

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Методические указания**  
по выполнению лабораторных и практических работ  
по дисциплине «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»  
для студентов специальности 10.05.01 Компьютерная безопасность  
специализация «Информационно-аналитическая и техническая экспертиза  
компьютерных систем»

Ставрополь  
2026

## СОДЕРЖАНИЕ

|                                                                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ЛАБОРАТОРНАЯ РАБОТА № 1. Управление доступом в ОС Windows и Linux .....                                                                             | 3  |
| ЛАБОРАТОРНАЯ РАБОТА № 2. Построение модели угроз ИСПДн .....                                                                                        | 8  |
| ЛАБОРАТОРНАЯ РАБОТА № 3. Реализация политики безопасности Харрисона–Рузо–<br>Ульмана .....                                                          | 13 |
| ЛАБОРАТОРНАЯ РАБОТА № 4. Реализация политики безопасности Белла–ЛаПадула .....                                                                      | 22 |
| ЛАБОРАТОРНАЯ РАБОТА № 5. Реализация ролевой политики безопасности .....                                                                             | 32 |
| ЛАБОРАТОРНАЯ РАБОТА № 6. Схема Фейстеля. Шифр DES .....                                                                                             | 36 |
| ЛАБОРАТОРНАЯ РАБОТА № 7. Шифр ГОСТ 28147-89. Шифр Blowfish .....                                                                                    | 43 |
| ЛАБОРАТОРНАЯ РАБОТА № 8. Распределение ключей по схеме Диффи–Хеллмана.<br>Криптографическая система RSA. Криптографическая система Эль–Гамала ..... | 53 |
| ЛАБОРАТОРНАЯ РАБОТА № 9. Хэш-функции без ключа. Алгоритм SHA-1. Хэш-<br>функции с ключом .....                                                      | 64 |

## ЛАБОРАТОРНАЯ РАБОТА № 1. Управление доступом в ОС Windows и Linux

### 1. Цель работы

Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

|                                             |        |
|---------------------------------------------|--------|
| Вступительная часть                         | 2 мин  |
| Проверка готовности студентов к занятию     | 5 мин  |
| <b><i>Программа лабораторной работы</i></b> |        |
| 1. Описание лабораторной работы.            | 35 мин |
| 2. Задание.                                 | 35 мин |
| Проверка выполнения лабораторной работы     | 10 мин |
| Заключительная часть                        | 3 мин  |

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### 4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### 4.2. Требования безопасности во время работы

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### 4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы «L\_LUX.EXE»

## 7. Описание лабораторной работы

Для выполнения лабораторной работы необходимо запустить программу L\_LUX.EXE. На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения зашифрованных и расшифрованных текстов), в верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу «ENTER», вернуться в главное меню или вовсе выйти из него – «ESC».

А теперь более подробно рассмотрим каждый из пунктов главного меню.

### 7.1 Редактор

Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы.

Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню (кроме создания документа, открытия файла, выхода из программы, информации о программе) и большая часть клавиш панели управления (за исключением создания документа, открытия файла и выхода из программы).

**Создать документ (Ctrl+N)** – данный подпункт делает доступным для работы тестовый редактор (пользователь получает право создать свой текстовый файл, который впоследствии можно будет использовать при работе с программой), также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

**Открыть файл (Ctrl+L)** – при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в окне редактора текстов.

Аналогично пункту “Создать документ” доступным для работы становится текстовый редактор с отображаемым текстом, а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

**Сохранить файл (Ctrl+S)** - при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое редактора текстов.

**Выход из программы (Ctrl+X)** - при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

### 7.2 Гистограмма

Вывод на экран двух гистограмм, отображающих частоту встречаемости символов в тексте.

Имеется возможность просмотра следующих сочетаний гистограмм:

- гистограммы исходного и зашифрованного файла,
- гистограммы зашифрованного и расшифрованного файла,
- гистограммы стандартного распределения и зашифрованного текста,
- гистограммы стандартного распределения и расшифрованного текста.

В гистограммах с целью масштабирования используются левая и правая клавиши мыши.

Например, после шифрования текста большого объема пользователь хочет посмотреть гистограммы исходного и зашифрованного файла. Поскольку размеры текста достаточно большие, то на экран будут выведены две гистограммы с большим количеством столбцов в каждой (столбец соответствует одному символу текста), однако трудно будет сказать, какой из

этих столбцов соответствует тому или иному символу текста, и какова частота встречаемости данного символа. Поэтому у пользователя есть возможность увеличить масштаб любой из двух гистограмм с целью более точного определения требуемого значения частоты встречаемости конкретного символа. Для этого необходимо навести указатель мыши на левую границу того участка гистограммы, который требуется увеличить, затем нажать левую клавишу мыши, и не отпуская ее растянуть прямоугольник так, чтобы его нижний правый угол совпал с правой границей увеличиваемого участка гистограммы.

После этого следует отпустить левую клавишу мыши и на экране появится увеличенное изображение нужного участка.

Причем, нажав и не отпуская правую клавишу мыши, можно перемещать гистограмму в любом направлении с целью изучения всего полученного распределения в увеличенном масштабе. Для того, чтобы от увеличенного масштаба вернуться к исходному виду, нужно навести указатель мыши на гистограмму, затем нажать левую клавишу мыши, и, не отпуская ее, снизу вверх растянуть небольшой по размерам прямоугольник, после этого следует отпустить левую клавишу мыши и на экране появится исходное изображение гистограммы.

### **7.3 Шифрование**

Выполнение шифрования текстового файла осуществляется одним из семи методов, рассматриваемых в лабораторной работе.

1. Одноалфавитный метод (с фиксированным смещением).
2. Одноалфавитный метод с задаваемым смещением (от 2 до 20).
3. Перестановка символов.
4. По дополнению до 255 (инверсный метод).
5. Многоалфавитный метод (с фиксированным ключом).
6. Многоалфавитный метод с ключом фиксированной длины.
7. Многоалфавитный метод с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей «ENTER».

Затем появляется окно в котором в зависимости от метода шифрования требуется указать те или иные параметры, и либо подтвердить процесс кодировки, либо отказаться от него. После этого в окне редактора будет выдан зашифрованный текст.

### **7.4. Расшифрование**

Аналогично предыдущему пункту выбирается метод расшифрования (должен соответствовать методу, которым был зашифрован файл).

Снова появляется окно, в котором в зависимости от метода расшифрования требуется указать те или иные параметры, и либо подтвердить процесс расшифрования, либо отказаться от него.

После этого в окно редактора будет выдан расшифрованный текст. При правильном расшифровании, полученный текст совпадает с исходным.

## **8. Задания**

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение.

Для этого:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;
- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов,
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:

1) с помощью программы, после чего проверить в редакторе правильность расшифрования;

2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

3. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):

- для своего исходного текста выполнить шифрование с произвольным смещением;
- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;

- расшифровать текст с помощью программы;
- имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.

4. Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

1) вручную (объясните ваши действия);

2) с помощью программы.

5. Для инверсного кодирования:

- для своего произвольного файла выполните шифрование;
- просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
- дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

6. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе.

Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

7. Для многоалфавитного шифрования с ключом фиксированной длины:

- для файла, состоящего из строки одинаковых символов выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;
- для файла произвольного текста произвести шифрование и рас- шифрование;
- просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.

8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п.7.

9. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с

общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из рассмотренных, вы выберете? Обоснуйте свой выбор.
4. Целесообразно ли повторно применять для уже зашифрованного текста:  
а) метод многоалфавитного шифрования?  
б) метод Цезаря?

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А. И., Самсонов Б. Б., Кречет Т. В., Плохов Е. М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И.Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К.Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л.Добрушина и О.Б.Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 2. Построение модели угроз ИСПДн

### 1. Цель работы

Изучение методов шифрования/расшифрования перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера.

Исследование и сравнение стойкости различных методов, на основе атак путем перебора всех возможных ключей.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

|                                             |        |
|---------------------------------------------|--------|
| Вступительная часть                         | 2 мин  |
| Проверка готовности студентов к занятию     | 5 мин  |
| <b><i>Программа лабораторной работы</i></b> |        |
| 1. Описание лабораторной работы.            | 35 мин |
| 2. Задание.                                 | 35 мин |
| Проверка выполнения лабораторной работы     | 10 мин |
| Заключительная часть                        | 3 мин  |

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### 4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### 4.2. Требования безопасности во время работы

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### 4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

## **5. Аппаратное обеспечение**

Класс персональных ЭВМ, классная доска, мел (маркеры).

## **6. Программное обеспечение**

Программное обеспечение для выполнения лабораторной работы «*LAB\_RAB.exe*»

## **7. Описание лабораторной работы**

Для выполнения лабораторной работы необходимо запустить программу *LAB\_RAB.exe*, используемую для шифрования/расшифрования, а также дешифрования (методом протяжки вероятного слова) файлов.

Система реализует следующие функции:

- ввод, удаление и селекция ключей пользователя;
- поддержка списка ключей;
- шифрование и расшифрование текста;
- дешифрование текста путем подбора ключей, методом протяжки вероятного слова.

Система поддерживает следующие методы криптографического преобразования информации:

- замена;
- перестановка;
- гаммирование;
- таблица Виженера.

При запуске утилит шифрования и расшифрования у пользователя запрашивается подтверждение на правильность выбранного метода для работы и соответствия заданного ключа целям пользователя (также всегда при изменении файла в текстовом редакторе выдается запрос на сохранение изменений при каждом шаге, дальнейшее развитие которого приведет к необратимым изменениям в файле и потере изначальной информации).

