работе: написать программу для решения системы уравнений сравнения с одной неизвестной и различными модулями.

Контрольные вопросы

1. Сформулируйте китайскую теорему об остатках.
2. Приведите примеры практических задач, решаемых с помощью китайской теоремы об остатках

Лабораторная работа 8. Программная реализация классических шифров с симметричным ключом

Цель работы. Изучить классические шифры с симметричным ключом и научиться применять их для шифрования и дешифрования текстовой информации.

Задание к работе

Написать программу «Шифрование текста», которая позволяет зашифровывать и расшифровывать текстовый файл или сообщение. Шифрование реализует преобразование текста в соответствии с вариантом задания.

Вариант задания определяется порядковым номером студента в списке группы.

№ варианта	Способ шифрования	Алфавит исходного текста
1	мультипликативный шифр замены	заглавные латинские буквы
2	аффинный шифр замены	строчные латинские буквы
3	моноалфавитный шифры замены	заглавные латинские буквы
4	автоключевой шифр	строчные русские буквы
5	шифр Плейфера	заглавные русские буквы
6	шифр Полибия	заглавные и строчные русские буквы
7	шифр с двойной перестановкой	строчные латинские буквы
8	роторный шифр	строчные русские буквы
9	шифр одноразового блокнота (Вернама)	заглавные русские буквы
10	маршрутный шифр	заглавные и строчные русские буквы
11	ключевой шифр перестановки	заглавные латинские буквы
12	шифр Хилла	заглавные русские буквы
13	шифр Виженера	строчные русские буквы
14	шифр Атбаш	строчные латинские буквы
15	шифр диграммной замены	заглавные латинские буквы
16	[illegible]	заглавные русские буквы
17	[illegible] перестановки	заглавные и строчные русские буквы

Контрольные вопросы

1. Сформулируйте принцип Керкгоффса.
2. Определите шифр с симметричным ключом.
3. Перечислите четыре вида атак криптоанализа.
4. Как противостоять атаке грубой силы и статистической атаке?
5. Поясните отличия между шифром подстановки (замены) и шифром перестановки.
6. Поясните отличия между моноалфавитным и многоалфавитным шифрами.
7. Поясните отличия между шифром потока и блочным шифром.
8. Все ли шифры потока являются моноалфавитными? Поясните.
9. Все ли блочные шифры являются многоалфавитными? Поясните.
10. Перечислите известные вам моноалфавитные шифры.
11. Перечислите известные вам многоалфавитные шифры.
12. Перечислите виды шифров перестановки.
13. По каждому виду традиционного шифра необходимо знать алгоритм шифрования и характеристики его криптостойкости.

6 семестр

Лабораторная работа 9. Программная реализация основных компонентов современных шифров с симметричным ключом

Цель работы – выполнить подготовительную работу для создания криптографической системы шифрования данных на основе алгоритма шифровании DES.

Задание к работе

Написать подпрограммы, необходимые для дальнейшей реализации алгоритма шифрования DES в соответствии с вариантом задания.

Перечень подпрограмм:

1. Функция генерации случайной битовой последовательности длины n.
2. Подпрограмма реализация P-блока.
3. Подпрограмма разбиения блока длины n на два блока длины n/2.
4. Подпрограмма объединения двух блоков длины n/2 в один блок длины n.
5. Подпрограмма замены левого и правого блоков длины n.
6. Подпрограмма операции **XOR** между двумя битовыми последовательнос-тями длины n.
7. Подпрограмма операции левого сдвига.
8. Подпрограмма операции правого сдвига.
9. Функция перевода двоичного блока в десятичное число.
10. Функция перевода десятичного числа в двоичный блок длины n.
11. Функция перевода 16-ричного блока в двоичный блок.
12. Функция перевода двоичного блока в 16-ричный блок.
13. Функция добавления в двоичный блок проверочных битов.

