ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 2
по учебной дисциплине
«Защита информации»
на тему:

«Защита программных средств от несанкционированного копирования, исследования, модификации»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «Защита программных средств от несанкционированного копирования, исследования, модификации».

Учебная цель: овладение навыками составления и отладки модуля защиты ПО от исследования.

Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Методические разработки по программированию модулей защиты ПО от копирования, исследования и модификации.
3. Варианты типовых заданий на практическое занятие.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	Вступительная часть. Контрольный опрос.	10
2.	Учебные вопросы. ОСНОВНАЯ ЧАСТЬ: 1. Разработка программного модуля для защиты ПО от исследования. 2. Проверка работоспособности модуля путём установки его на любую программу 3. Составление отчёта о проделанной работе, защита программы у преподавателя.	 80 40 45
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	5

III. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части занятия производится контроль присутствия и готовности обучающихся к занятию. Объявляется тема, цель, учебные вопросы занятия и особенности его проведения.

Готовность группы к занятию проверяется контрольным опросом.

Вопрос 1: Что подразумевают под понятием защита от исследования?

Вопрос 2: Какими способами организуются защита от исследования?

Вопрос 3: Для чего необходим механизм защиты от исследования?

При отработке первого вопроса занятия основное внимание обратить на усвоение обучающимися принципов построения модулей защиты программ от исследования программ и их реализацию средствами языка си++, java.

При отработке второго вопроса отметить необходимость и важность модуля защиты от исследования в структуру любой программы, как решающего фактора своевременного и правильного решения задачи защиты ПО.

При отработке третьего вопроса необходимо акцентировать внимание на структуре отчета о проделанной работе и защите его основных положений.

В заключительной части занятия подвести итоги, оценить действия обучающихся, ответить на вопросы.

Дать задание на самоподготовку. Объявить тему следующего занятия.

IV. УЧЕБНЫЕ МАТЕРИАЛЫ

1. Сведения из теории

1. Самым простым шифром является **ШИФР С ЗАМЕНОЙ БУКВ ЦИФРАМИ**. Каждой букве соответствует число по алфавитному порядку.

A-1, B-2, C-3 и т.д. Например слово «*TOWN*» можно записать как «*20 15 23 14*», но особой секретности и сложности в дешифровке это не вызовет.

2. Также можно зашифровывать сообщения с помощью **ЦИФРОВОЙ ТАБЛИЦЫ**. Её параметры могут быть какими угодно, главное чтобы получатель и отправитель были в курсе. Пример цифровой таблицы.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	1	2	3	4
7	5	6	7	8	9
8	o	.	,	?	!

Первая цифра в шифре – столбец, вторая – строка или наоборот. Так слово «*MIND*» можно зашифровать как «*33 24 34 14*».

3. КНИЖНЫЙ ШИФР

В таком шифре ключом является некая книга, имеющаяся и у отправителя и у получателя. В шифре обозначается страница книги и строка, первое слово которой и является разгадкой. Дешифровка невозможна, если книги у отправителя и корреспондента разных годов издания и выпуска. Книги обязательно должны быть идентичными.

4. ШИФР ЦЕЗАРЯ (шифр сдвига, сдвиг Цезаря)

Известный шифр. Сутью данного шифра является замена одной буквы другой, находящейся на некоторое постоянное число позиций левее или правее от неё в алфавите. Гай Юлий Цезарь использовал этот способ шифрования при переписке со своими генералами для защиты военных сообщений. Этот шифр довольно легко взламывается, поэтому используется редко. Сдвиг на 4. A = E, B= F, C=G, D=H и т.д.

Пример шифра Цезаря: зашифруем слово « *DEDUCTION* » . Получаем: *GHGXFWLRQ* . (сдвиг на 3)

5. ШИФР С КОДОВЫМ СЛОВОМ ЕЩЕ ОДИН ПРОСТОЙ СПОСОБ КАК В ШИФРОВАНИИ, ТАК И В РАСШИФРОВКЕ.

