МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ. В.Ф. УТКИНА»

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
«Информационная безопасность»

Направление подготовки

38.03.04 «Государственное и муниципальное управление»

Направленность (профиль) подготовки

Информационные технологии в государственном и муниципальном управлении

Квалификация выпускника – бакалавр

Форма обучения – очная

г. Рязань

1. ПЛАНЫ ПРАКТИЧЕСКИХ РАБОТ

Лабораторная работа № 1
Шифр Цезаря. Шифр Атбаш

Цель работы: изучение алгоритма шифрования текстовых данных на основе шифра Цезаря и шифра Атбаш.

Краткие теоретические сведения

Шифр Цезаря – один из наиболее простых и широко известных алгоритмов шифрования текстовых данных. Этот метод назван в честь римского полководца Гая Юлия Цезаря, который применял шифр для личной переписки с подчиненными.

Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – ключом.

Пример. Ключ = 5. Получаем последовательность:

Русский алфавит:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифр:

Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д

То есть А заменяем на Е, Б на Ё, и т.д.

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \,\%\, Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \,\%\, Q. \quad (2)$$

где m – открытый текст;

k – ключ шифрования;

Q – количество символов в алфавите;

c – зашифрованный текст;

оператор % вычисляет остаток после деления первого операнда на второй.

Если символ исходного текста отсутствует в алфавите, то он кодируется самим собой.

Таблица 1 – Номера символов алфавита

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16

Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Шифр Атбаш – простой метод шифрования с помощью подстановки для алфавитного письма.

Алгоритм шифрования заключается в замене *k*-го символа алфавита символом с порядковым номером $\boldsymbol{n - k + 1}$, где *n* – количество символов в алфавите.

Таблица 2 – Таблица замены символов для русского языка

Символ исходный	Символ закодированный
А	„ „(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И

Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д

Задание

1. Выполнить шифрование заданного сообщения шифром Цезаря.
2. Выполнить шифрование заданного сообщения шифром Атбаш.

Выполнение работы

Этап 1. Выполнить кодирование последовательности “начинайте подготовку к экзамену” с ключом $k = 1$, количеством символов $Q = 33$ (по формуле (1)) с помощью шифра Цезаря.

Расчет.

1) символ “н”:

Encrypt = (33 + 14 + 1) % 33 = 48 % 33 = 15. Получили н -> о

2) символ “а”:

Encrypt = (33 + 0 + 1) % 33 = 34 % 33 = 1. Получили а -> б

3) символ “ч”:

Encrypt = (33 + 24 + 1) % 33 = 58 % 33 = 25. Получили ч -> ш

…

В итоге получаем текст:

обшйобкуё рпедпупглф л юлибнёоф

Этап 2. Выполнить декодирование полученной последовательности с ключом k = 1, количеством символов Q = 33 (по формуле (2)) с помощью шифра Цезаря.

Расчет.

1) символ “о”:

Decrypt = (33 + 15 - 1) % 33 = 47 % 33 = 14. Получили о -> н

2) символ “б”:

Decrypt = (33 + 1 - 1) % 33 = 33 % 33 = 0. Получили б -> а

3) символ “ш”:

Decrypt = (33 + 25 - 1) % 33 = 57 % 33 = 24. Получили ш -> ч

…

В итоге получаем текст:

начинайте подготовку к экзамену

Таким образом, результат дешифрования совпал с исходным сообщением. Поэтому результат шифрования верен.

Этап 3. Написание программы на языке C# (шифр Цезаря).

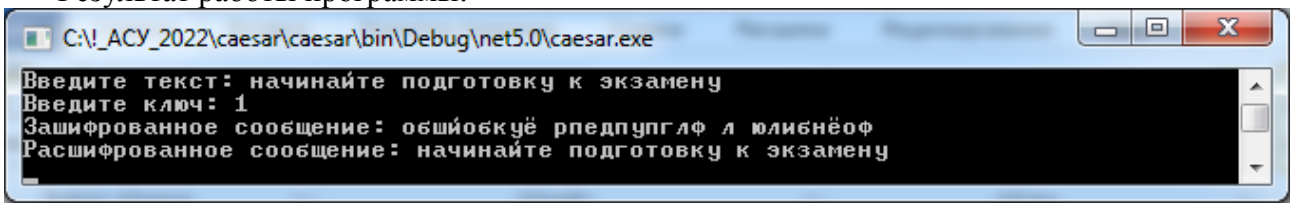
Program.cs

caesar — Program

```
using System;

ссылка: 1
public class CaesarCipher
{
    //символы русской азбуки
    const string alfabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

    Ссылок: 2
    private string CodeEncode(string text, int k)
    {
        //добавляем в алфавит маленькие буквы
        var fullAlfabet = alfabet + alfabet.ToLower();
        var letterQty = fullAlfabet.Length;
        var retVal = "";
        for (int i = 0; i < text.Length; i++)
        {
            var c = text[i];
            var index = fullAlfabet.IndexOf(c);
            if (index < 0)
            {
                //если символ не найден, то добавляем его в неизменном виде
                retVal += c.ToString();
            }
            else
            {
                var codeIndex = (letterQty + index + k) % letterQty;
                retVal += fullAlfabet[codeIndex];
            }
        }

        return retVal;
    }

    //шифрование текста
    ссылка: 1
    public string Encrypt(string plainMessage, int key)
        => CodeEncode(plainMessage, key);

    //дешифрование текста
    ссылка: 1
    public string Decrypt(string encryptedMessage, int key)
        => CodeEncode(encryptedMessage, -key);
}
```

```
42  class Program
43  {
        Ссылок: 0
44      static void Main(string[] args)
45      {
46          var cipher = new CaesarCipher();
47          Console.Write("Введите текст: ");
48          var message = Console.ReadLine();
49          Console.Write("Введите ключ: ");
50          var secretKey = Convert.ToInt32(Console.ReadLine());
51          var encryptedText = cipher.Encrypt(message, secretKey);
52          Console.WriteLine("Зашифрованное сообщение: {0}", encryptedText);
53          Console.WriteLine("Расшифрованное сообщение: {0}", cipher.Decrypt(encryptedText, secretKey));
54          Console.ReadLine();
55      }
56  }
```

Результат работы программы:



Видно, что результат работы программы совпал с расчетами.

Этап 4. Выполнить кодирование последовательности “начинайте подготовку к экзамену” (шифр Атбаш).

Расчет.

1) н -> т:
2) а -> „ „
3) ч -> и

…

В итоге получаем текст:

т ичт цныарсьэснсюхмахагхш уытм

Этап 5. Выполнить декодирование полученной последовательности (шифр Атбаш).

Расчет.

1) т -> н
2) „ „ -> а
3) и -> ч

…

В итоге получаем текст:

начинайте подготовку к экзамену

Таким образом, результат дешифрования совпал с исходным сообщением. Поэтому результат шифрования верен.

Этап 6. Написание программы на языке C# (шифр Атбаш).