Описание интерфейса.

- Окно текстового редактора с широким набором дополнительных функций.
- Таблица всех ключей, введенных в систему с быстрым доступом для ввода, удаления или выбора текущего ключа.
- Список всех методов шифрования для быстрого и удобного переключения между ними.
- Основное меню (вверху экрана).
- Дополнительное меню (вызывается нажатием правой кнопки мыши).
- Набор вспомогательных кнопок для быстрого и удобного интерфейса.

Поля вывода текущего состояния системы:

- текущий ключ;
- вероятное слово;
- сила ключа для протяжки.

### **7.1 Пример работы с программой**

1. Вводится список ключей.
2. Вводится вероятное слово (необязательно вначале, до его ввода все меню запуска протяжки все равно недоступны).
3. Выбирается необходимый метод шифрования.
4. Загружается исходный или зашифрованный файл (открываются соответствующие меню для шифрования и расшифрования).
5. Запускается необходимый процесс:
  - шифрование;
  - расшифрование;

- протяжка вероятного слова;
- конвертация текста.
- 6. Продолжение работы в любом порядке в соответствии с описанными пунктами.
- 7. При завершении работы не забудьте сохранить необходимые результаты (при закрытии и загрузке новых файлов система автоматически запрашивает подтверждение на запись).

## **7.2 Шифрование**

1. Открыть файл.
2. Внести необходимые изменения.
3. Настроить соответствующие параметры:
  - тип шифрования;
  - ключ;
  - прочие.

F5. 7.3 Запустить процесс шифрования через пункт меню УТИЛИТЫ \ ЗАШИФРОВАТЬ

## **7.4 Расшифрование**

1. Открыть файл.
2. Произвести необходимые изменения.
3. Настроить соответствующие параметры:
  - тип шифрования;
  - прочие.

7.4. Запустить процесс расшифрования через пункт меню УТИЛИТЫ \ РАСШИФРОВАТЬ F6.

## **7.5 Протяжка вероятного слова (дешифрование)**

1. Вводится вероятное слово (длинной от 1(3) до 9)
2. Для отделения вновь найденных ключей от предыдущих между ними добавляется надпись "подбор".
3. Перебор ключей.
4. Расшифровывается первая вся строка текста по текущему ключу.
5. Порциями, равными длине вероятного слова, сравнивается содержимое этой строки со значением вероятного слова.
6. Если найдено хоть одно совпадение, запоминаем ключ.
7. Переходим к новому ключу.
8. Переходим к следующей строке.

9. Результаты должны содержаться в списке ключей. Если совпадений не найдено, в список ключей ничего не добавляется.

## **7.6 Операции с ключами**

С базой ключей могут осуществляться следующие действия:

- добавить новый ключ;
- удалить одну запись;
- изменить активную запись;
- очистить всю таблицу введенных ключей.

## **7.7 Ключи для перестановки**

В каждый момент времени в системе может быть только один текущий ключ для перестановки.

Правила ввода ключа для перестановки:

1. При переключении в списке поддерживаемых системой методов шифрования на пункт "Перестановка" вызывается окно ввода ключа перестановки. Окно состоит из двух кнопок

(Отмены и Выхода без изменений и кнопки Enter – подтверждение установленной длины ключа) и окна задания длины ключа для перестановки.

2. В окне задания длины ключа необходимо выбрать необходимую длину (параметры заменяются в пределах 1 ... 9), и подтвердить желание использовать ключ именно такой длины.

3. После подтверждения в окне высветятся кнопки с цифрами на лицевой стороне (в количестве, равном длине ключа), при нажатии на кнопку происходит фиксация кнопки (ее обесцвечивание) для невозможности ее дальнейшего использования (так как все цифры в ключе перестановки должны быть неповторяющимися).

4. После перебора всех кнопок система запоминает введенный ключ, выводит его в поле ввода ключей и выходит из окна ввода ключа перестановки в окно основной программы.

## **8. Задания**

1. Ознакомиться с описанием лабораторной работы и заданием.

2. Выполнить настройку программы: выбрать метод шифрования; ввести ключи для всех методов; ввести вероятное слово; осуществить все остальные системные настройки.

3. Для метода замены (одноалфавитного метода):

- выбрать данный алгоритм в списке доступных методов шифрования;
- установить необходимое смещение;
- открыть произвольный файл;
- просмотреть содержимое исходного файла;
- выполнить для этого файла шифрование (при необходимости можно задать имя зашифрованного файла);
- просмотреть в редакторе зашифрованный файл;
- ввести вероятное слово;
- ввести вероятную длину ключа (кроме метода замены);
- подобрать ключ;
- выполнить расшифрование со всеми найденными ключами;
- найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;

– расшифровать файл исходным ключом;

– проверить результат.

4. Для метода перестановки:

- выбрать метод перестановки;
- в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
- далее действия полностью соответствуют изложенным в предыдущем пункте задания.

5. Для метода гаммирования:

- выбрать метод гаммирования;
- ввести ключ гаммирования;
- полностью повторить п. 3.

6. Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

7. Привести в отчете ответы на контрольные вопросы, в соответствии с номером

варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы.

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Чем отличается “псевдооткрытый” текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста? В чем преимущества и недостатки одноалфавитных методов?
2. Как зависит время вскрытия шифра описанным выше способом подбора
3. ключей от длины “вероятного” слова?
4. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
5. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 3. Реализация политики безопасности Харрисона-Рузо-Ульмана

### 1. Цель работы

Изучение принципов шифрования/расшифрования информации, используемых в шифровальной машине Энигма. Ознакомление с общими принципами действия шифровальной машины Энигма на примере эмулятора. Предварительно необходимо установить программу эмулятор Enigma3S.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

|                                             |        |
|---------------------------------------------|--------|
| Вступительная часть                         | 2 мин  |
| Проверка готовности студентов к занятию     | 5 мин  |
| <b><i>Программа лабораторной работы</i></b> |        |
| 1. Описание лабораторной работы.            | 35 мин |
| 2. Задание.                                 | 35 мин |
| Проверка выполнения лабораторной работы     | 10 мин |
| Заключительная часть                        | 3 мин  |

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### 4.1. Требования безопасности перед началом работ

**ЗАПРЕЩАЕТСЯ:**

- переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.
- получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### 4.2. Требования безопасности во время работы

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### 4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

## **5. Аппаратное обеспечение**

Класс персональных ЭВМ, классная доска, мел (маркеры).

## **6. Программное обеспечение**

Программное обеспечение для выполнения лабораторной работы «LAB\_RAB.exe»

## **7. Описание лабораторной работы**

### **7.1 Энигма, устройство и принцип действия**



Рис. 3.1. Внешний вид шифровальной машины Энигма

Энигма (*Enigma*) – портативная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Более точно, Энигма – целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

Энигма использовалась в коммерческих целях, а также в военных и государственных службах во многих странах мира, но наибольшее распространение получила в Германии во время второй мировой войны. Именно Энигма Вермахта (*Wehrmacht Enigma*) – немецкая военная модель – чаще всего является предметом изучения.

Хотя шифр Энигмы, с точки зрения криптографии, был достаточно слаб, но на практике лишь сочетание этого фактора с другими, такими, как ошибки операторов, процедурные изъяны и захваты экземпляров Энигмы и шифровальных книг, позволило английским криптоаналитикам вскрывать сообщения, зашифрованные шифром Энигмы.

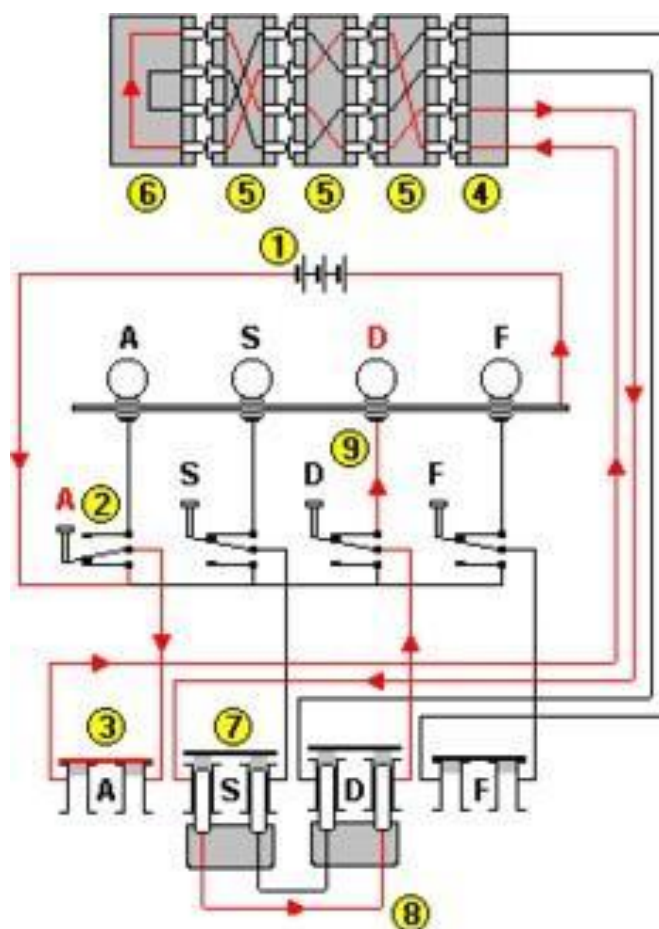


Рис. 3.2. Электрическая схема Энигмы (замена в тексте буквы 'A' буквой 'D')

Шифрующее действие Энигмы показано для двух последовательно нажатых клавиш – ток течет через роторы, "отражается" от рефлексора, затем снова возвращается через роторы. Серыми линиями на рисунке показаны другие возможные электрические цепи внутри каждого ротора. Буква "А" заменяется в шифротексте по-разному при последовательных нажатиях клавиши, сначала на "G", затем на "C". Сигнал идет по другому маршруту за счет поворота ротора.