Используется кодовое слово (любое слово без повторяющихся букв). Данное слово вставляется впереди алфавита и остальные буквы по порядку дописываются, исключая те, которые уже есть в кодовом слове. Пример: кодовое слово – NOTEPAD.
Исходный: 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
Замена: N O T E P A D B C F G H I J K L M Q R S U V W X Y Z

6. ШИФР АТБАШ

Один из наиболее простых способов шифрования. Первая буква алфавита заменяется на последнюю, вторая – на предпоследнюю и т.д.
Пример: « *SCIENCE* » = *HXRVMXV*

7. ШИФР ФРЕНСИСА БЭКОНА

Один из наиболее простых методов шифрования. Для шифрования используется алфавит шифра Бэкона: каждая буква слова заменяется группой из пяти букв «A» или «B» (двоичный код).

a AAAAA g AABBA m ABABB s BAAAB y BABBA

b AAAAB h AABBB n ABBAA t BAABA z BABBB

c AAABA i ABAAA o ABBAB u BAABB

d AAABB j BBBAA p ABBBA v BBBAB

e AABAA k ABAAB q ABBBB w BABAA

f AABAB l ABABA r BAAAA x BABAB

Сложность дешифрования заключается в определении шифра. Как только он определен, сообщение легко раскладывается по алфавиту.
Существует несколько способов кодирования.
Также можно зашифровать предложение с помощью двоичного кода. Определяются параметры (например, «A» - от A до L, «B» - от L до Z). Таким образом, *BAABAAAAABAAAABABABB* означает *TheScience of Deduction* ! Этот способ более сложен и утомителен, но намного надежнее алфавитного варианта.

8. ШИФР БЛЕЗА ВИЖЕНЕРА

Этот шифр использовался конфедератами во время Гражданской войны. Шифр состоит из 26 шифров Цезаря с различными значениями сдвига (26 букв лат.алфавита). Для зашифровывания может использоваться tabula recta (квадрат Виженера). Изначально выбирается слово-ключ и исходный текст. Слово ключ записывается циклически, пока не заполнит всю длину исходного текста. Далее по таблице буквы ключа и исходного текста пересекаются в таблице и образуют зашифрованный текст.

	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

9. ШИФР ЛЕСТЕРА ХИЛЛА

Основан на линейной алгебре. Был изобретен в 1929 году. В таком шифре каждой букве соответствует число (A = 0, B =1 и т.д.). Блок из n-букв рассматривается как n-мерный вектор и умножается на (n x n) матрицу по mod 26. Матрица и является ключом шифра. Для возможности расшифровки она должна быть обратима в Z_{26}^n. Для того, чтобы расшифровать сообщение, необходимо обратить зашифрованный текст обратно в вектор и умножить на обратную матрицу ключа. Для подробной информации – Википедия в помощь.

10. ШИФР ТРИТЕМИУСА

Усовершенствованный шифр Цезаря. При расшифровке легче всего пользоваться формулой:

$$L = (m+k)\ mod N\ ,$$

L-номер зашифрованной буквы в алфавите, m-порядковый номер буквы шифруемого текста в алфавите, k-число сдвига, N-количество букв в алфавите. Является частным случаем аффинного шифра.

11. ШИФР ГРОНСФЕЛЬДА

По своему содержанию этот шифр включает в себя шифр Цезаря и шифр Виженера, однако в шифре Гронсфельда используется числовой ключ. Зашифруем слово “THALAMUS”, используя в качестве ключа число 4123. Вписываем цифры числового ключа по порядку под каждой буквой слова. Цифра под буквой будет указывать на количество позиций, на которые нужно сдвинуть буквы. К примеру вместо T получится X и т.д.

T H A L A M U S
4 1 2 3 4 1 2 3

T U V W **X** Y Z
0 1 2 3 **4**

В итоге: *THALAMUS = XICOENWV*

12.ПОРОСЯЧЬЯ ЛАТЫНЬ

Чаще используется как детская забава, особой трудности в дешифровке не вызывает. Обязательно употребление английского языка, латынь здесь ни при чем.

В словах, начинающихся с согласных букв, эти согласные перемещаются назад и добавляется “суффикс” *ay. Пример : question = estionquay.* Если же слово начинается с гласной, то к концу просто добавляется *ay, way, yay*или *hay* (*пример :*

a dog = aay ogday).