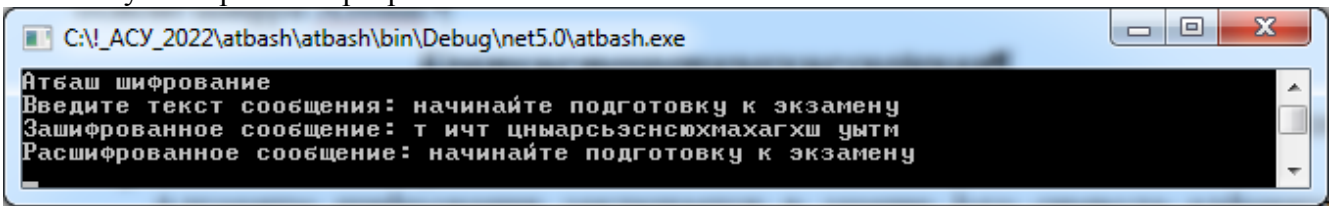
Program.cs

atbash — Atbash

```
using System;

//Атбаш
ссылка: 1
public class Atbash
{
    //алфавит языка
    private const string alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя ";

    //метод для переворачивания строки
    Ссылок: 2
    private string Reverse(string inputText)
    {
        //переменная для хранения результата
        var reversedText = string.Empty;
        foreach (var s in inputText)
        {
            //добавляем символ в начало строки
            reversedText = s + reversedText;
        }

        return reversedText;
    }

    //метод шифрования/дешифрования
    Ссылок: 2
    private string EncryptDecrypt(string text, string symbols, string cipher)
    {
        //переводим текст в нижний регистр
        text = text.ToLower();

        var outputText = string.Empty;
        for (var i = 0; i < text.Length; i++)
        {
            //поиск позиции символа в строке алфавита
            var index = symbols.IndexOf(text[i]);
            if (index >= 0)
            {
                //замена символа на шифр
                outputText += cipher[index].ToString();
            }
        }

        return outputText;
    }
```

```
44          //шифрование текста
            ссылка: 1
45          public string EncryptText(string plainText)
46          {
47              return EncryptDecrypt(plainText, alphabet, Reverse(alphabet));
48          }
49
50          //расшифровка текста
            ссылка: 1
51          public string DecryptText(string encryptedText)
52          {
53              return EncryptDecrypt(encryptedText, Reverse(alphabet), alphabet);
54          }
55      }
56
        Ссылок: 0
57      class Program
58      {
            Ссылок: 0
59          static void Main(string[] args)
60          {
61              Console.WriteLine("Атбаш шифрование");
62              var atbash = new Atbash();
63              Console.Write("Введите текст сообщения: ");
64              var message = Console.ReadLine();
65              var encryptedMessage = atbash.EncryptText(message);
66              Console.WriteLine("Зашифрованное сообщение: {0}", encryptedMessage);
67              var decryptedMessage = atbash.DecryptText(encryptedMessage);
68              Console.WriteLine("Расшифрованное сообщение: {0}", decryptedMessage);
69              Console.ReadLine();
70          }
71      }
```

Результат работы программы:



Видно, что результат работы программы совпал с расчетами.

Варианты заданий

№ варианта	Сообщение	Ключ
1	выполняйте практическую работу	2
2	пора писать реферат	3
3	скоро неделя отработки	4
4	не забывайте о сессии	5
5	не нужно много бездельничать	6
6	зачетная неделя начнется внезапно	7
7	лабораторные работы нужно делать	8
8	в понедельник начинаются зачеты	9
9	экзамены бывают по воскресеньям	10
10	в субботу проводятся зачеты	11

Рекомендуемая литература:

1. Информационная безопасность и защита информации: метод. указ. к лаб. работам / РГРТА. Сост.: Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин. Рязань, 2005. 32 с.

2. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2009.- 24 с.

3. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2011.- 24 с.

Лабораторная работа № 2
Шифр XOR

Краткие теоретические сведения

Шифр XOR – это алгоритм шифрования данных с использованием операции «исключающее ИЛИ».

Алгоритм XOR-шифрования заключается в “наложении” последовательности случайных чисел на текст, который необходимо зашифровать. Последовательность случайных чисел называется **гамма-последовательность**, и используется для шифрования и расшифровки данных.

Формула для получения закодированного текста:

$$C_n = M_n \ \mathbf{xor}\ K_n,$$

где M_n – символ исходного сообщения;
K_n – символ ключа (пароля).

Ключ шифрования можно получить двумя способами:

1. Повторять ключевое слово пока длина гаммы не будет равна длине сообщения (используется в работе).
2. Сгенерировать последовательность псевдослучайных чисел, равную по длине тексту сообщения.

Таблица 1 – Таблица истинности функции «ИСКЛЮЧАЮЩЕЕ ИЛИ»

X1	X2	X1 ⊕ X2
0	0	0
0	1	1
1	0	1
1	1	0

Выполнение работы

Этап 1. Выполнить кодирование последовательности “начинайте подготовку к экзамену”.

Расчет.

В итоге получаем текст:

Этап 2. Выполнить декодирование полученной последовательности.

Расчет.

…

В итоге получаем текст:

начинайте подготовку к экзамену

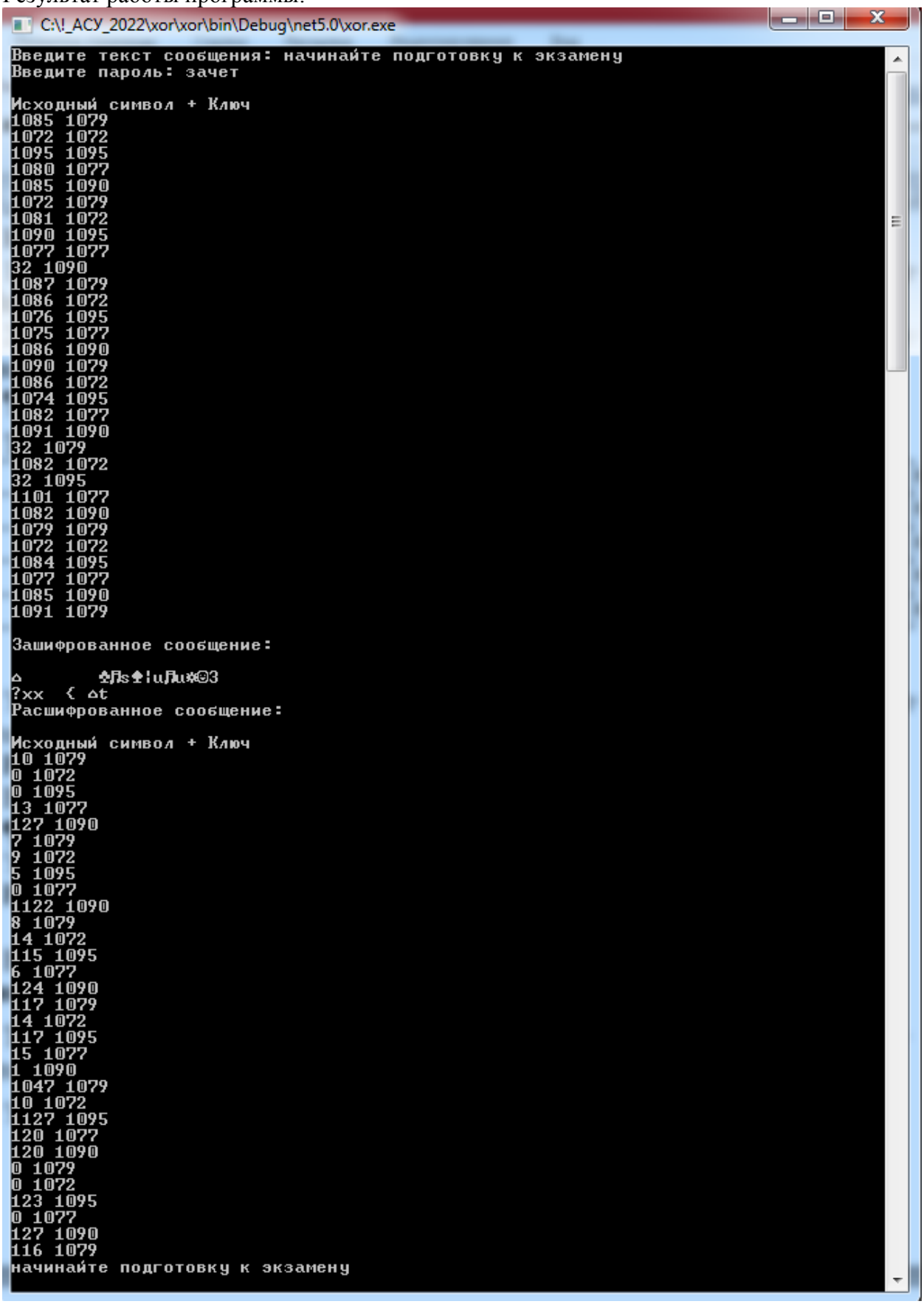
Таким образом, результат дешифрования совпал с исходным сообщением. Поэтому результат шифрования верен.

Этап 3. Написание программы на языке C#.

```
using System;
```

```
namespace xor
{
    public class XORCipher
    {
        //генератор повторений пароля
        private string GetRepeatKey(string s, int n)
        {
            var r = s;
            while (r.Length < n)
            {
                r += r;
            }

            return r.Substring(0, n);
        }

        //метод шифрования/дешифровки
        private string Cipher(string text, string secretKey)
        {
            Console.WriteLine();
            Console.WriteLine("Исходный символ + Ключ");
            var currentKey = GetRepeatKey(secretKey, text.Length);
            var res = string.Empty;
            for (var i = 0; i < text.Length; i++)
            {
                res += ((char)(text[i] ^ currentKey[i])).ToString();
                Console.WriteLine((int)text[i] + " " + (int)currentKey[i]);
            }

            return res;
        }

        //шифрование текста
        public string Encrypt(string plainText, string password)
            => Cipher(plainText, password);

        //расшифровка текста
        public string Decrypt(string encryptedText, string password)
            => Cipher(encryptedText, password);
    }

    class Program
    {
        static void Main(string[] args)
        {
            var x = new XORCipher();
            Console.Write("Введите текст сообщения: ");
            var message = Console.ReadLine();
            Console.Write("Введите пароль: ");
            var pass = Console.ReadLine();
            var encryptedMessageByPass = x.Encrypt(message, pass);
            Console.WriteLine();
            Console.WriteLine("Зашифрованное сообщение:");
            Console.WriteLine(encryptedMessageByPass);
            Console.WriteLine("Расшифрованное сообщение:");
            Console.WriteLine(x.Decrypt(encryptedMessageByPass, pass));
            Console.ReadLine();
        }
    }
}
```

Результат работы программы:



Видно, что результат работы программы совпал с расчетами.

Варианты заданий

№ варианта	Сообщение	
1	выполняйте практическую работу	
2	пора писать реферат	
3	скоро неделя отработки	
4	не забывайте о сессии	
5	не нужно много бездельничать	
6	зачетная неделя начнется внезапно	
7	лабораторные работы нужно делать	
8	в понедельник начинаются зачеты	
9	экзамены бывают по воскресеньям	
10	в субботу проводятся зачеты	

Рекомендуемая литература:

1. Информационная безопасность и защита информации: метод. указ. к лаб. работам / РГРТА. Сост.: Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин. Рязань, 2005. 32 с.

2. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2009.- 24 с.

3. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2011.- 24 с.

Лабораторная работа № 3
Шифр Виженера

Цель работы: изучение алгоритма шифрования текстовых данных на основе шифра Виженера.

Краткие теоретические сведения

Шифр Виженера – это алгоритм шифрования текстовых данных с помощью ключевого слова.

Шифрование Виженера можно представить как несколько шифров Цезаря с различными ключами. Проще всего шифры представить в виде таблицы, для английского алфавита мы получим 26 строк шифра Цезаря, в каждой строке сдвиг на единицу больше предыдущей:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Математически шифр Виженера можно описать следующими формулами:

$$Encrypt(m_n) = (Q + m_n + k_n) \% Q;$$

$$Decrypt(c_n) = (Q + c_n - k_n) \% Q.$$

где m_n - позиция символа открытого текста;
k_n - позиция символа ключа шифрования;
Q - количество символов в алфавите;
c_n - позиция символа зашифрованного текста.

Выполнение работы

Этап 1. Написание программы на языке C#.