Как и другие роторные машины, Энигма состояла из комбинации механических и электрических систем. Механическая часть включала клавиатуру, набор вращающихся дисков (роторов), расположенных вдоль вала, и ступенчатого механизма, приводящего в движение один или более роторов при каждом нажатии клавиши. Движение роторов приводит к различным вариантам подстановки символов при каждом следующем нажатии клавиши на клавиатуре.

Механические части двигались, образуя меняющийся электрический контур – то есть, фактически, шифрование осуществлялось электрически. При нажатии клавиш контур замыкался, ток проходил через различные компоненты и в итоге включал одну из множества лампочек, отображавшую выводимую букву. Например, при шифровании сообщения, начинающегося "ANX...", оператор вначале нажимал кнопку "А", и загоралась лампочка "Z", то есть "Z" становилась первой буквой криптограммы. Оператор продолжал шифрование, нажимая на клавиатуре "N" и, так далее, до конца исходного сообщения.

Постоянное изменение электрической цепи, через которую шел ток, вследствие вращения роторов, позволяло реализовать многоалфавитный шифр подстановки, что давало высокую стойкость для того времени.

## 7.2 Роторы

Роторы – это сердце Энигмы. Каждый ротор представляет собой диск примерно 10

см в диаметре, сделанный из твердой резины или бакелита, с пружинными штыревыми контактами на одной стороне ротора, расположенными по окружности; на другой стороне соответствующее количество плоских электрических контактов. Штыревые и плоские контакты соответствуют буквам в алфавите; обычно это 26 букв “А”...“Z”. При соприкосновении контакты соседних роторов замыкают электрическую цепь. Внутри ротора каждый штыревой контакт соединен с некоторым плоским.

Порядок соединения может быть различным.

Сам по себе ротор воспроизводит шифрование простой заменой символов. Например, контакт, отвечающий за букву “Е”, может быть соединен с контактом буквы “Т” на другой стороне ротора. Но при использовании нескольких роторов в связке (обычно трех или четырех), за счет их постоянного движения, получается более стойкий тип многоалфавитного шифрования.

Ротор может занимать одну из 26 позиций в машине. Он может быть повернут вручную при помощи рифленого пальцевого колесика, которое выдается наружу, как показано на Рис. 3.5. Чтобы оператор всегда мог определить положение ротора, на каждом ободе находится алфавитное кольцо; одна из букв видна через окошко. В ранних моделях Энигмы алфавитное кольцо было фиксировано; в более поздних версиях ввели усложненную конструкцию с возможностью его регулировки. Каждый ротор содержит выемку (или несколько выемок), используемых для управления движением роторов.

Военные версии Энигмы выпускались с несколькими роторами; первая модель содержала только три. В 1938 г. их стало пять, но только три из них одновременно использовались в машине. Эти типы роторов были маркированы римскими цифрами I, II, III, IV, V, и все с одной выемкой, расположенной в разных местах алфавитного кольца. В военно-морских версиях *Wehrmacht Enigma* содержалось большее количество роторов, чем в других: шесть, семь или восемь.

В *Wehrmacht Enigma* каждый ротор прикреплен к регулируемому кольцу с выемками. Пять базовых роторов (I-V) имели по одной выемке, тогда как военно-морские с дополнительными роторами (VI-VIII) — по две. В определенный момент, выемка попадает напротив собачки, позволяя ей зацепить храповик следующего ротора при последующем нажатии клавиши.

Когда же собачка не попадает в выемку, она просто проскальзывает по поверхности кольца, не цепляя шестеренки. В системе с одной выемкой второй ротор продвигается вперед на одну позицию в то время, как первый продвигается на 26. Аналогично, третий ротор продвигается на один шаг в то время, как второй делает 26 шагов. Особенностью было то, что второй ротор также поворачивался, если поворачивался третий; это означает, что второй ротор мог повернуться дважды при двух последовательных нажатиях клавиш, так называемое "двухшаговое движение", что приводит к уменьшению периода при шифровании.



Рис. 3.7. Роторы Энигмы в собранном состоянии. Три подвижных ротора помещены между двумя неподвижными деталями: входное кольцо и рефлексор (помечен "В" слева)

## 7.2 Входное колесо

Входное колесо (*Eintrittswalze* по-немецки), или входной статор, соединяет

коммутационную панель, или (в случае ее отсутствия) клавиатуру и ламповую панель, с роторами. Несмотря на то, что фиксированное соединение проводов имеет сравнительно меньшее значение с точки зрения безопасности, это оказалось некоторым препятствием в работе польского криптоаналитика Марьяна Реджевски, когда он пытался определить способ коммутации проводов внутри роторов. Коммерческая версия Энигмы соединяла буквы в порядке их следования на клавиатуре: QA, WB, EC и так далее. Однако, военная версия соединяла их в прямом алфавитном порядке: AA, BB, CC и т.д.

### **7.3 Рефлектор**

За исключением ранних моделей A и B, за последним ротором следовал рефлектор (*Umkehrwalze* по-немецки), запатентованная деталь, отличавшая семейство Энигмы от других роторных машин, разработанных в то время.

Рефлектор соединяет контакты последнего ротора попарно, коммутируя ток через роторы в обратном направлении, но по другому маршруту. Рефлектор гарантирует, что преобразование, реализуемое Энигмой, есть инволюция, т.е. процесс расшифрования симметричен процессу шифрования. Кроме того, рефлектор придает Энигме то свойство, что никакая буква не может быть зашифрована собой же. Это было серьезным концептуальным недостатком, впоследствии использованным дешифровальщиками.

### **7.4 Коммутационная панель**

Коммутационная панель, позволяющая оператору варьировать соединения проводов, впервые появилась в немецких военных версиях в 1930 г. и вскоре успешно использовалась и в военно-морских версиях.

Коммутационная панель внесла огромный вклад в усложнение шифра Энигмы, даже больший, чем введение дополнительного ротора. С Энигмой без коммутационной панели – "*unsteckered*" Энигмой – дешифровальщик может справиться практически вручную, однако эти методы оказывались беспомощными при добавлении коммутационной панели, и взломщики были вынуждены конструировать специальные дешифровальные машины. Кабель, помещенный на коммутационную панель, соединяет буквы попарно, например, "E" и "Q" могут быть соединены в пару. Эффект состоит в перестановке этих букв до и после прохождения сигнала через роторы. Например, когда оператор нажимал "E", сигнал направлялся в "Q", и только после этого уже во входной ротор. Одновременно могло использоваться несколько таких пар (до 13).

### **7.5 Аксессуары**

Удобной деталью, использовавшейся на M4 Энигма, был "*Schreibmax*", маленькое печатающее устройство, которое могло печатать все 26 букв на небольшом листе бумаги.

### **7.6 Процедуры использования Энигмы**

Во время второй мировой войны немецкие операторы использовали шифровальную книгу только для установки роторов и настроек колец. Для каждого сообщения, они выбирали случайную стартовую позицию, допустим "WZA", и случайный ключ сообщения, допустим "SXT". Далее оператор устанавливал роторы в стартовую позицию "WZA", и шифровал ключ сообщения "SXT". Предположим, что в результате шифрования ключа получится "UHL". Далее оператор ставил ключ сообщения "SXT", как начальную позицию роторов, и шифровал сообщение. Затем оператор отправлял стартовую позицию "WZA" и зашифрованный ключ "UHL" вместе с сообщением. Получатель устанавливал стартовую позицию в соответствии с первой трехграммой "WZA" и, расшифровывая вторую триграмму "UHL" Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем, распознавал исходный ключ "SXT". Далее, получатель использовал этот ключ как стартовую позицию для расшифровки сообщения. Обычно срок действия ключей составлял один день.

Военная версия Энигмы использовала только 26 букв. Прочие символы заменялись редкими комбинациями букв. Пробел пропускался либо заменялся "X". Символ "X" также использовался для обозначения точки либо конца сообщения.

Некоторые особые символы использовались в отдельных вооруженных частях, например, *Wehrmacht* заменяла запятую двумя символами “ZZ” и вопросительный знак – “FRAGE” либо “FRAQ”. А *Kriegsmarine* заменяла запятую – “Y” и вопросительный знак – “UD”. Два, три или четыре нуля заменялись CENTA, MILLE и MYRIA соответственно.

При выполнении лабораторной работы для исследования шифра Энигмы используется программа-эмулятор **Enigma3S**.

## 8. Задания

1. Запустите эмулятор Энигмы **Enigma3S** из папки, указанной преподавателем. Ознакомьтесь с файлом справки: опция меню Help=>Help.
2. В меню программы выберите пункт Settings => Reset,
3. Установите значения для колец 01 01 01 путем выбора пункта меню View=>Open Cover. В меню Settings=>Inner Settings установите следующие значения Reflector – B, Left – I, Middle – II, Right – III, Ringstellung – A-A-A (Будем считать данное положение начальным), рис.3.10, 3.11.