Номер варианта	Номера подпрограмм для реализации
1	1, 7
2	2, 8
3	3, 9
4	4, 10
5	5, 11

6	6, 12
7	7, 13
8	8, 3
9	9, 4
10	10, 5
11	11, 6
12	12, 7
13	13, 8
14	1, 9
15	2, 10
16	3, 11
17	4, 12

Контрольные вопросы

1. Укажите различия между современными и традиционными шифрами с симметричным ключом.
2. Объясните, почему современные блочные шифры спроектированы как шифры замены вместо того, чтобы применять шифры перестановки.
3. Перечислите основные компоненты современного блочного шифра.
4. Определите P -блок и перечислите его три варианта. Какой вариант является обратимым?
5. Определите S -блок и покажите необходимое условие обратимости S -блока.
6. Определите составной шифр и перечислите два класса составных шифров.
7. Укажите различие между рассеиванием и перемешиванием.
8. Укажите различие между блочным шифром Фейстеля и не-Фейстеля.
9. Укажите различие между синхронным и несинхронным шифрами потока.
10. Определите регистр сдвига с обратной связью и перечислите два варианта, используемые в шифре потока.

Лабораторная работа 10. Программная реализация шифра DES.

Цель работы – создать криптографическую систему шифрования данных, которая базируется на алгоритме шифровании DES.

Задание к работе

Реализовать алгоритм шифрования DES в виде отдельного класса **DES**.

Класс должен содержать в виде функций (методов) реализацию всех компонентов шифра, а также методы для шифрования и дешифрования текста.

Класс должен содержать также стандартные таблицы алгоритма DES в виде списков – атрибутов класса: StartPermutationTable, FinalPermutationTable, ExtensionTable, ParityDropTable, ShiftTable , KeyPermuteTable, SBlockTables.

Контрольные вопросы

1. Какова длина блока в DES? Каков размер ключа шифра в DES? Каков размер ключей подшифра в DES?
2. Каково число раундов в DES?

3. Сколько смесителей и устройств замены используется при шифровании и дешифровании?
4. Сколько перестановок используется в алгоритме шифра DES?
5. Сколько операций ИСКЛЮЧАЮЩЕЕ ИЛИ используется в DES-шифре?
6. Почему DES-функции необходима расширяющая перестановка?
7. Почему генератор ключей раунда нуждается в удалении проверочных бит?
8. Что такое двукратный DES? Что такое трехкратный DES?

Лабораторная работа 11. Подготовка к реализации шифра RSA

Цель работы – подготовить подпрограммы для реализации криптографической системы с открытым ключом на основе алгоритма *RSA*.

Задание к работе

Написать следующие подпрограммы (методы) для последующей реализации алгоритма шифрования RSA:

– алгоритм Евклида для нахождения НОД двух заданных чисел;

– алгоритм нахождения мультипликативной инверсии заданного числа по заданному модулю (с использованием расширенного алгоритма Эвклида);

– алгоритм проверки заданного числа на простоту в соответствии с номером варианта;

– алгоритм генерации простого числа из заданного диапазона в соответствии с номером варианта.

Контрольные вопросы

1. Способы проверки на простое число.
2. Алгоритм «Решето Эратосфена».
3. Phi-функция Эйлера.
4. Простые числа Мерсенны.
5. Простые числа Ферма.
6. Детерминированные алгоритмы проверки чисел на простоту.
7. Вероятностные алгоритмы проверки чисел на простоту.

Лабораторная работа 12. Программная реализация шифра RSA

Цель работы - создать учебный вариант криптографической системы с открытым ключом на алгоритме *RSA*, которая является первой из криптосистем с открытым ключом.

Задание к работе

Реализовать программно алгоритм шифрования RSA. В интерфейсе предусмотреть режим задания параметров системы и режим генерирования параметров системы.

В качестве параметров алгоритмы генерации простых чисел и проверки чисел на простоту, а также алгоритм нахождения мультипликативной инверсии (используя расширенный алгоритм Эвклида). Оформить программы генерации простого числа и

нахождения мультипликативной инверсии, как подпрограммы (методы), чтобы при необходимости их можно было заменить на другие программные реализации.

Подготовить для демонстрации программы контрольный пример.

Контрольные вопросы

1. Дать определение односторонней функции.
2. Дать определение односторонней функции с секретом.
3. На какой базе обычно создаются криптографические системы с открытыми ключами?
4. Перечислить число параметров в криптографической системе *RSA*.
5. Перечислить секретные параметры системы *RSA*.
6. Перечислить открытые параметры системы RSA.
7. На каком математическом результате базируется система RSA.
8. Какими свойствами должны удовлетворять параметры p и q системы RSA.
9. Какими свойствами должны удовлетворять параметры e и d системы RSA.
10. На какой достаточно трудной задаче из теории чисел базируется криптографическая система RSA.
11. Опишите схему шифрования текста с использованием алгоритма RSA.
12. Опишите схему дешифрования текста с использованием алгоритма RSA.
13. Опишите схему формирование цифровой подписи с применение алгоритма RSA.
14. Сформулировать теорему Ферма.
15. Сформулировать теорему Эйлера.