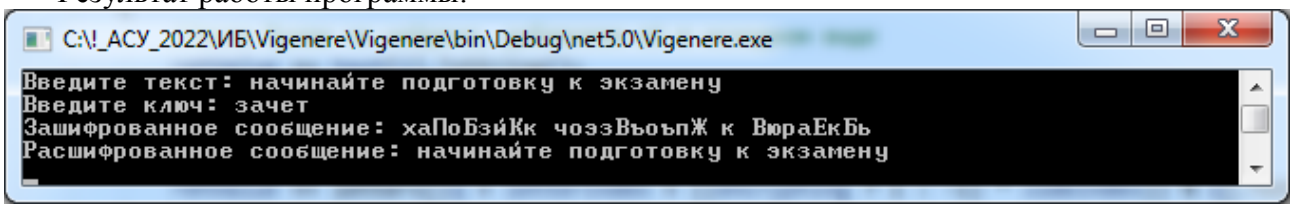
Program.cs

Vigenere | Vigenere.VigenereCipher

```
using System;

namespace Vigenere
{
    Ссылок: 2
    public class VigenereCipher
    {
        const string defaultAlphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
        readonly string letters;

        ссылка: 1
        public VigenereCipher(string alphabet = null)
        {
            letters = string.IsNullOrEmpty(alphabet) ? defaultAlphabet : alphabet;
        }

        //генерация повторяющегося пароля
        ссылка: 1
        private string GetRepeatKey(string s, int n)
        {
            var p = s;
            while (p.Length < n)
            {
                p += p;
            }

            return p.Substring(0, n);
        }
        2
        2
        Ссылок: 2
        private string Vigenere(string text, string password, bool encrypting = true)
        {
            var gamma = GetRepeatKey(password, text.Length);
            var retValue = "";
            var q = letters.Length;

            for (int i = 0; i < text.Length; i++)
            {
                var letterIndex = letters.IndexOf(text[i]);
                var codeIndex = letters.IndexOf(gamma[i]);
                if (letterIndex < 0)
                {
                    //если буква не найдена, добавляем её в исходном виде
                    retValue += text[i].ToString();
                }
                else
                {
                    retValue += letters[(q + letterIndex + ((encrypting ? 1 : -1) * codeIndex)) % q].ToString();
                }
            }

            return retValue;
        }

        //шифрование текста
        ссылка: 1
        public string Encrypt(string plainMessage, string password)
            => Vigenere(plainMessage, password);

        //дешифрование текста
        ссылка: 1
        public string Decrypt(string encryptedMessage, string password)
            => Vigenere(encryptedMessage, password, false);
    }
```

```
Ссылок: 0
class Program
{
    Ссылок: 0
    static void Main(string[] args)
    {
        //передаем в конструктор класса буквы русского алфавита
        var cipher = new VigenereCipher("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзиклмнопрстуфхцчшщъьэюя");
        Console.Write("Введите текст: ");
        var inputText = Console.ReadLine();//.ToUpper();
        Console.Write("Введите ключ: ");
        var password = Console.ReadLine().ToUpper();
        var encryptedText = cipher.Encrypt(inputText, password);
        Console.WriteLine("Зашифрованное сообщение: {0}", encryptedText);
        Console.WriteLine("Расшифрованное сообщение: {0}", cipher.Decrypt(encryptedText, password));
        Console.ReadLine();
    }
}
```

Результат работы программы:



Видно, что результат работы программы совпал с расчетами.

Варианты заданий

№ варианта	Сообщение	Ключ
1	выполняйте практическую работу	2
2	пора писать реферат	3
3	скоро неделя отработки	4
4	не забывайте о сессии	5
5	не нужно много бездельничать	6
6	зачетная неделя начнется внезапно	7
7	лабораторные работы нужно делать	8
8	в понедельник начинаются зачеты	9
9	экзамены бывают по воскресеньям	10
10	в субботу проводятся зачеты	11

Рекомендуемая литература:

1. Информационная безопасность и защита информации: метод. указ. к лаб. работам / РГРТА. Сост.: Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин. Рязань, 2005. 32 с.

2. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2009.- 24 с.

3. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2011.- 24 с.

Лабораторная работа № 4
Шифр Скитала

Краткие теоретические сведения

Шифр Скитала – это шифрование текста при помощи деревянного цилиндра и пергамента, также известен как шифр Древней Спарты. Этот метод шифрования использовался античными спартанцами и греками, для обмена сообщениями во время войны.

Для шифрования текста используется цилиндр фиксированного диаметра, на который наматывается узкая полоска пергамента. Сообщение записывают вдоль цилиндра, а затем разматывают, в итоге получается зашифрованное сообщение, которое можно расшифровать применяя цилиндр того же диаметра. При этом диаметр цилиндра выступает в роле ключа шифрования.

Пример. Шифрование сообщения с ключом 4 можно представить в виде таблицы, где открытый текст записывается в строки, а разматывание полоски – это склейка всех столбцов в один:

Ш	И	Ф	Р	_
Д	Р	Е	В	Н
Е	Й	_	С	П
А	Р	Т	Ы	_

Получается словосочетание “ШИФР ДРЕВНЕЙ СПАРТЫ” преобразуется в “ШДЕАИРЙРФЕ_ТРВСЫ_НП_”.

Выполнение работы

Этап 1. Написание программы на языке C#.

Program.cs

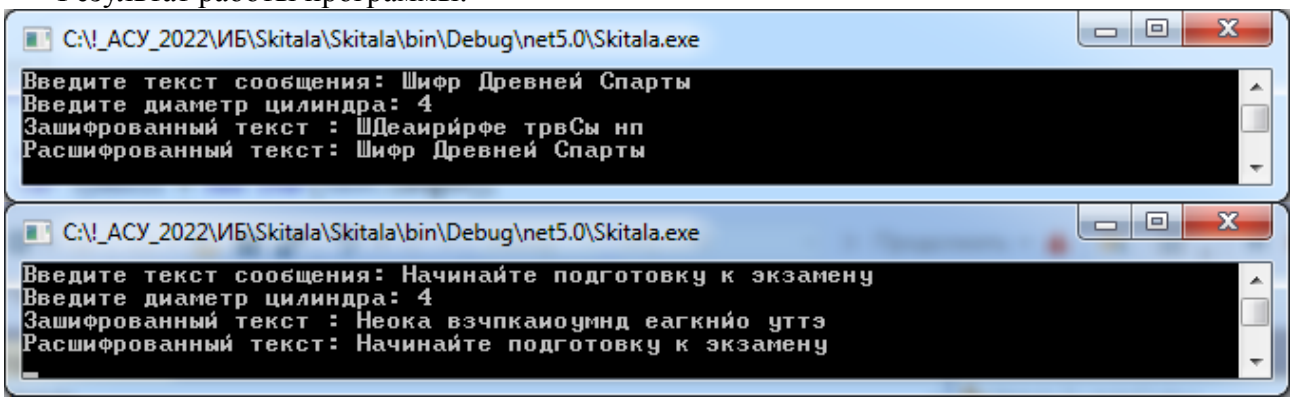
Skitala

Skitala.ScytaleCipher

```
using System;

namespace Skitala
{
    ссылка: 1
    public class ScytaleCipher
    {
        ссылка: 1
        public string Encrypt(string text, int d)
        {
            var k = text.Length % d;
            if (k > 0)
            {
                //дополняем строку пробелами
                text += new string(' ', d - k);
            }

            var column = text.Length / d;
            var result = "";

            for (int i = 0; i < column; i++)
            {
                for (int j = 0; j < d; j++)
                {
                    result += text[i + column * j].ToString();
                }
            }

            return result;
        }
```

```
ссылка: 1
30          public string Decrypt(string text, int d)
31          {
32              var column = text.Length / d;
33              var symbols = new char[text.Length];
34              int index = 0;
35              for (int i = 0; i < column; i++)
36              {
37                  for (int j = 0; j < d; j++)
38                  {
39                      symbols[i + column * j] = text[index];
40                      index++;
41                  }
42              }
43
44              return string.Join("", symbols);
45          }
46      }
47
        Ссылок: 0
48      class Program
49      {
            Ссылок: 0
50          static void Main(string[] args)
51          {
52              var scytale = new ScytaleCipher();
53              Console.Write("Введите текст сообщения: ");
54              var message = Console.ReadLine();
55              Console.Write("Введите диаметр цилиндра: ");
56              var diameter = Convert.ToInt32(Console.ReadLine());
57              var encText = scytale.Encrypt(message, diameter);
58              Console.WriteLine("Зашифрованный текст : {0}", encText);
59              Console.WriteLine("Расшифрованный текст: {0}", scytale.Decrypt(encText, diameter));
60              Console.ReadLine();
61          }
62      }
63  }
```

Результат работы программы:



Видно, что результат работы программы совпал с расчетами.