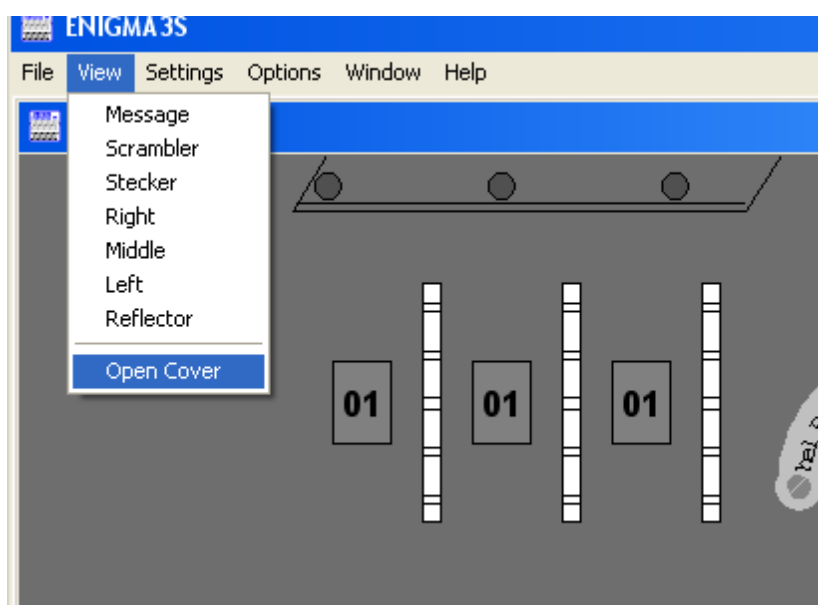


Рис. 3.10. Просмотр начальных установок

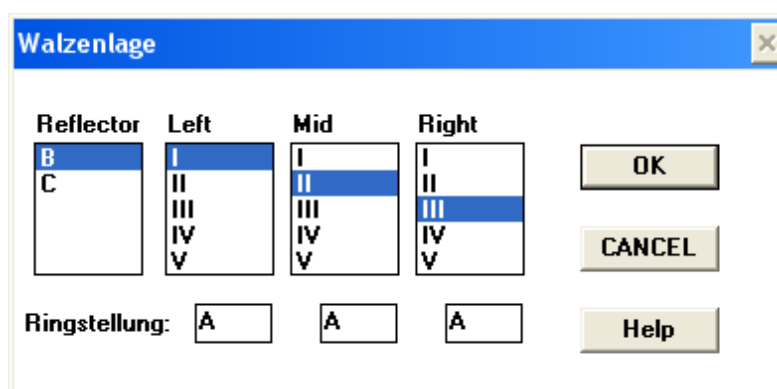


Рис. 3.11. Установки Reflector, Left, Mid, Right

4. Введите на клавиатуре Энигмы сообщение “SECRET MESSAGE”. Какое сообщение получено на выходе?
5. Повторите пункт 3, изменив настройки Ringstellung – A-A-A на Ringstellung – A-B-C
6. Введите на клавиатуре Энигмы сообщение “SECRET MESSAGE”. Какое

сообщение получено на выходе? Насколько оно отличается от сообщения, полученного в пункте 4?

7. Сохраните полученный в пункте 6 шифротекст при помощи опции меню File=>Save CT as

8. Создайте в корне папки с программой эмулятором файл с расширением .pln, откройте его для редактирования в блокноте и запишите в него открытый текст для шифрования.

9. В меню программы выберите опцию File=>Open Pt и выберите файл, созданный в пункте 9. Получите шифротекст из открытого текста, выбрав опцию меню Options=>Encipher Text.

10. Установите эмулятор в начальное положение. В меню программы выберите пункт Window=> Scrambler. Введите при помощи клавиатуры произвольное сообщение из 22 символов (варианты указаны в *таблице 3.1*), обращая внимание на положение колец. Введите последовательность из 22 символов еще раз. Как изменилось положение колец? Отличается ли новая зашифрованная последовательность от начальной? Почему изменилась выходная последовательность?

11. Используя окно Scrambler проследите за тем как изменяется шифротекст в зависимости от настройки положения контактных колес. Что дает возможность настройки порядка следования контактных колес?

12. В окне программы выберите опцию View=>Right, рис. 3.13.

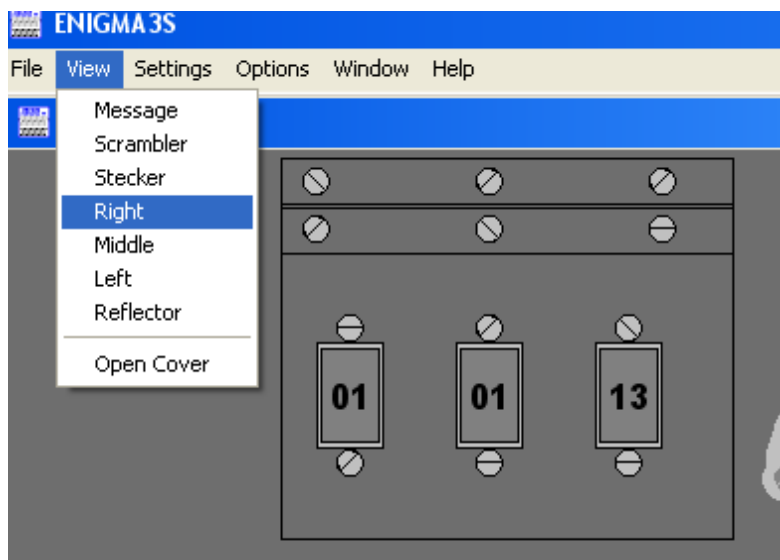


Рис. 3.13. Просмотр установок для выполнения задания

Заполните таблицу соответствия для 5-ти букв (варианты указаны в *таблице 3.1*) для 12-ти первых угловых положений правого колеса.

Таблица 3.1

| Буквы<br>на<br>входе | Угловые положения колеса |   |   |   |   |   |   |   |   |    |    |    |
|----------------------|--------------------------|---|---|---|---|---|---|---|---|----|----|----|
|                      | 1                        | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|                      |                          |   |   |   |   |   |   |   |   |    |    |    |
|                      |                          |   |   |   |   |   |   |   |   |    |    |    |
|                      |                          |   |   |   |   |   |   |   |   |    |    |    |
|                      |                          |   |   |   |   |   |   |   |   |    |    |    |
|                      |                          |   |   |   |   |   |   |   |   |    |    |    |

13. Зная, что эмулятор установлен в начальное положение расшифруйте текст в

соответствии с номером варианта, указанным преподавателем (варианты контрольных заданий указаны в *таблицах 3.2, 3.3, 3.4*).

Таблица 3.2

| Номера вариантов   | Исходный алфавит            |
|--------------------|-----------------------------|
| 1,5,9,13,17        | QRTYU FBNAK GHERL ADLKE DS  |
| 2,6,10,14,18,22    | UIERT PAEVC DSNCY OPLKD BV  |
| 3,7,11,15,19,23,27 | UIFGH KLBVQ FDIIT QKJLS DB  |
| 4,8,12,16,20,24,28 | LLWER TYYWV BAFDP WRTOPF JK |
| 21,25,29,26,30     | OPJHG JFDPJ GFDSK LDFHU BX  |

Таблица 3.3

| Номера вариантов   | Шифротекст |
|--------------------|------------|
| 1,5,9,13,17        | ABCDE      |
| 2,6,10,14,18,22    | FGHIJK     |
| 3,7,11,15,19,23,27 | LMNOP      |
| 4,8,12,16,20,24,28 | QRSTU      |
| 21,25,29,26,30     | VWXYZ      |

Таблица 3.4

| Номера вариантов   | Шифротекст          |
|--------------------|---------------------|
| 1,5,9,13,17        | FQGAH WABUN NL      |
| 2,6,10,14,18,22    | QIKOL RCRJS EGBSS X |
| 3,7,11,15,19,23,27 | OOKWE PRFMI M       |
| 4,8,12,16,20,24,28 | KIXDI ACTHI L       |
| 21,25,29,26,30     | XLXOO EABUN NL      |

## 9. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы.

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## 10. Контрольные вопросы

1. Чем отличается “псевдооткрытый” текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста? В чем преимущества и недостатки одноалфавитных методов?
2. Как зависит время вскрытия шифра описанным выше способом подбора
3. ключей от длины “вероятного” слова?
4. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?

5. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

#### **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К.Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л.Добрушина и О.Б.Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 4. Реализация политики безопасности Белла-ЛаПадула

### 1. Цель работы

Ознакомление с принципами шифрования, используемыми в алгоритме симметричного шифрования AES RIJNDAEL.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

## 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы «RijndaelDemo.exe».

## 7. Описание лабораторной работы

### 7.1 Состояние, ключ шифрования и число циклов

Rijndael представляет собой итеративный блочный шифр, имеющий переменную длину блоков и различные длины ключей. Длина ключа и длина блока могут быть независимо друг от друга 128, 192 или 256 бит.

Разнообразные преобразования работают с промежуточным результатом, называемым Состоянием (State).

Состояние можно представить в виде прямоугольного массива байтов.

Этот массив имеет 4 строки, а число столбцов обозначено как Nb и равно длине блока, деленной на 32.