В русском языке такой метод тоже используется. Называют его по-разному: “синий язык”, “солёный язык”, “белый язык”, “фиолетовый язык”. Таким образом, в Синем языке после слога, содержащего гласную, добавляется слог с этой же гласной, но с добавлением согласной “с” (т.к. язык синий). Пример : *Информация поступает в ядра таламуса = Инсифорсомасацисияся поссотусупасаетсе в ядсяраса тасаласамусусаса.*

13. КВАДРАТ ПОЛИБИЯ

Подобие цифровой таблицы. Существует несколько методов использования квадрата Полибия. Пример квадрата Полибия: составляем таблицу 5x5 (6x6 в зависимости от количества букв в алфавите).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1 МЕТОД. Вместо каждой буквы в слове используется соответствующая ей буква снизу *(A = F, B = G и т.д.)*. Пример: *CIPHER - HOUNIW.*

2 МЕТОД. Указываются соответствующие каждой букве цифры из таблицы. Первой пишется цифра по горизонтали, второй - по вертикали. *(A = 11, B = 21…)*. Пример: *CIPHER = 31 42 53 32 51 24*

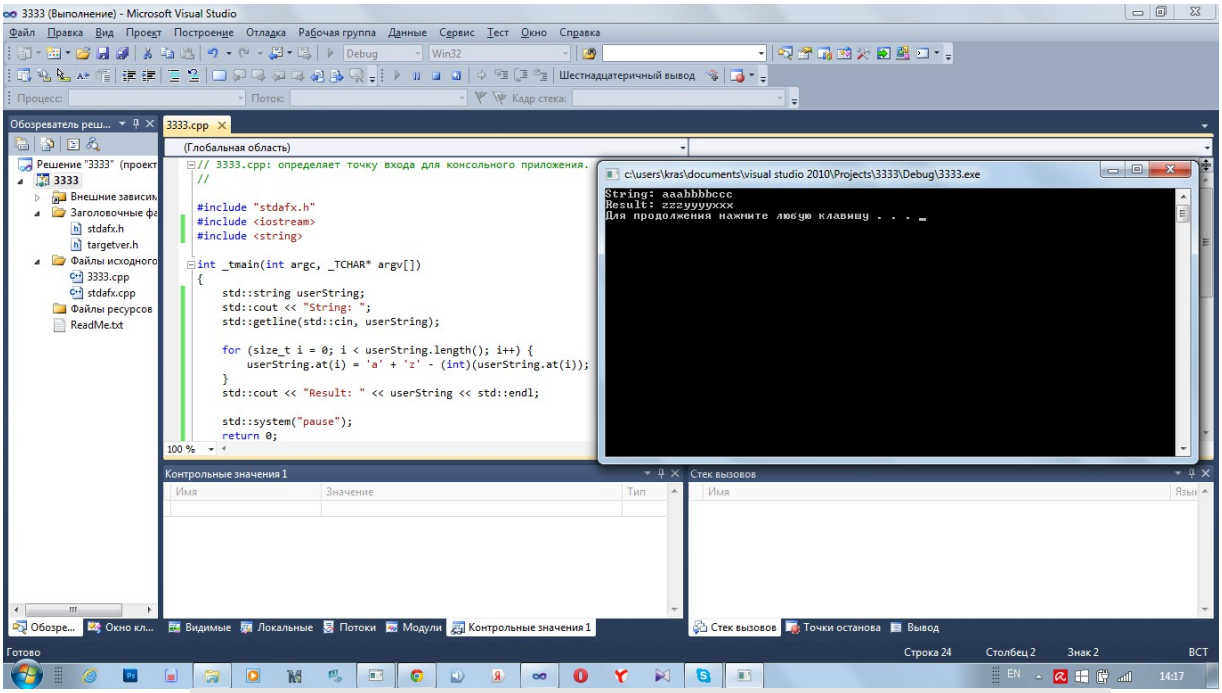
3 МЕТОД. Основываясь на предыдущий метод, запишем полученный код слитно. *314253325124.* Делаем сдвиг влево на одну позицию.*142533251243.* Снова разделяем код попарно.*14 25 33 25 12 43.* В итоге получаем шифр. Пары цифр соответствуют букве в таблице: *QWNWFO.*