Варианты заданий

№ варианта	Сообщение	Ключ
1	выполняйте практическую работу	3
2	пора писать реферат	4
3	скоро неделя отработки	5
4	не забывайте о сессии	6
5	не нужно много бездельничать	7

6	зачетная неделя начнется внезапно	3
7	лабораторные работы нужно делать	4
8	в понедельник начинаются зачеты	5
9	экзамены бывают по воскресеньям	6
10	в субботу проводятся зачеты	7

Рекомендуемая литература:

1. Информационная безопасность и защита информации: метод. указ. к лаб. работам / РГРТА. Сост.: Ю.И. Малинин, С.В. Аникеев, Д.Ю. Малинин. Рязань, 2005. 32 с.

2. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2009.- 24 с.

3. Информационная безопасность и защита информации: методические указания к лабораторным работам / РГРТУ. Сост. Ю.И.Малинин.- Рязань, 2011.- 24 с.

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Перед началом изучения дисциплины студенту необходимо ознакомиться с содержанием рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале РГРТУ и сайте кафедры.

Методические рекомендации студентам по работе над конспектом лекции

Основу теоретического обучения студентов составляют лекции. Они дают систематизированные знания студентам о наиболее сложных и актуальных проблемах изучаемой дисциплины. На лекциях особое внимание уделяется не только усвоению студентами изучаемых проблем, но и стимулированию их активной познавательной деятельности, творческого мышления, развитию научного мировоззрения, профессионально-значимых свойств и качеств.

Перед каждой лекцией студенту необходимо просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы.

Перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях. Не оставляйте «белых пятен» в освоении материала.

Во время лекции студенты должны не только внимательно воспринимать действия преподавателя, но и самостоятельно мыслить, добиваться понимания изучаемого предмета. Студенты должны аккуратно вести конспект. В случае недопонимания какой-либо части предмета следует задать вопрос в установленном порядке преподавателю. В процессе работы на лекции необходимо так же выполнять в конспектах модели изучаемого предмета (рисунки, схемы, чертежи и т.д.), которые использует преподаватель.

Слушая лекцию, нужно из всего получаемого материала выбирать и записывать самое главное. Следует знать, что главные положения лекции преподаватель обычно выделяет интонацией или повторяет несколько раз. Именно поэтому предварительная подготовка к лекции позволит студенту уловить тот момент, когда следует перейти к конспектированию, а когда можно просто внимательно слушать лекцию. В связи с этим нелишне перед началом сессии еще раз бегло просмотреть учебники или прежние конспекты по изучаемым предметам. Это станет первичным знакомством с тем материалом, который прозвучит на лекции, а также создаст необходимый психологический настрой.

Чтобы правильно и быстро конспектировать лекцию важно учитывать, что способы подачи лекционного материала могут быть разными. Преподаватель может диктовать материал, или рассказывать его, не давая ничего под запись, или проводить занятие в форме диалога со студентами. Чаще всего можно наблюдать соединение двух или трех вышеназванных способов.

Эффективность конспектирования зависит от умения владеть правильной методикой записи лекции. Конечно, способы конспектирования у каждого человека индивидуальны. Однако существуют некоторые наиболее употребляемые и целесообразные приемы записи лекционного материала.

Запись лекции можно вести в виде тезисов – коротких, простых предложений, фиксирующих только основное содержание материала. Количество и краткость тезисов может определяться как преподавателем, так и студентом. Естественно, что такая запись лекции требует впоследствии обращения к дополнительной литературе. На отдельные лекции можно приносить соответствующий иллюстративный материал на бумажных или электронных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции.

Кроме тезисов важно записывать примеры, доказательства, даты и цифры. Значительно облегчают понимание лекции те схемы и графики, которыми преподаватель иллюстрирует теоретический материал. По мере возможности студенты должны переносить их в тетрадь рядом с тем текстом, к которому эти схемы и графики относятся.

Хорошо если конспект лекции дополняется собственными мыслями, суждениями, вопросами, возникающими в ходе прослушивания содержания лекции. Те вопросы, которые возникают у студента при конспектировании лекции, не всегда целесообразно задавать сразу при их возникновении, чтобы не нарушить ход рассуждений преподавателя. Студент может попытаться ответить на них сам в процессе подготовки к практическим занятиям либо обсудить их с преподавателем на консультации.

Важно и то, как будет расположен материал в лекции. Если запись тезисов ведется по всей строке, то целесообразно отделять их время от времени красной строкой или пропуском строки. Примеры же и дополнительные сведения можно смещать вправо или влево под тезисом, а также на поля. В тетради нужно выделять темы лекций, записывать рекомендуемую для самостоятельной подготовки литературу, внести фамилию, имя и отчество преподавателя. Наличие полей в тетради позволяет не только получить «ровный» текст, но и дает возможность при необходимости вставить важные дополнения и изменения в конспект лекции.

При составлении конспектов необходимо использовать избыточность русского языка, сокращая слова. Так в процессе совершенствования навыков конспектирования лекций важно выработать индивидуальную систему записи материала, научиться рационально сокращать слова и отдельные словосочетания.

Практика показывает, что не всегда студенту удается успевать записывать слова лектора даже при использовании приемов сокращения слов. В этом случае допустимо обратиться к лектору с просьбой повторить сказанное. При обращении важно четко сформулировать просьбу, указать какой отрывок необходимо воспроизвести еще раз. Однако не всегда удобно прерывать ход лекции. В этом случае можно оставить пропуск, и после лекции устранить его при помощи конспекта соседа. Важно сделать это в короткий срок, пока свежа память о воспринятой на лекции информации.

Работу над конспектом следует начинать с его доработки, желательно в тот же день, пока материал еще легко воспроизводим в памяти (через 10 часов после лекции в памяти остается не более 30-40 % материала). С целью доработки необходимо прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Далее следует прочитать материал по рекомендуемой литературе, разрешая в ходе чтения возникшие ранее затруднения, вопросы, а также дополняя и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. В ходе доработки конспекта углубляются, расширяются и закрепляются знания, а также дополняется, исправляется и совершенствуется конспект.

Подготовленный конспект и рекомендуемая литература используются при подготовке к практическим занятиям. Подготовка сводится к внимательному прочтению учебного материала, к выводу с карандашом в руках всех утверждений и формул, к решению примеров, задач, к ответам на вопросы. Примеры, задачи, вопросы по теме являются средством самоконтроля.