Ключ шифрования также представлен в виде прямоугольного массива с четырьмя строками. Число столбцов обозначено как Nk и равно длине ключа, деленной на 32. Это показано на рис.4.1.

В некоторых случаях ключ шифрования показан как линейный массив четырехбайтовых слов. Слова состоят из 4-х байтов, которые находятся в одном столбце (при представлении в виде прямоугольного массива).

|           |           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|-----------|
| $a_{0,0}$ | $a_{0,1}$ | $a_{0,2}$ | $a_{0,3}$ | $a_{0,4}$ | $a_{0,5}$ |
| $a_{1,0}$ | $a_{1,1}$ | $a_{1,2}$ | $a_{1,3}$ | $a_{1,4}$ | $a_{1,5}$ |
| $a_{2,0}$ | $a_{2,1}$ | $a_{2,2}$ | $a_{2,3}$ | $a_{2,4}$ | $a_{2,5}$ |
| $a_{3,0}$ | $a_{3,1}$ | $a_{3,2}$ | $a_{3,3}$ | $a_{3,4}$ | $a_{3,5}$ |

|           |           |           |           |
|-----------|-----------|-----------|-----------|
| $k_{0,0}$ | $k_{0,1}$ | $k_{0,2}$ | $k_{0,3}$ |
| $k_{1,0}$ | $k_{1,1}$ | $k_{1,2}$ | $k_{1,3}$ |
| $k_{2,0}$ | $k_{2,1}$ | $k_{2,2}$ | $k_{2,3}$ |
| $k_{3,0}$ | $k_{3,1}$ | $k_{3,2}$ | $k_{3,3}$ |

Рис 4. 1. Пример представления Состояния (Nb=6) и Ключа шифрования (Nk=4)

Входные данные для шифра обозначаются как байты состояния в порядке  $a_{0,0}$ ,  $a_{1,0}$ ,  $a_{2,0}$ ,  $a_{3,0}$ ,  $a_{0,1}$ ,  $a_{1,1}$ ,  $a_{2,1}$ ,  $a_{3,1}$  ... После завершения действия шифра выходные данные получаются из байтов состояния в том же порядке.

Число циклов обозначено как Nr и зависит от значений Nb и Nk.

Таблица 4.1. Число циклов (Nr) как функция от длины ключа и длины блока

| Nr     | Nb = 4 | Nb = 6 | Nb = 8 |
|--------|--------|--------|--------|
| Nk = 4 | 10     | 12     | 14     |
| Nk = 6 | 12     | 12     | 14     |
| Nk = 8 | 14     | 14     | 14     |

### 7.2 Цикловое преобразование

Цикловое преобразование состоит из четырех различных преобразований.

На псевдо-Си это выглядит следующим образом:

```

Round (State, RoundKey)
{
    ByteSub(State); // замена байт ShiftRow(State); // сдвиг строк MixColumn(State); //
    замешивание столбцов
    AddRoundKey(State, RoundKey); // добавление циклового ключа
}
Последний цикл шифра немного отличается: FinalRound(State, RoundKey)
{
    ByteSub(State); // замена байт ShiftRow(State); // сдвиг строк
    AddRoundKey(State, RoundKey); // добавление циклового ключа
}

```

Как можно заметить, последний цикл отличается от простого цикла только отсутствием замешивания столбцов. Каждое из приведенных преобразований подробно рассмотрено далее.

### 7.3 Замена байт (ByteSub)

Преобразование ByteSub представляет собой нелинейную замену байт, выполняемую независимо с каждым байтом состояния.

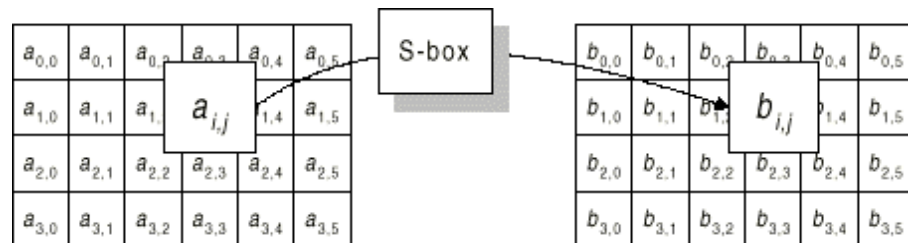


Рис.4. 2. ByteSub действует на каждый байт состояния.

Замена происходит по массиву SboxE при шифровании и по массиву SboxD при расшифровании, причем  $SboxD[SboxE[a]] = a$ .

```

SboxE = {
    0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B,
    0xFE, 0xD7, 0xAB, 0x76,
    0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD, 0xD4, 0xA2,
    0xAF, 0x9C, 0xA4, 0x72, 0xC0, 0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC,
    0x34, 0xA5, 0xE5, 0xF1,
    0x71, 0xD8, 0x31, 0x15,
    0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2,
    0xEB, 0x27, 0xB2, 0x75,
    0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3,
    0x29, 0xE3, 0x2F, 0x84, 0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A,
    0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF, 0xD0, 0xEF, 0xAA, 0xFB, 0x43,
    0x4D, 0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8, 0x51, 0xA3,
    0x40, 0x8F, 0x92, 0x9D, 0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3,
    0xD2, 0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D,
    0x64, 0x5D, 0x19, 0x73, 0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46,
    0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB, 0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06,
    0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79, 0xE7, 0xC8, 0x37,
    0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08,

    0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F,
    0x4B, 0xBD, 0x8B,

```

```

49
0x8A,
0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6, 0x0E, 0x61, 0x35, 0x57, 0xB9,
0x86, 0xC1, 0x1D, 0x9E,
0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9,
0xCE, 0x55, 0x28, 0xDF,
0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F,
0xB0, 0x54, 0xBB, 0x16
};
SboxD = {
0x52, 0x09, 0x6A, 0xD5, 0x30, 0x36, 0xA5, 0x38, 0xBF, 0x40, 0xA3, 0x9E,
0x81, 0xF3, 0xD7, 0xFB,
0x7C, 0xE3, 0x39, 0x82, 0x9B, 0x2F, 0xFF, 0x87, 0x34, 0x8E, 0x43, 0x44,
0xC4, 0xDE, 0xE9, 0xCB,
0x54, 0x7B, 0x94, 0x32, 0xA6, 0xC2, 0x23, 0x3D, 0xEE, 0x4C, 0x95, 0x0B,
0x42, 0xFA, 0xC3, 0x4E,
0x08, 0x2E, 0xA1, 0x66, 0x28, 0xD9, 0x24, 0xB2, 0x76, 0x5B, 0xA2, 0x49,
0x6D, 0x8B, 0xD1, 0x25,
0x72, 0xF8, 0xF6, 0x64, 0x86, 0x68, 0x98, 0x16, 0xD4, 0xA4, 0x5C, 0xCC,
0x5D, 0x65, 0xB6, 0x92,
0x6C, 0x70, 0x48, 0x50, 0xFD, 0xED, 0xB9, 0xDA, 0x5E, 0x15, 0x46, 0x57,
0xA7, 0x8D, 0x9D, 0x84,
0x90, 0xD8, 0xAB, 0x00, 0x8C, 0xBC, 0xD3, 0x0A, 0xF7, 0xE4, 0x58, 0x05,
0xB8, 0xB3, 0x45, 0x06,
0xD0, 0x2C, 0x1E, 0x8F, 0xCA, 0x3F, 0x0F, 0x02, 0xC1, 0xAF, 0xBD, 0x03,
0x01, 0x13, 0x8A, 0x6B,
0x3A, 0x91, 0x11, 0x41, 0x4F, 0x67, 0xDC, 0xEA, 0x97, 0xF2, 0xCF, 0xCE,
0xF0, 0xB4, 0xE6, 0x73, 0x96, 0xAC, 0x74, 0x22, 0xE7, 0xAD, 0x35, 0x85, 0xE2,
0xF9, 0x37, 0xE8,
0x1C, 0x75, 0xDF, 0x6E,
0x47, 0xF1, 0x1A, 0x71, 0x1D, 0x29, 0xC5, 0x89, 0x6F, 0xB7, 0x62, 0x0E,
0xAA, 0x18, 0xBE, 0x1B,
0xFC, 0x56, 0x3E, 0x4B, 0xC6, 0xD2, 0x79, 0x20, 0x9A, 0xDB, 0xC0, 0xFE,
0x78, 0xCD, 0x5A, 0xF4,
0x1F, 0xDD, 0xA8, 0x33, 0x88, 0x07, 0xC7, 0x31, 0xB1, 0x12, 0x10, 0x59,
0x27, 0x80, 0xEC, 0x5F,
0x60, 0x51, 0x7F, 0xA9, 0x19, 0xB5, 0x4A, 0x0D, 0x2D, 0xE5, 0x7A, 0x9F,
0x93, 0xC9, 0x9C, 0xEF,
0xA0, 0xE0, 0x3B, 0x4D, 0xAE, 0x2A, 0xF5, 0xB0, 0xC8, 0xEB, 0xBB,
0x3C, 0x83, 0x53, 0x99, 0x61,
0x17, 0x2B, 0x04, 0x7E, 0xBA, 0x77, 0xD6, 0x26, 0xE1, 0x69, 0x14, 0x63,
0x55, 0x21, 0x0C, 0x7D
};

```

#### 7.4 Преобразование сдвига строк (ShiftRow)

Последние три строки состояния циклически сдвигаются на различное число байт. Строка 1 сдвигается на C1 байт, строка 2 - на C2 байт и строка 3 - на C3 байт. Значения сдвигов C1, C2 и C3 зависят от длины блока Nb. Их величины приведены в таблице 4.2.