Лабораторная работа 13. Программная реализация ЭЦП

Цель работы - создать программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.

Задание к работе

Реализовать ЭЦП на базе алгоритма Эль-Гамаля и алгоритма *RSA*. Предусмотреть режимы формирования параметров криптосистемы Эль-Гамаля. Программу оформить, как интегрируемую среду с удобным интерфейсом формирования ЭЦП и ее проверки. Подготовить отчет, в который включить алгоритмы формирования системы Эль-Гамаля, описание функций из которых состоит программа. Подготовить для демонстрации контрольный пример. При формировании цифровой подписи предусмотреть схему ЭЦП с использованием хэш-функций.

Контрольные вопросы

1. Перечислить число параметров в криптографической системе Эль-Гамаля.
2. Перечислить секретные параметры системы Эль-Гамаля.
3. Перечислить открытые параметры системы Эль-Гамаля.
4. На какой достаточно трудной задаче из теории чисел базируется криптографическая система Эль-Гамаля.

5. Описать схему формирования ЭЦП с использованием алгоритма Эль-Гамаля.

6. Описать схему проверку ЭЦП с использованием алгоритма Эль-Гамаля.

7. Описать схему формирование цифровой подписи с применение алгоритма RSA.

8. Описать схему проверки цифровой подписи с применение алгоритма RSA.

9. Что общего между обычной и цифровой подписями? Чем они различаются?

10. Какие задачи позволяет решить цифровая подпись?

11. В чем заключается принципиальная сложность в практическом применении систем цифровой подписи?

12. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать для шифрования и цифровой подписи?

13. Проверить, что указанный в тексте способ подбора подписанных сообщений для схемы Эль-Гамаля действительно дает верные цифровые подписи.

Лабораторная работа 14. Программная реализация криптографических протоколов

Цель работы - ознакомится с криптографическими протоколами, которые в настоящее время широко используются для обеспечения информационной безопасности. Освоить основные понятия, которые связаны с криптографическими протоколами.

Задание к работе

Реализовать два простейших протокола. Протокол Диффи-Хелмана формирования общего ключа и протокол подбрасывания монеты. Подготовить отчет. В отчете дать алгоритмы протоколов и описать их программные реализации. Подготовить для демонстрации учебные варианты контрольных примеров, которые моделируют работу с использованием криптографических протоколов.

Контрольные вопросы

1. Дать определение протокола.

2. Перечислить задачи защиты информации, в которых используются криптографические протоколы.

3. Способы классификации криптографических протоколов.

4. Классификация криптографических протоколов по функциональному назначению.

5. Назначение протокола аутентификации сообщений.

6. Назначение протокола идентификации.

7. Назначение протокола обмена секретами.

8. Перечислить основные виды атак на протоколы.

5.1.1. Перечень основной литературы:

1. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428998.

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks».

5.1.2. Перечень дополнительной литературы:

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/ 63800.html

2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл., схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php?page=book&id=231673.

3. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=

5.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации»
2. Методические указания к лабораторным работам по дисциплине «Методы и средства криптографической защиты информации»

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Методы и средства криптографической защиты информации»
2. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.
3. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия.
4. http://www.iprbookshop.ru – ЭБС «IPRbooks».
5. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online».
6. http://window.edu.ru – образовательные ресурсы ведущих вузов.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине
«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»
для направления подготовки 10.03.01 Информационная безопасность
направленность (профиль) Безопасность компьютерных систем

Пятигорск
2022

ВВЕДЕНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины: формирование набора универсальных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачи дисциплины: ознакомить студентов с современными системами шифрования на основе симметричных и асимметричных алгоритмов; научить выбирать параметры псевдослучайных последовательностей для генерирования криптостойких ключей; изучить стандарты систем шифрования; изучить криптографические протоколы.