Непременным условием глубокого усвоения учебного материала является знание основ, на которых строится изложение материала. Обычно преподаватель напоминает, какой ранее изученный материал и в какой степени требуется подготовить к очередному занятию. Обращение к ранее изученному материалу не только помогает восстановить в памяти известные положения, выводы, но и

приводит разрозненные знания в систему, углубляет и расширяет их. Каждый возврат к старому материалу позволяет найти в нем что-то новое, переосмыслить его с иных позиций, определить для него наиболее подходящее место в уже имеющейся системе знаний. Неоднократное обращение к пройденному материалу является наиболее рациональной формой приобретения и закрепления знаний.

Методические рекомендации студентам по работе с литературой

В рабочей программе дисциплины для каждого раздела и темы дисциплины указывается основная и дополнительная литература, позволяющая более глубоко изучить данный вопрос. Обычно список всей рекомендуемой литературы преподаватель озвучивает на первой лекции или дает ссылки на ее местонахождение (на образовательном портале РГРТУ, на сайте кафедры и т.д.).

При работе с рекомендуемой литературой целесообразно придерживаться такой последовательности. Сначала лучше прочитать заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать.

План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала.

Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:

- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу.

В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации студентам по подготовке к лабораторным работам

Лабораторная работа — это форма организации учебного процесса, когда обучающиеся по заданию и под руководством преподавателя самостоятельно проводят вычислительные расчеты и экспериментальные исследования на основе специально разработанных заданий.

Для проведения лабораторных работ используется вычислительная техника, которые размещаются в специально оборудованных учебных лабораториях. Перед началом цикла практических работ преподаватель или другое ответственное лицо проводит с обучающимися инструктаж о правилах техники безопасности в данной лаборатории, после чего студенты расписываются в специальном журнале техники безопасности.

По каждой лабораторной работе разрабатываются методические указания по их проведению. Они используются обучающимися при выполнении практической работы.

Применяются разные формы организации обучающихся на практических работах: фронтальная, групповая и индивидуальная. При фронтальной форме организации занятий все обучающиеся выполняют одновременно одну и ту же работу. При групповой форме организации занятий одна и та же работа выполняется группами по 2-5 человек. При индивидуальной форме организации занятий каждый обучающийся выполняет индивидуальное задание. Выбор метода зависит от учебно-методической базы и задач курса.

До начала лабораторной работы студент должен ознакомиться с теоретическими вопросами, которые будут изучаться или исследоваться в этой работе. Также необходимо познакомиться с принципами работы лабораторного оборудования, используемого в практической работе. Перед началом практической работы преподаватель может провести проверку знаний обучающихся - их теоретической готовности к выполнению задания. По итогам этой проверки студент допускается или не допускается к данной работе. О такой исходной проверке преподаватель информирует студентов заранее. Также возможна ситуация, когда допуском к очередной практической работе является своевременная сдача предыдущей практической работы (или подготовка отчета по ней).

Во время лабораторной работы обучающиеся выполняют запланированное практическое задание. Все полученные результаты необходимо зафиксировать в черновике отчета или сохранить в электронном виде на сменном носителе.

Завершается лабораторная работа оформлением индивидуального отчета и его защитой перед преподавателем.

Приступая к работе в лаборатории студенту следует знать, что в отличии от других видов занятий, пропущенную или некачественно выполненную практическую работу нельзя отработать в любое время. Для этого существуют специальные дополнительные дни ликвидации учебных задолженностей. Поэтому пропускать практическую работу без уважительной причины крайне нежелательно.

При подготовке к лабораторным работам по дисциплине «Информационная безопасность» следует использовать методические указания [1-3].

Методические рекомендации студентам по подготовке к зачету

При подготовке к зачету студент должен повторно изучить конспекты лекций и рекомендованную литературу, просмотреть решения основных задач, решенных самостоятельно и на лабораторных работах.

Необходимо помнить, что промежутки между очередными зачетами обычно составляют всего несколько дней. Поэтому подготовку к ним нужно начинать заблаговременно в течение семестра. До наступления сессии уточните у преподавателя порядок проведения промежуточной аттестации по его предмету и формулировки критериев для количественной оценивания уровня подготовки студентов. Для итоговой положительной оценки по предмету необходимо вовремя и с нужным качеством выполнить или защитить контрольные работы, практические работы, так как всё это может являться обязательной частью учебного процесса по данной дисциплине.

Рекомендуется разработать план подготовки к каждому зачету, в котором указать, какие вопросы или билеты нужно выучить, какие задачи решить за указанный в плане временной отрезок.

Также бывает полезно вначале изучить более сложные вопросы, а затем переходить к изучению более простых вопросов. При этом желательно в начале каждого следующего дня подготовки бегло освежить в памяти выученный ранее материал.

В период экзаменационной сессии организм студента работает в крайне напряженном режиме и для успешной сдачи сессии нужно не забывать о простых, но обязательных правилах:

- по возможности обеспечить достаточную изоляцию: не отвлекаться на разговоры с друзьями, просмотры телепередач, общение в социальных сетях;
- уделять достаточное время сну;
- отказаться от успокоительных. Здоровое волнение – это нормально. Лучше снимать волнение небольшими прогулками, самовнушением;
- внушать себе, что сессия – это не проблема. Это нормальный рабочий процесс. Не накручивайте себя, не создавайте трагедий в своей голове;
- помогите своему организму – обеспечьте ему полноценное питание, давайте ему периоды отдыха с переменой вида деятельности;
- следуйте плану подготовки.

Методические рекомендации студентам по проведению самостоятельной работы

Самостоятельная работа студента над учебным материалом является неотъемлемой частью учебного процесса в вузе.

В учебном процессе образовательного учреждения выделяются два вида самостоятельной работы:

1) аудиторная – выполняется на учебных занятиях, под непосредственным руководством преподавателя и по его заданию), студентам могут быть предложены следующие виды заданий:

– выполнение самостоятельных работ;

– выполнение практических работ;

– составление схем, диаграмм, заполнение таблиц;

– решение задач;

– работу со справочной, нормативной документацией и научной литературой;

– защиту выполненных работ;

– тестирование и т.д.

2) внеаудиторная – выполняется по заданию преподавателя, но без его непосредственного участия, включает следующие виды деятельности.

– подготовку к аудиторным занятиям (теоретическим и практическим работам);

– изучение учебного материала, вынесенного на самостоятельную проработку: работа над определенными темами, разделами, вынесенными на самостоятельное изучение в соответствии с рабочими программами учебной дисциплины или профессионального модуля;

– выполнение домашних заданий разнообразного характера;

– выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы;

– подготовку к практической работе, зачету;

– другие виды внеаудиторной самостоятельной работы.

Внеаудиторные самостоятельные работы представляют собой логическое продолжение аудиторных занятий, проводятся по заданию преподавателя, который инструктирует студентов и устанавливает сроки выполнения задания.

При планировании заданий для внеаудиторной самостоятельной работы используются следующие типы самостоятельной работы:

– воспроизводящая (репродуктивная), предполагающая алгоритмическую деятельность по образцу в аналогичной ситуации. Включает следующую основную деятельность: самостоятельное прочтение, просмотр, конспектирование учебной литературы, прослушивание записанных лекций, заучивание, пересказ, запоминание, Internet–ресурсы, повторение учебного материала и др.