Таблица 4.2. Величина сдвига для разной длины блоков

| № | C1 | C2 | C3 |
|---|----|----|----|
| 4 | 1  | 2  | 3  |
| 6 | 1  | 2  | 3  |
| 8 | 1  | 3  | 4  |

Операция сдвига последних трех строк состояния на определенную величину обозначена как ShiftRow(State).

#### Преобразование замешивания столбцов (MixColumn)

Преобразование представляет собой умножение состояния на матрицу ME при шифровании или матрицу MD при расшифровании:

ME  $\otimes$  State

MD  $\otimes$  State

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix} \otimes \begin{vmatrix} b1 & b5 & b9 & b13 \\ b2 & b6 & b10 & b14 \\ b3 & b7 & b11 & b15 \\ b4 & b8 & b12 & b16 \end{vmatrix}$$

$$b1 = (b1 * 2) \text{ XOR } (b2 * 3) \text{ XOR } (b3 * 1) \text{ XOR } (b4 * 1)$$

Умножение двух байт происходит по следующему алгоритму:

- если один из байт равен 0, результатом будет 0;
- если один из байт равен 1, результатом будет другой байт;
- в остальных случаях происходит замена каждого байта по таблице L, заменённые байты складываются, при необходимости вычитается 255 для попадания в интервал [0, 255] и происходит замена по таблице E, что и даёт результат.

L = {0x00, 0x19, 0x01, 0x32, 0x02, 0x1A, 0xC6, 0x4B, 0xC7, 0x1B, 0x68, 0x33, 0xEE, 0xDF, 0x03, 0x64, 0x04, 0xE0, 0x0E, 0x34, 0x8D, 0x81, 0xEF, 0x4C, 0x71, 0x08, 0xC8, 0xF8, 0x69, 0x1C, 0xC1, 0x7D, 0xC2, 0x1D, 0xB5, 0xF9, 0xB9, 0x27, 0x6A, 0x4D, 0xE4, 0xA6, 0x72, 0x9A, 0xC9, 0x09, 0x78, 0x65, 0x2F, 0x8A, 0x05, 0x21, 0x0F, 0xE1, 0x24, 0x12, 0xF0, 0x82, 0x45, 0x35, 0x93, 0xDA, 0x8E, 0x96, 0x8F, 0xDB, 0xBD, 0x36, 0xD0, 0xCE, 0x94, 0x13, 0x5C, 0xD2, 0xF1, 0x40, 0x46, 0x83, 0x38, 0x66, 0xDD, 0xFD, 0x30, 0xBF, 0x06, 0x8B, 0x62, 0xB3, 0x25, 0xE2, 0x98, 0x22, 0x88, 0x91, 0x10, 0x7E, 0x6E, 0x48, 0xC3, 0xA3, 0xB6, 0x1E, 0x42, 0x3A, 0x6B, 0x28, 0x54, 0xFA, 0x85, 0x3D, 0xBA, 0x2B, 0x79, 0x0A, 0x15, 0x9B, 0x9F, 0x5E, 0xCA, 0x4E, 0xD4, 0xAC, 0xE5, 0xF3, 0x73, 0xA7, 0x57, 0xAF, 0x58, 0xA8, 0x50, 0xF4, 0xEA, 0xD6, 0x74, 0x4F, 0xAE, 0xE9, 0xD5, 0xE7, 0xE6, 0xAD, 0xE8, 0x2C, 0xD7, 0x75, 0x7A, 0xEB, 0x16, 0x0B, 0xF5, 0x59, 0xCB, 0x5F, 0xB0, 0x9C, 0xA9, 0x51, 0xA0, 0x7F, 0x0C, 0xF6, 0x6F, 0x17, 0xC4, 0x49, 0xEC, 0xD8, 0x43, 0x1F, 0x2D, 0xA4, 0x76, 0x7B, 0xB7, 0xCC, 0xBB, 0x3E, 0x5A, 0xFB, 0x60, 0xB1, 0x86, 0x3B, 0x52, 0xA1, 0x6C, 0xAA, 0x55, 0x29, 0x9D, 0x97, 0xB2, 0x87, 0x90, 0x61, 0xBE, 0xDC, 0xFC, 0xBC, 0x95, 0xCF, 0xCD, 0x37, 0x3F, 0x5B, 0xD1, 0x53, 0x39, 0x84, 0x3C, 0x41, 0xA2, 0x6D, 0x47, 0x14, 0x2A, 0x9E, 0x5D, 0x56, 0xF2, 0xD3, 0xAB, 0x44, 0x11, 0x92, 0xD9, 0x23, 0x20, 0x2E, 0x89, 0xB4, 0x7C, 0xB8, 0x26, 0x77, 0x99, 0xE3, 0xA5, 0x67, 0x4A, 0xED, 0xDE, 0xC5, 0x31, 0xFE, 0x18, 0x0D, 0x63, 0x8C, 0x80, 0xC0, 0xF7, 0x70, 0x07};

E = {0x01, 0x03, 0x05, 0x0F, 0x11, 0x33, 0x55, 0xFF, 0x1A, 0x2E, 0x72, 0x96, 0xA1, 0xF8, 0x13, 0x35, 0x5F, 0xE1, 0x38, 0x48, 0xD8, 0x73, 0x95, 0xA4, 0xF7, 0x02, 0x06, 0x0A, 0x1E, 0x22, 0x66, 0xAA, 0xE5, 0x34, 0x5C, 0xE4, 0x37, 0x59, 0xEB, 0x26, 0x6A, 0xBE, 0xD9, 0x70, 0x90, 0xAB, 0xE6, 0x31, 0x53, 0xF5, 0x04, 0x0C, 0x14, 0x3C, 0x44, 0xCC,

0x4F, 0xD1, 0x68, 0xB8, 0xD3, 0x6E, 0xB2, 0xCD, 0x4C, 0xD4, 0x67, 0xA9, 0xE0, 0x3B, 0x4D, 0xD7, 0x62, 0xA6, 0xF1, 0x08, 0x18, 0x28, 0x78, 0x88, 0x83, 0x9E, 0xB9, 0xD0, 0x6B, 0xBD, 0xDC, 0x7F, 0x81, 0x98, 0xB3, 0xCE, 0x49, 0xDB, 0x76, 0x9A, 0xB5, 0xC4, 0x57, 0xF9, 0x10, 0x30, 0x50, 0xF0, 0x0B, 0x1D, 0x27, 0x69, 0xBB, 0xD6, 0x61, 0xA3, 0xFE, 0x19, 0x2B, 0x7D, 0x87, 0x92, 0xAD, 0xEC, 0x2F, 0x71, 0x93, 0xAE, 0xE9, 0x20, 0x60, 0xA0, 0xFB, 0x16, 0x3A, 0x4E, 0xD2, 0x6D, 0xB7, 0xC2, 0x5D, 0xE7, 0x32, 0x56, 0xFA, 0x15, 0x3F, 0x41, 0xC3, 0x5E, 0xE2, 0x3D, 0x47, 0xC9, 0x40, 0xC0, 0x5B, 0xED, 0x2C, 0x74, 0x9C, 0xBF, 0xDA, 0x75, 0x9F, 0xBA, 0xD5, 0x64, 0xAC, 0xEF, 0x2A, 0x7E, 0x82, 0x9D, 0xBC, 0xDF, 0x7A, 0x8E, 0x89, 0x80, 0x9B, 0xB6, 0xC1, 0x58, 0xE8, 0x23, 0x65, 0xAF, 0xEA, 0x25, 0x6F, 0xB1, 0xC8, 0x43, 0xC5, 0x54, 0xFC, 0x1F, 0x21, 0x63, 0xA5, 0xF4, 0x07, 0x09, 0x1B, 0x2D, 0x77, 0x99, 0xB0, 0xCB, 0x46, 0xCA, 0x45, 0xCF, 0x4A, 0xDE, 0x79, 0x8B, 0x86, 0x91, 0xA8, 0xE3, 0x3E, 0x42, 0xC6, 0x51, 0xF3, 0x0E, 0x12, 0x36, 0x5A, 0xEE, 0x29, 0x7B, 0x8D, 0x8C, 0x8F, 0x8A, 0x85, 0x94, 0xA7, 0xF2, 0x0D, 0x17, 0x39, 0x4B, 0xDD, 0x7C, 0x84, 0x97, 0xA2, 0xFD, 0x1C, 0x24, 0x6C, 0xB4, 0xC7, 0x52, 0xF6, 0x01}; 52

### 7.5 Добавление циклового ключа

В данной операции цикловой ключ добавляется к состоянию посредством простого EXOR. Цикловой ключ вырабатывается из ключа шифрования посредством алгоритма выработки ключей (key schedule). Длина циклового ключа равна длине блока Nb.