3. Пример разработки программного модуля

Шифрование текста путем замены символов

```
#include <iostream>
#include <string>
```

```
int main()
{
   std::string userString;
   std::cout << "String: ";
   std::getline(std::cin, userString);

   for (size_t i = 0; i < userString.length(); i++) {
      userString.at(i) = 'a' + 'z' - (int)(userString.at(i));
   }
   std::cout << "Result: " << userString << std::endl;

   std::system("pause");
   return 0;
}
```



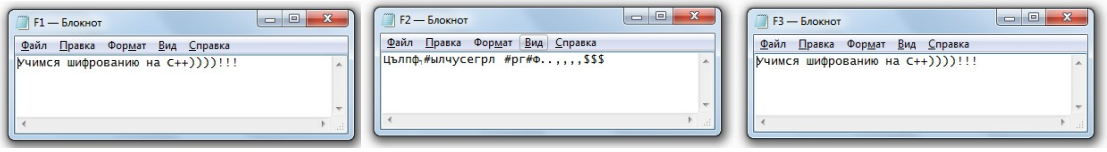
// Шифрование строки путем прибавления к коду символа числа

```
#include "stdafx.h"
#include <iostream>
#include <windows.h>
#include <fstream>

using namespace std;

void shifr_in(char str[], int key);   // зашифровка одной строки текста
void shifr_out(char str[], int key);  // расшифровка

int main()
{
   const int key = 3;  // постоянное число для прибавления к коду каждого символа
```

```
    char line[500];     // для временного хранения одной строки текста
    ifstream fin;       // файл для чтения
    ofstream fout;      // файл для записи

    // Зашифровка и запись в F2.txt
    fin.open("F1.txt"); // открытие файлов.
    fout.open("F2.txt");

    while ( fin.good() )    // пока ввод успешен и не достигнут конец файла ...
    {
        fin.getline(line, 500); // считываем одну строку во временную переменную line
        shifr_in(line, key);    // зашифровка этой строки
        fout << line << endl;   // запись зашифрованной строки в файл F2.txt
    }

    fin.close();        // закрытие файлов
    fout.close();


    // Расшифровка и запись в F3.txt
    fin.open("F2.txt");     // открытие файлов
    fout.open("F3.txt");

    while ( fin.good() )    // пока ввод успешен и не достигнут конец файла, ...
    {
        fin.getline(line, 500); // считываем одну строку зашифрованного текста во времнную пере-
менную
        shifr_out(line, key);   // дешифровка этой строки
        fout << line << endl;   // запись в F3.txt
    }

    fin.close();    // закрытие файлов
    fout.close();

    return 0;
}


void shifr_in(char str[], int key)
{
    for (int i=0; str[i]; i++)
        str[i] += key;
}

void shifr_out(char str[], int key)
{
    for (int i=0; str[i]; i++)
        str[i] -= key;
```

}

Результат работы программы



4. Общие методические указания курсантам (слушателям) по подготовке к практическим занятиям

Практические занятия по дисциплине «Защита информации» проводятся в классе ПЭВМ. Индивидуальные задания выполняются каждым курсантом лично.

Перед выполнением задания обучающийся изучает материал, приведенный в разделе «Учебные материалы», в ходе которого необходимо разобрать приведенные примеры и выполнить задания раздела. На следующем этапе работы обучающийся выполняет индивидуальное задание.

Результаты работы оформляются в виде отчета. Содержание отчета приведено в руководстве по соответствующему практическому занятию.

По готовности к защите работы курсант (слушатель) докладывает преподавателю.

5. Индивидуальные задания к практическому занятию

Задание 1

1. Разработать программный модуль для защиты ПО от исследования, используя шифр Цезаря.
2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:
   Строка № 1) Защита информации;
   Строка № 2) Организация защиты информации.
3. Зашифровать текстовый фаил при помощи разработанного модуля.

Задание 2

Разработать программный модуль для защиты ПО от исследования, используя шифр Цезаря, с возможностью декодировки.

Создать текстовй фаил «F1.txt» состоящий из следующих строк:
   Строка № 1) Лмбттоьк шбт;
   Строка № 2) Вёмпё тпмочё рфтуьой.
3. Декодировать текстовый фаил при помощи разработанного модуля.