– реконструктивная, связанная с использованием накопленных знаний и известного способа действия в частично измененной ситуации, предполагает подготовку отчетов по практическим работам, подбор литературы по дисциплинарным проблемам, подготовка к защите практических работ и др.

– эвристическая (частично-поисковая) и творческая, направленная на развитие способностей студентов к исследовательской деятельности.

Одной из важных форм самостоятельной работы студента является работа с литературой ко всем видам занятий. Самостоятельная работа студента с литературой позволяет ему более углубленно вникнуть в изучаемую тему.

Один из методов работы с литературой – повторение: прочитанный текст можно заучить наизусть. Простое повторение воздействует на память механически и поверхностно. Полученные таким путем сведения легко забываются.

Более эффективный метод – метод кодирования: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию и закодировать ее для хранения, важно провести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными. Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения.

Изучение научной, учебной и иной литературы требует ведения рабочих записей. Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

План – структура письменной работы, определяющая последовательность изложения материала. Он является наиболее краткой и потому самой доступной и распространенной формой записей содержания исходного источника информации. По существу, это перечень основных вопросов, рассматриваемых в источнике. План может быть простым и развернутым. Их отличие состоит в степени детализации содержания и, соответственно, в объеме.

Преимущество плана состоит в том, что план позволяет наилучшим образом уяснить логику мысли автора, упрощает понимание главных моментов произведения. Кроме того, он позволяет быстро и глубоко проникнуть в сущность построения произведения и, следовательно, гораздо легче ориентироваться в его содержании и быстрее обычного вспомнить прочитанное. С помощью плана гораздо удобнее отыскивать в источнике нужные места, факты, цитаты и т.д.

Выписки представляют собой небольшие фрагменты текста (неполные и полные предложения, отдельные абзацы, а также дословные и близкие к дословным записи об излагаемых в нем фактах), содержащие в себе основной смысл содержания прочитанного. Выписки представляют собой более сложную форму записи содержания исходного источника информации. По сути, выписки – не что иное, как цитаты, заимствованные из текста. Выписки позволяют в концентрированные форме и с максимальной точностью воспроизвести наиболее важные мысли автора. В отдельных случаях – когда это оправдано с точки зрения продолжения работы над текстом – вполне допустимо заменять цитирование изложением, близким дословному.

Тезисы – сжатое изложение содержания изученного материала в утвердительной (реже опровергающей) форме. Отличие тезисов от обычных выписок состоит в том, что тезисам присуща значительно более высокая степень концентрации материала. В тезисах отмечается преобладание выводов над общими рассуждениями. Записываются они близко к оригинальному тексту, т. е. без использования прямого цитирования.

Аннотация – краткое изложение основного содержания исходного источника информации, дающее о нем обобщенное представление. К написанию аннотаций прибегают в тех случаях, когда подлинная ценность и пригодность исходного источника информации исполнителю письменной работы окончательно неясна, но в то же время о нем необходимо оставить краткую запись с обобщающей характеристикой.

Резюме – краткая оценка изученного содержания исходного источника информации, полученная, прежде всего, на основе содержащихся в нем выводов. Резюме весьма сходно по своей сути с аннотацией. Однако, в отличие от последней, текст резюме концентрирует в себе данные не из основного содержания исходного источника информации, а из его заключительной части, прежде всего, выводов. Но, как и в случае с аннотацией, резюме излагается своими словами – выдержки из оригинального текста в нем практически не встречаются.

Конспект представляет собой сложную запись содержания исходного текста, включающая в себя заимствования (цитаты) наиболее примечательных мест в сочетании с планом источника, а также сжатый анализ записанного материала и выводы по нему.

При выполнении конспекта требуется внимательно прочитать текст, уточнить в справочной литературе непонятные слова и вынести справочные данные на поля конспекта. Нужно выделить главное, составить план. Затем следует кратко сформулировать основные положения текста, отметить аргументацию автора. Записи материала следует проводить, четко следуя пунктам плана и выражая мысль своими словами. Цитаты должны быть записаны грамотно, учитывать 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. Необходимо указывать библиографическое описание конспектируемого источника.

3. ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

ПК-2.1:

1. Информационная безопасность – это:

а) состояние защищенности информационных ресурсов от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства

b) состояние уязвимости информационных ресурсов от внутренних и внешних угроз,

способных нанести ущерб интересам личности, общества, государства

c) состояние защищенности граждан от внутренних и внешних угроз, способных нанести ущерб интересам личности

2. Безопасность информации – это:

а) защищенность информации от нежелательного ее разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования

b) защищенность информации от желательного ее разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования

c) доступность информации для ее тиражирования

3. Информационная система – это:

а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

b) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий

c) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку технических средств

4. _____ – это возможность за приемлемое время получить требуемую информационную услугу (**доступность**)

5. _____ – это защита от несанкционированного доступа к информации (**конфиденциальность**)

6. _____ – это промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется (**окно опасности**)

7. _____ – это потенциальная возможность определенным образом нарушить информационную безопасность (**угроза**)

8. _____ – это попытка реализации угрозы (**атака**)

9. _____ – это код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы (**вирусы**)

10. _____ – это код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (**черви**)

11. Угроза нарушения конфиденциальности реализуется когда:

а) информация становится известной лицу, не располагающему полномочиями доступа к ней

b) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую

c) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы

12. Угроза нарушения целостности реализуется когда:

а) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую

b) информация становится известной лицу, не располагающему полномочиями доступа к ней

c) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы

13. Угроза нарушения доступности реализуется когда:

а) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы

b) информация становится известной лицу, не располагающему полномочиями доступа к ней

c) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую

14. _____ – это выполнение действий под видом лица, обладающего полномочиями для доступа к данным (**маскарад**)

15. Принцип разделения обязанностей предписывает как:

а) распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс

b) распределять роли и ответственность, чтобы несколько человек не могли нарушить критически важный для организации процесс

c) распределять роли и ответственность, чтобы один человек мог нарушить критически важный для организации процесс

16. Принцип минимизации привилегий предписывает выделять:

a) пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей

b) пользователям максимальное количество прав доступа

c) пользователям права доступа, которые необходимы им для выполнения служебных обязанностей, а также некоторые дополнительные права

17. Основной принцип физической защиты формулируется как:

а) "непрерывность защиты в пространстве и времени"

b) "непрерывность защиты в пространстве"

c) "непрерывность защиты во времени"

18. Какие меры позволяют контролировать и при необходимости ограничивать вход и *выход* сотрудников и посетителей? (**меры физического управления доступом**)

19. Реакция на нарушения режима безопасности преследует цели:

a) локализация инцидента и уменьшение наносимого вреда, выявление нарушителя, предупреждение повторных нарушений

b) локализация инцидента и уменьшение наносимого вреда, предупреждение повторных нарушений

b) локализация инцидента и уменьшение наносимого вреда, выявление нарушителя

20. Планирование восстановительных работ позволяет:

а) подготовиться к авариям, уменьшить ущерб от аварий, сохранить способность к функционированию хотя бы в минимальном объеме

b) подготовиться к авариям, сохранить способность к функционированию хотя бы в минимальном объеме

c) уменьшить ущерб от аварий, сохранить способность к функционированию хотя бы в минимальном объеме

21. Корпоративная сеть имеет:

а) несколько территориально разнесенных частей, связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией

b) одну территориально разнесенную часть

c) несколько территориально разнесенных частей, связи между которыми отсутствуют

22. К принципам архитектурной безопасности относятся:

а) непрерывность защиты в пространстве и времени, минимизация привилегий, разделение обязанностей, усиление самого слабого звена

b) непрерывность защиты в пространстве и времени, минимизация привилегий, разделение обязанностей, усиление самого сильного звена

c) непрерывность защиты в пространстве и времени, максимизация привилегий, разделение обязанностей, усиление самого слабого звена

23. Идентификация позволяет субъекту:

а) сообщить своё имя

b) узнать чужое имя

c) изменить своё имя

24. Повысить надежность парольной аутентификации позволяют следующие меры:

а) наложение технических ограничений, управление сроком действия пароля, ограничение доступа к файлу паролей, использование программных генераторов паролей

b) наложение технических ограничений, отсутствие управления сроком действия пароля, ограничение доступа к файлу паролей, использование программных генераторов паролей

c) отсутствие технических ограничений, управление сроком действия пароля, ограничение доступа к файлу паролей, запрет использования программных генераторов паролей

ПК-2.2:

25. Государственная тайна – это:

а) защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

b) защищаемые организацией сведения в области экономической деятельности, распространение которых может нанести ущерб безопасности организации

c) защищаемые государством сведения в области экономической, деятельности, распространение которых может нанести ущерб безопасности ряда организаций на территории Российской Федерации

26. Служебная тайна содержит:

a) информацию ограниченного распространения, к которой относятся несекретные сведения, касающиеся деятельности организации, ограничения на распространение которых диктуются служебной необходимостью

b) защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

c) сведения, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, когда к ним нет свободного доступа на законном основании и обладатель этих сведений принимает меры к охране их конфиденциальности

27. Какие меры способствуют повышению образованности общества в области информационной безопасности, помогают в разработке и распространении средств обеспечения информационной безопасности? (**направляющие и координирующие меры**)

28. Какие меры направлены на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности? (**меры ограничительной направленности**)

29. _____ – это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (**обладатель информации**)

30. _____ – это возможность получения информации и ее использования (**доступ к информации**)

31. _____ – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (**конфиденциальность информации**)

32. _____ – это действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц (**предоставление информации**)

33. _____ – это действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц (**распространение информации**)

34. _____ – это любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных (**обработка персональных данных**)

35. _____ – это обработка персональных данных с помощью средств вычислительной техники (**автоматизированная обработка персональных данных**)

36. _____ – это действия, направленные на раскрытие персональных данных неопределенному кругу лиц (**распространение персональных данных**)

37. _____ – это действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (**предоставление персональных данных**)

38. _____ – это временное прекращение обработки персональных данных (**блокирование персональных данных**)

39. _____ – это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (**уничтожение персональных данных**)

40. Для обеспечения высокой доступности необходимо соблюдать следующие принципы архитектурной безопасности:

a) внесение в конфигурацию избыточности, наличие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, отсутствие единой точки отказа

b) внесение в конфигурацию избыточности, наличие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, наличие единой точки отказа

c) внесение в конфигурацию избыточности, отсутствие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, отсутствие единой точки отказа

41. Под протоколированием понимается:

a) сбор и накопление информации о событиях, происходящих в информационной системе

b) сбор и накопление информации об операциях аутентификации, происходящих в информационной системе

c) сбор и накопление информации об операциях с файлами, происходящих в информационной системе

42. Аудит – это:

a) анализ накопленной информации, проводимый оперативно, в реальном времени или периодически

b) анализ накопленной информации, проводимый нерегулярно

c) накопление информации во времени

43. Сигнатура атаки – это:

a) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию

b) совокупность условий, при выполнении которых атака считается несостоявшейся

c) совокупность условий, при выполнении которых атака считается имеющей место, что не вызывает заранее определенной реакции

44. В симметричном шифровании используется:

a) один ключ

b) два ключа
c) три ключа

45. Хэш-функция – это:

а) труднообратимое преобразование данных, реализуемое средствами симметричного шифрования со связыванием блоков

b) легкообратимое преобразование данных, реализуемое средствами симметричного шифрования со связыванием блоков

c) средство архивирования данных

46. Экран – это:

а) средство разграничения доступа клиентов из одного множества к серверам из другого множества

b) средство доступа клиентов из одного множества к серверам из другого множества

c) средство доступа клиентов между рабочими станциями сети

47. Отказ – это:

а) событие, которое заключается в нарушении работоспособности изделия

b) событие, которое заключается в нарушении доступа к изделию

c) событие, которое заключается в улучшении работоспособности изделия

4. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

а) основная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html.— ЭБС «IPRbooks»

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.html.— ЭБС «IPRbooks»

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»

5. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 c.— Режим доступа: http://www.iprbookshop.ru/72341.html.— ЭБС «IPRbooks»

6. Дождиков В.Г. Краткий энциклопедический словарь по информационной безопасности [Электронный ресурс]/ Дождиков В.Г., Салтан М.И.— Электрон. текстовые данные.— М.: Энергия, 2010.— 239 c.— Режим доступа: http://www.iprbookshop.ru/5729.html.— ЭБС «IPRbooks»

7. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

8. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие / Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный

университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»

б) дополнительная литература

9. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие / Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011. — 260 с.— Режим доступа: http://www.iprbookshop.ru/26486.html.— ЭБС «IPRbooks»

5. КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
3. Сложные системы. Структурный подход.
4. Основные определения и критерии классификации угроз.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Управление персоналом. Физическая защита.
15. Поддержание работоспособности.
16. Реагирование на нарушения режима безопасности.
17. Планирование восстановительных работ.
18. Основные понятия программно-технического уровня. Архитектурная безопасность.
19. Экранирование. Анализ защищённости.
20. Отказоустойчивость. Безопасное восстановление.
21. Основные понятия криптографии.
22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos.
23. Идентификация/аутентификация с помощью биометрических данных.
24. Управление доступом. Ролевое управление доступом.
25. Активный аудит. Шифрование.
26. Симметричный метод шифрования.
27. Асимметричный метод шифрования.
28. Секретный и открытый ключ.
29. Криптография. Контроль целостности
30. Цифровые сертификаты.
31. Электронная цифровая подпись.
32. Экранирование. Фильтрация. Межсетевые экраны.
33. Классификация межсетевых экранов.
34. Архитектурная безопасность.
35. Транспортное экранирование. Анализ защищенности.

36. Сетевой сканер. Антивирусная защита. 34. Индекс функционирования для расписания, индекс функционирования по стоимости.