2. Наименование лабораторных занятий

№ темы	Наименование работы	Обьем часов	Из них практическая подготовка, часов
	5 семестр		
2	Основы теории делимости.	1,5	
3	Модульная арифметика.	1,5	
4	Матрицы вычетов.	1,5	
5	Проверка чисел на простоту.	1,5	
6	Алгоритмы генерации простых чисел.	1,5	
7	Разложение чисел на простые множители.	1,5	
8	Китайская теорема об остатках	1,5	
9-10	Алгебраические основы криптологии. Эллиптические кривые.	1,5	
13	Традиционные шифры с симметричным ключом.	1,5	
	Итого за 5 семестр	**13,5**	
	6 семестр		
19-20	Современные блочные и поточные шифры с симметричным ключом.	1,5	
21-22	Современные стандарты симметричного шифрования DES и AES.	1,5	
23	Российские стандарты симметричного шифрования.	1,5	
24-27	Тема 24. Алгоритмы шифрования с открытыми ключами. Криптосистемы RSA, Рабина, Эль-Гамаля.	1,5	
28	Криптосистемы на основе метода эллиптических кривых.	1,5	
29	Тема 29. Аутентификация данных. Электронная цифровая подпись.	1,5	
30-31	Тема 30. Стандарты ЭЦП.	1,5	
32-34	Криптографические протоколы.	1,5	
	Итого за 6 семестр	**12**	
	Итого	**25,5**	

ОСНОВНОЕ СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическая работа №1

Цель и содержание: исследовать основные теории делимости.

Содержание работы:

1. Изучить теоретические аспекты теории делимости.
2. Признаки делимости.

Задачи:

1. Произведение двух двузначных чисел равно 444. Найдите эти числа.

2. Для детских новогодних подарков закупили 78 плиток шоколада, 156 пряников, 52 пачки печенья, 104 апельсина и 130 яблок. Какое наибольшее число одинаковых подарков можно собрать из этих лакомств?

3. На некоторой остановке одновременно остановились трамвай, троллейбус и автобус. Через какое наименьшее время повторится их встреча, если движение проходит строго по графику, и трамвай совершит полный рейс за 90 минут, автобус - за 120 минут, а троллейбус - за 60 минут.

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий.

Практическая работа №2

Цель и содержание: научиться выполнять основные арифметические операции в различных системах счисления.

Содержание работы:

1. Изучить теоретические аспекты арифметики.
2. Свойства арифметики.
3. Операторы.
4. арифметические операции с классами вычетов

Задачи:

1. Проверка сравнимости по модулю m, модульное умножение, модульное возведение в квадрат, модульное деление
2. Сложение по модулю m, модульное возведение в квадрат, проверка сравнимости по модулю m, модульное вычитание
3. Модульное умножение, модульное возведение в квадрат модульное сложение переменных типа CLINT и USHORT, модульное деление
4. Модульное вычитание, модульное умножение, модульное деление переменной типа CLINT на переменную типа USHORT, модульное сложение
5. Модульное вычитание, модульное деление, модульное возведение в квадрат, сложение по модулю m

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий.

Практическая работа №3

Цель и содержание: научиться выполнять матрицы вычетов.

Содержание работы:

1. Изучить теоретические аспекты матрицы.
2. Свойства матриц.
3. Операции на матрицах вычетов.

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий.

Практическая работа №4

Цель и содержание: научиться осуществлять проверку чисел на простоту.

Содержание работы:

1. Изучить определения простых чисел.
2. Виды простых чисел.
3. Проверка на простоту чисел.
4. Проверка на простоту за корень
5. Разложение на простые множители

Задачи:

1. Найдите этим способом на бумажке все простые числа до 50, потом проверьте с программой:

```
N = 50
prime = [1] * (N + 1)
prime[0], prime[1] = 0, 0
for i in range(2, N + 1): # можно и до sqrt(N)
    if prime[i]:
        for j in range(2 * i, N + 1, i): # идем с шагом i, можно начиная с i * i
            prime[j] = 0
for i in range(1, N + 1):
    if prime[i]:
        print(i)
```

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий.

Практическая работа №5

Цель и содержание: Освоить методы генерации больших простых чисел и методы проверки больших чисел на простоту. Познакомиться с теоремой Эйлера, научиться строить первообразные корни по модулю n. Изучить схему обмена ключами Диффи-Хеллмана.

Задание:

Реализовать приложение, позволяющее выполнять следующие действия:

1. Генерировать большие простые числа:

1) программа по заданным (количество проверок в тесте Рабина-Миллера) и (количество бит) должна генерировать простое n-битное число, отображая при этом, сколько итераций алгоритма генерации простого числа потребовалось выполнить для его генерации и сколько времени было затрачено на это;

2) программа по заданным границам диапазона должна выводить все простые числа из этого диапазона, отображая время, затраченное на генерацию всех чисел.