Задание 3

Шифр Виженера. Это шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т.д. Используя в качестве ключевого слово ЗИМА, закодировать слова: АЛГОРИТМИЗАЦИЯ, КОМПЬЮТЕР, ИНТЕРНЕТ.

1. Разработать программный модуль для защиты ПО от исследования, используя Шифр Виженера.
2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) Защита информации;

Строка № 2) Организация защиты информации.

3. Зашифровать текстовый фаил при помощи разработанного модуля.

Задание 4

1. Разработать программный модуль для защиты ПО от исследования, используя шифр Виженера, с возможностью декодировки.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) Слово получено с помощью шифра Виженера – ЖПЮЩЕБ;

Строка № 2) Ключевое слово – БАНК.

3. Декодировать текстовый фаил при помощи разработанного модуля.

Задание 5

1. Разработать программный модуль для защиты ПО от исследования, используя в качестве ключа расположение букв на клавиатуре вашего компьютера.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) D ktce hjlbkfcm `kjxrf?;

Строка № 2) D ktce jyf hjckf?.

3. Декодировать текстовый фаил при помощи разработанного модуля.

Задание 6

1. Разработать программный модуль для защиты ПО от исследования, используя используя в качестве ключа расположение букв на клавиатуре вашего компьютера.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) Москва - столица России.

3. Закодировать текстовый фаил при помощи разработанного модуля.

Задание 7

1. Разработать программный модуль для защиты ПО от исследования, используя шифр перестановки, кодирование осуществляется перестановкой букв в слове по одному и тому же правилу

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) НИМАРЕЛ.

Строка № 2) ЛЕТОФЕН.

Строка № 3) НИЛКЙЕА.

Строка № 4) НОМОТИР.

Строка № 5) РАКДНАША.

3. Восстановить слова и определить правило перестановки.

Задание 8

Разработать программный модуль для защиты ПО от исследования, используя шифр перестановки, кодирование осуществляется перестановкой букв в слове по одному и тому же правилу

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) КЭРНОЦЛИТКЭЛУОНПИЕЖДАИФЯ.

Строка № 2) УКРОГРЕОШЛАЕКВИСЧТЕВМО.

3. Восстановить слова и определить правило шифрования и расшифрования слов.

Задание 9

Разработать программный модуль для защиты ПО от исследования, используя ключ.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) АКБМУНИЯДКУМВРЛ ИКСЯМТР.

Строка № 2) ТДЯДФМУУЫЙ АРЗГМВМА.

Строка № 3) Ключ: РА ДЕ КИ МО НУ ЛЯ.

3. Расшифровать текстовый фаил при помощи разработанного модуля.

Задание 10

Разработать программный модуль для защиты ПО от исследования, используя ключ.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) Рыбак рыбака видит издалека.

Строка № 2) Сделал дело - гуляй смело.

Строка № 3) Ключ: РА ДЕ КИ МО НУ ЛЯ.

3. Зашифровать текстовый фаил при помощи разработанного модуля.

Задание 11

Разработать программный модуль для защиты ПО от исследования, используя ключ.

2. Создать текстовй фаил «F1.txt» состоящий из следующих строк:

Строка № 1) Бит - это минимальная единица измерения информации.

Строка № 2) Ключ: придумать.

3. Зашифровать текстовый фаил при помощи разработанного модуля.

6. Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

– название практического занятия;

– текст индивидуального задания;

– блок-схему алгоритма решения задачи;

– исходный текст программы;

– результаты тестирования решения.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

7. Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

8.Задание и методические указания курсантам на самостоятельную подготовку:

1. Повторить по конспекту лекций и рекомендованной литературе основные методы защиты от исследования.
2. Быть готовыми к самостоятельному составлению программ с использованием программных модулей защиты от исследования.

V. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Информационная безопасность: – учебное пособие / В.М.Зима, СПб.: ВКА имени А.Ф.Можайского, 2017 с.

2. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Ч.2. Сетевые ОС и принципы обеспечения информационной безопасности в сетях / С.И. Макаренко, А.А. Ковальский, С.А. Краснов СПб.: Наукоемкие технологии 2020.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.