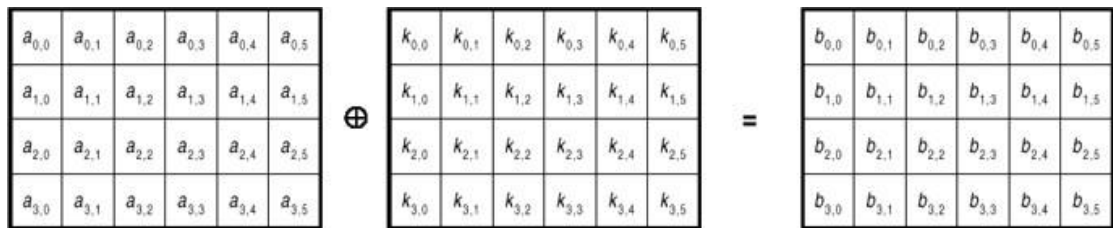


Рис. 4. 5. При добавлении ключа цикловой ключ складывается посредством EXOR с состоянием

При шифровании части расширенного ключа выбираются от начала к концу, при расшифровании – от конца к началу.

### 7.6 Расширение ключа (Key Expansion)

Расширенный ключ представляет собой линейный массив 4-х байтовых слов и обозначен как  $W[Nb*(Nr+1)]$ . Первые  $Nk$  слов содержат ключ шифрования. Все остальные слова определяются рекурсивно из слов с меньшими индексами. Алгоритм выработки ключей зависит от величины  $Nk$ : ниже приведена версия для  $Nk$  равного или меньшего 6 и версия для  $Nk$  большего 6.

Для  $Nk < 6$  или  $Nk = 6$  мы имеем:

```

KeyExpansion(CipherKey, W)
{
  for (i = 0; i < Nk; i++) W[i] = CipherKey[i]; for (j = Nk; j < Nb*(Nk+1); j+=Nk)
  {
    W[j] = W[j-Nk] ^ SubByte( Rotl( W[j-1] ) ) ^ Rcon[j/Nk]; for (i = 1; i < Nk && i+j <
Nb*(Nr+1); i++)
    W[i+j] = W[i+j-Nk] ^ W[i+j-1];
  }
}

```

Как можно заметить, первые  $Nk$  слов заполняются ключом шифрования. Каждое

последующее слово  $W[i]$  получается посредством EXOR предыдущего слова  $W[i-1]$  и слова на  $N_k$  позиций ранее  $W[i-N_k]$ . Для слов, позиция которых кратна  $N_k$ , перед EXOR применяется преобразование к  $W[i-1]$ , а затем еще прибавляется цикловая константа. Преобразование содержит циклический сдвиг байтов в слове, обозначенный как Rotl, затем следует SubByte - применение замены байт.

Для  $N_k > 6$  мы имеем:

```
KeyExpansion(CipherKey,W)
{
  for (i=0; i<Nk; i++) W[i]=CipherKey[i]; for (j=Nk; j<Nb*(Nk+1); j+=Nk)
  {
    W[j] = W[j-Nk] ^ SubByte(Rotl(W[j-1])) ^ Rcon[j/Nk];
    for (i=1; i<4; i++) W[i+j] = W[i+j-Nk] ^ W[i+j-1];
    W[j+4] = W[j+4-Nk] ^ SubByte(W[j+3]);
    for (i=5; i<Nk; i++) W[i+j] = W[i+j-Nk] ^ W[i+j-1];
  }
}
```

Отличие для схемы при  $N_k > 6$  состоит в применении SubByte для каждого 4-го байта из  $N_k$ .

Цикловая константа независит от  $N_k$  и определяется следующим образом:

$Rcon[i] = ( RC[i], '00', '00', '00' )$ , где  $RC[0]='01'$   
 $RC[i]=xtime(Rcon[i-1])$

## 7.7 Шифрование

Шифр Rijndael включает следующие преобразования:

- начальное добавление циклового ключа;
- $N_r-1$  циклов;
- заключительный цикл.

На псевдо-Си это выглядит следующим образом:

```
Rijndael (State, CipherKey)
{
  KeyExpansion(CipherKey, ExpandedKey); // Расширение ключа
  AddRoundKey(State, ExpandedKey); // Добавление циклового ключа
  For ( i=1 ; i<Nr ; i++) Round(State,ExpandedKey+Nb*i); // циклы
  FinalRound(State, ExpandedKey+Nb*Nr); // заключительный цикл
}
```

Если предварительно выполнена процедура расширения ключа, то процедура будет выглядеть следующим образом:

```
Rijndael (State, CipherKey)
{
  AddRoundKey(State, ExpandedKey);
  For ( i=1 ; i<Nr ; i++) Round(State,ExpandedKey+Nb*i); FinalRound(State,
ExpandedKey+Nb*Nr);
}
```

## 7.8 Описание демонстрационной программы

Программа выполнена на языке C# и состоит из двух элементов – файла Rijndael.dll, содержащего реализацию алгоритма шифрования, и демонстрационного приложения RijndaelDemo.exe. Для работы приложения необходима ОС Windows с установленным .NET Framework v1.1.

В основном окне демонстрационной программы задаются длина ключа, длина блока, можно посмотреть расширенный ключ шифрования, вычисляемый в соответствии с заданным ключом шифрования.

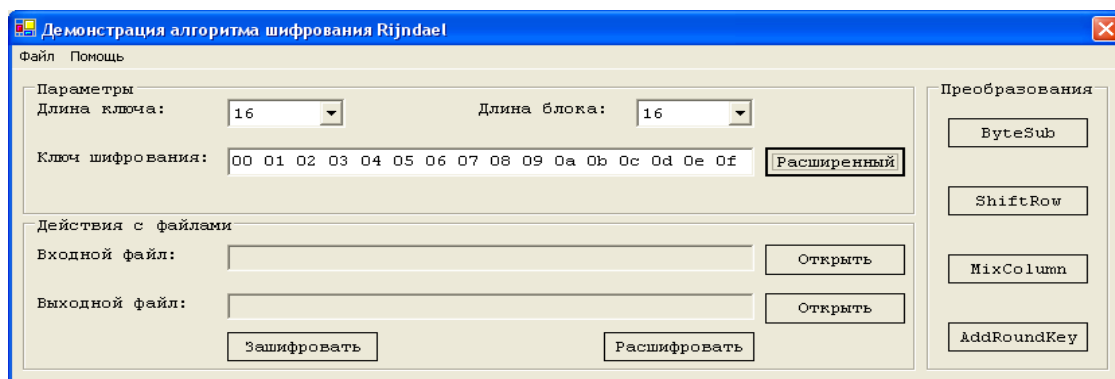


Рис. 4.6. Главное окно демонстрационной программы

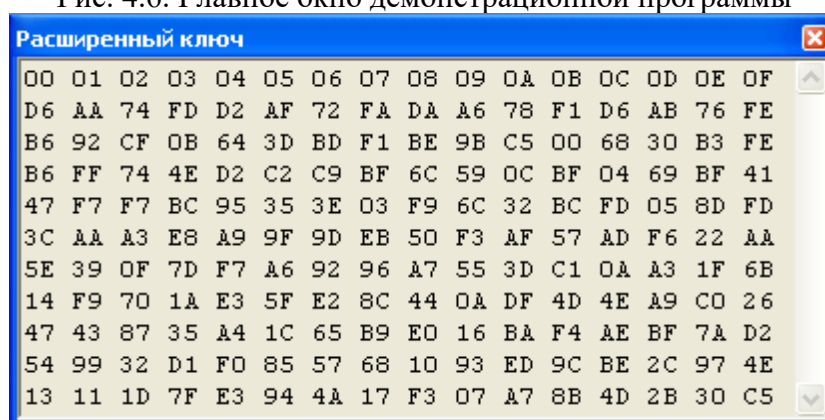


Рис. 4.7. Окно расширенного ключа

Также есть возможность подробно рассмотреть действие всех цикловых преобразований (ByteSub, ShiftRow, MixColumn, AddRoundKey) как при шифровании, так и при расшифровании, рис.4.8, 4.9.