2. Определять для заданного числа первые 100 первообразных корней, отображая при этом суммарное время, затраченное программой на их поиск.

3. Моделировать обмен ключами между абонентами по схеме Диффи-Хеллмана. Программа должна получать большие простые числа X , X и случайным образом с

помощью алгоритма генерации простого числа, а также предоставлять пользователю возможность задавать их. II.

С помощью реализованного приложения выполнить следующие задания:

1. Протестировать правильность работы разработанного приложения.
2. Сделать выводы о проделанной работе.

Вопросы для защиты .

Первая часть защиты (обязательная):

1. Для чего нужно большое простое число? Как проверить, является число простым или нет? Как сгенерировать большое простое число?

2. Алгоритм эффективной реализации возведения целого числа в целую степень по модулю .

3. На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

4. Как происходит обмен ключами по схеме Диффи-Хеллмана?

5. Доказать, что в схеме Диффи-Хеллмана $K\ K$.

5 II. Вторая часть защиты: Для заданного найти функцию Эйлера ( ). 1. ; 2. ; 3. ; 4. ; 5. ; 6. .

III. Третья часть защиты: Для заданного найти все первообразные корни. 1. ; 2. ; 3. ; 4. ; 5. ; 6. .

Практическая работа №6

Цель и содержание: научиться выполнять разложение чисел на простые множители.

Содержание работы:

1. Что значит разложить число на простые множители?
2. Каноническое разложение числа на простые множители.
3. Алгоритм разложения числа на простые множители.
4. Примеры разложения на простые множители.
5. Использование признаков делимости для разложения на простые множители.

Задачи:

1. как разложить число 2378 на простые множители?
2. разложите 81375 на простые множители.
3. разложить 15845 на простые множители.

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий, ответы на контрольные вопросы.

Практическая работа №7

Цель и содержание: научиться применять алгебраические основы криптологии, изучить криптологию.

Содержание работы:

1. Криптография, основная на группах
2. Алгебраическое шифрование
3. Анализ схем криптографии
4. Научиться применять доказательства

Задача:

1. Множество целых чисел, входящих в вычет с оператором сложения, G = $<Z_n, +>$, является конечной группой. Мы можем выполнить сложение и вычитание на элементах этого множества, не выходя за его пределы.

2. Множество Z_{n*} с оператором умножения $G = <Z_{n*}, >$, является также абелевой группой. Мы можем выполнить умножение и деление на элементах этого множества, не выходя за его пределы. Это облегчает проверку первых трех свойств. Нейтральный элемент равен 1. Каждый элемент имеет *инверсию*, которая может быть найдена согласно расширенному *алгоритму Евклида*.

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий, ответы на контрольные вопросы.

Практическая работа № 8

Цель и содержание: научиться использовать шифрование, уметь читать зашифрованный текст.

Задача:

1. Приведенный ниже пример показывает исходный текст и соответствующий ему зашифрованный текст. Мы используем строчные символы, чтобы показать исходный текст, и заглавные буквы (символы верхнего регистра), чтобы получить зашифрованный текст. Шифр моноалфавитный, потому что оба l зашифрованы как O. Исходный текст: hello Зашифрованный текст: KHOOR
2. Приведенный ниже пример показывает исходный текст и соответствующий ему зашифрованный текст. Шифр не является моноалфавитным, потому что каждая буква l (эль) зашифрована различными символами. Первая буква l (эль) зашифрована как N ; вторая — как Z. Исходный текст: hello Зашифрованный текст: ABNZF
3. Ева перехватила зашифрованный текст "UVACLYFZLJBYL". Покажите, как она может взломать шифр, используя атаку грубой силы.

Содержание отчета и его форма

Отчет по практической работе, представленный к защите, должен содержать: номер практической работы, тему, цель практической работы, перечень изученных вопросов, результаты выполненных заданий, ответы на контрольные вопросы.

Практическая работа № 9

Цель и содержание: научиться использовать блочное симметричное шифрование.

Содержание работы:

1. Описание алгоритмов шифрования DES и TEA
2. Алгоритм IDEA
3. Ответы на контрольные вопросы

Задача:

1. Привести SP-сети, содержащие в каждом раунде два слоя – подстановки (substitution), в котором обычно используются обратимые операции преобразования над шифруемым блоком и материалом ключа, и перестановки (permutation), в котором происходит перестановка бит внутри блока.
2. Реализовать систему симметричного блочного шифрования, позволяющую шифровать и дешифровать файл на диске с использованием заданного блочного шифра в заданном режиме шифрования. Перечень блочных шифров и режимов шифрования приведен в [6]. Выбор шифра и режима для реализации получить у преподавателя.

Алгоритм		Режим шифрования	
Номер	Название	Номер	Режим
1	TEA	а	ECB
2	IDEA	б	CBC
3	RC6	в	PCBC
4	ГОСТ	г	CFB
5	Rijndael	д	OFB
6	DES		

Контрольные вопросы

1. Перечислите основные обратимые операции, используемые в образующих функциях блочных шифров.
2. Что такое сеть Фейштеля? В чем ее основные достоинства?
3. Какие параметры блочных шифров влияют на его криптостойкость?
4. Какие блочные шифры, построенные по принципу сети Фейштеля, вам известны?
5. Проведите сравнительный анализ алгоритмов ГОСТ и Rijndael.
6. Проведите сравнительный анализ режимов шифрования CBC и ECB.
7. Проведите сравнительный анализ режимов шифрования CBC и CFB

Список литературы

Перечень основной литературы:

1. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id =428998.

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks».

Перечень дополнительной литературы:

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/ 63800.html

2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл., схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php?page=book&id=231673.

3. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=

Учебно-методического литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации»
2. Методические указания к лабораторным работам по дисциплине «Методы и средства криптографической защиты информации»
3. Методические указания к практическим работам по дисциплине «Методы и средства криптографической защиты информации»

Интернет ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Методы и средства криптографической защиты информации»
2. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.
3. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия.
4. http://www.iprbookshop.ru – ЭБС «IPRbooks».
5. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online».
6. http://window.edu.ru – образовательные ресурсы ведущих вузов.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов направления подготовки
10.03.01 Информационная безопасность
направленность (профиль) Безопасность компьютерных систем

Пятигорск, 2022

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Методы и средства криптографической защиты информации» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-3	Способность использовать необходимые математические методы для решения задач профессиональной деятельности
ОПК-7	Способность использовать языки программирования и технологии разработки программах средств для решения задач профессиональной деятельности
ОПК-9	Способность применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
5 семестр					
ОПК-3, ОПК-7, ОПК-9, ПК-4	Самостоятельное изучение литературы и источников	Собеседование	16,2	1,8	18
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к лабораторным работам	Отчет письменный	16,2	1,8	18
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к практическим занятиям	Отчет письменный	16,2	1,8	18
Итого за 5 семестр			**48,6**	**5,4**	**54**
6 семестр					
ОПК-3, ОПК-7, ОПК-9, ПК-4	Самостоятельное изучение литературы и источников	Собеседование	4,5	0,3	3
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка отчетов по лабораторным работам	Отчет письменный	4,5	0,3	3
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к практическим занятиям	Отчет письменный	4,5	0,3	3
ОПК-3, ОПК-7, ОПК-9, ПК-4	Подготовка к экзамену	Экзамен	24,3	2,7	27
Итого за 6 семестр			**32,4**	**3,6**	**36**
Итого			**81**	**9**	**90**

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данной дисциплине.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и

вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае неуверенности нужно еще раз внимательно разобраться в материале. Иногда правильность понимания того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение

решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Библиография литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.
- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.
- Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса
- Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.
- Приложение (при необходимости).

Требования к оформлению:

- текст с одной стороны листа;
- шрифт Times New Roman;
- кегль шрифта 14;
- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студентом над ним и устранения всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент

должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной

задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен. Допускаются фактические неточности. Студент	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационны	Проект представлен полностью и в срок.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	свободно отвечает на вопросы, связанные с проектом.		е способности.	
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими и информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, письменные отчеты по лабораторным и работам и экзамен.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id =428998.

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks».

Дополнительная литература:

4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/ 63800.html

5. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл., схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php?page=book&id=231673.

6. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=

Методическая литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации»

2. Методические указания к лабораторным работам по дисциплине «Методы и средства криптографической защиты информации»

Интернет-ресурсы:

7. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Методы и средства криптографической защиты информации»

8. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.

9. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия.

10. http://www.iprbookshop.ru – ЭБС «IPRbooks».

11. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online».

12. http://window.edu.ru – образовательные ресурсы ведущих вузов.