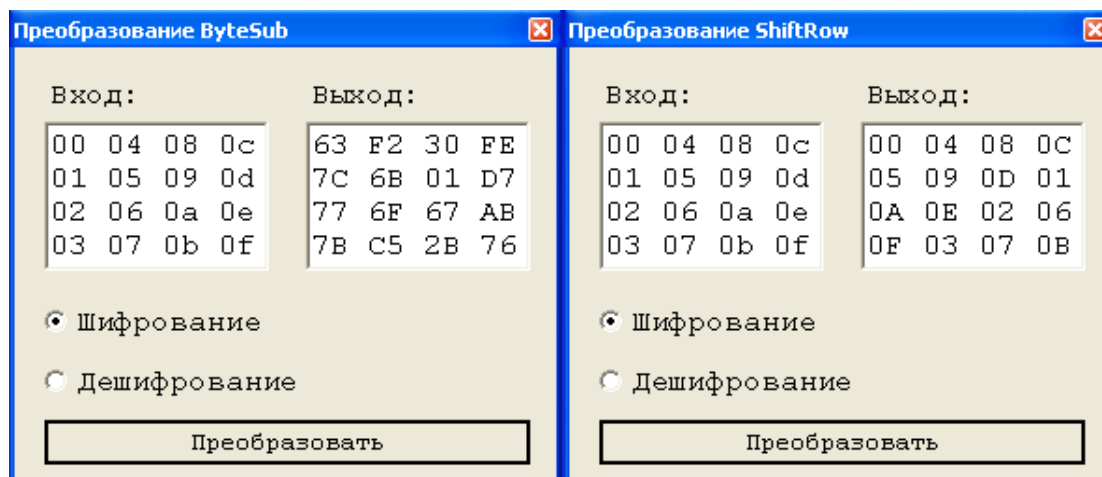


Рис. 4.8. Окна преобразований ByteSub и ShiftRow

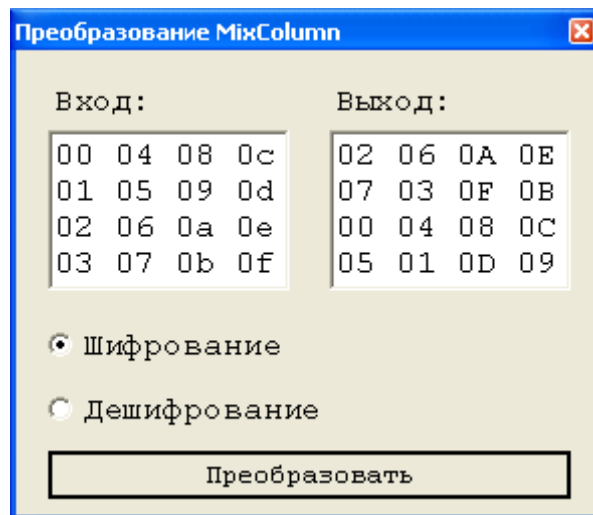


Рис. 4.9. Окна преобразований MixColumn и AddRoundKey

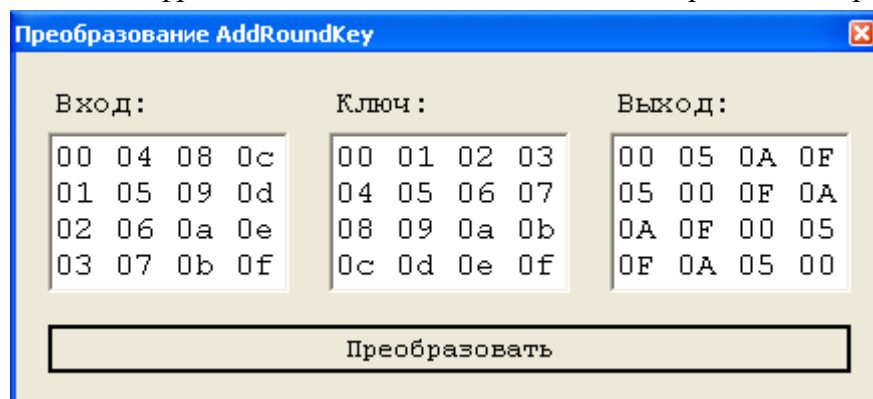
При шифровании предлагается выбрать исходный файл и файл, куда будет помещен результат шифрования, при расшифровании соответственно зашифрованный файл и файл, предназначенный для помещения результата расшифрования. В процессе используются, указанные в главном окне программы, ключ шифрования и длины ключа и блока.

## 8. Задания

1. Ознакомиться со сведениями о программе **RijndaelDemo**, изложенными в разделе 1. Запустить модуль **RijndaelDemo.exe**.
2. Изучить на примере обычных текстовых файлов способы шифрования и расшифрования с помощью алгоритма Rijndael.

Подробно рассмотреть действие всех цикловых преобразований (ByteSub, ShiftRow, MixColumn, AddRoundKey), как при шифровании, так и расшифровании.

Исходный текст для шифрования может быть подготовлен заранее и сохранен в



файле \*.txt.

3. Сохранить в отчете экранные формы, демонстрирующие процесс шифрования и расшифрования информации, проанализировать полученные результаты.
4. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта, указанным преподавателем.

## 9. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ

и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

#### **10. Контрольные вопросы**

1. Сравните основные характеристики алгоритмов Rijndael и ГОСТ 28147-89.
2. Сравните основные характеристики алгоритмов Rijndael и DES.
3. Опишите структуру сети Фейстеля.
4. Приведите обобщенные схемы шифрования данных с помощью алгоритма Rijndael и ГОСТ 28147-89. Дайте их сравнительный анализ.
5. Сравните один раунд шифрования данных с помощью алгоритма Rijndael и ГОСТ 28147-89.
6. Сравните эквивалентность прямого и обратного преобразований в алгоритмах Rijndael и ГОСТ 28147-89.
7. Сравните выработку ключевой информации в алгоритмах Rijndael и ГОСТ 28147-89.
8. Сравните алгоритмы Rijndael и ГОСТ 28147-89 по показателям диффузии.
9. Сравните алгоритмы Rijndael и ГОСТ 28147-89 по показателям стойкости.
10. Сравните алгоритмы Rijndael и ГОСТ 28147-89 по показателям производительности и удобству реализации.

#### **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б. Б., Кречет Т. В., Плохов Е. М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер. с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 5. Реализация ролевой политики безопасности

### 1. Цель работы

Изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

— ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

— Убедиться в целостности электрических розеток и разъемов.

— В лаборатории необходимо быть в сменной обуви.

— Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

— Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

— Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

— При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

— Докладить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## **6. Программное обеспечение**

Программное обеспечение для выполнения лабораторной работы «*L\_PROST.EXE*».

## **7. Описание лабораторной работы**

Для выполнения лабораторной работы необходимо запустить программу *L\_PROST.EXE*. На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения информации об осуществленных программой действиях), в верхней строке окна расположено главное меню, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, “ESC” – выход из основного меню.

Для удобства в программе предусмотрена работа с мышью. В этом случае указатель подводится к нужному пункту главного меню или к нужной кнопке на панели инструментов и нажимается левая клавиша мыши, для отказа достаточно нажать клавишу “ESC”.

Кроме основных функций главного меню (“Генерация простого Р”, “Поиск в интервале”, “Проверка на простоту” и так далее) панель инструментов содержит клавишу, при нажатии которой выводится информация о программе.

### **7.1 Генерация простого Р**

Возможность генерации простого числа; количество разрядов генерируемого числа задается пользователем (от 1 до 5).

### **7.2 Поиск в интервале**

Возможность поиска простых чисел в заданном интервале.

Пользователем задается: начало интервала – значение  $x$ , затем длина интервала – значение  $L$ . Поиск будет осуществляться в интервале  $(x, x+L)$ .

При проверке на простоту каждого числа интервала сначала выполняется тест пробных делений на первые по порядку простые числа, а затем проверка по тесту Ферма. Для задания способов проверки на простоту необходимо левой клавишей мыши отметить флажок рядом с названием нужного метода, а затем указать все необходимые данные для начала поиска.

В методе пробных делений исходные данные – количество первых простых чисел для деления, а в тесте Ферма надо указать количество оснований и их значения.

По окончании расчета на экран выведутся найденные простые числа и их количество. Полную картину результатов работы можно просмотреть в пункте меню “Вывод результатов”.

Возможность проверки на простоту любого числа. Необходимо ввести число и параметры расчета аналогично поиску в интервале.

### **7.3 Вывод результатов**

Возможность просмотра всех результатов последней обработки. При входе в программу, когда никаких расчетов еще не производилось, предоставляется возможность просмотра исходного файла первых простых чисел, используемых для теста пробных делений.

### **7.4 Дополнительные сведения о программе**

1. При запуске утилит генерации простого числа, поиска в интервале и проверки на простоту у пользователя запрашивается подтверждение на правильность выбранного метода для работы.

2. Во время работы длительных по исполнению процедур запускается прогресс процесса и гасится окно текстового редактора. По полоске прогресса можно наблюдать и оценивать примерную скорость работы алгоритма и время окончания текущего процесса.

3. Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся.

4. Описание "горячих клавиш":

Ctrl+F1 - 'Генерация простого P' Ctrl+F2 - 'Поиск в интервале' Ctrl+F3 - 'Проверка на простоту' Ctrl+F4 - 'Вывод результатов' Ctrl+X - 'Выход из программы'

5. В лабораторной работе из-за большого времени счета рекомендуется использовать числа не более пяти разрядов и длину интервала выбирать не более 500, количество оснований для теста Ферма – не более 5.

6. Для правильного функционирования программы, в рабочей директории (вместе с файлом *l\_prost.exe*) обязательно должны находиться файлы *prost.txt* и *work.txt*. Не рекомендуется вносить какие-либо изменения в эти текстовые файлы иначе последствия могут быть непредсказуемые.

## 8. Задания

1. Проверить на простоту два произвольных целых числа, разрядностью не менее 5.

2. Распределение простых чисел.

2.1. Задан интервал вида  $[x, x+L]$ . Вычислить количество  $\Pi(x, L)$  простых чисел в интервале и сравнить с величиной  $L/\ln(x)$ . При каких условиях  $\Pi(x, L)/L$  близко к  $1/\ln(x)$ ?

$x=2000, L=500$ ,

– количество простых чисел для деления: 5-15,

– количество оснований: 1-2.

2.2. Найти в заданном интервале все простые числа. Пусть  $L(i)$  – разность между двумя соседними простыми числами. Построить гистограмму для  $L(i)$ . Вычислить выборочное среднее  $L_{\text{сред.}}$ . Сравнить с величиной  $\ln(x)$ , где  $x$  – середина интервала.

Интервал: (1000, 1000+300):

– количество простых чисел для деления: 5-20,

– количество оснований: 1-3.

2.3. Для заданного набора чисел  $\{k\}$  оценить относительную погрешность формулы для  $k$ -го простого числа:

$p(k)=k/\ln(k), k=\{10, 15, 20, 30, 35\}$ .

3. Методы генерации простых чисел.

3.1. В заданном интервале построить график относительного количества натуральных чисел, проходящих "решето Эратосфена"

(т. е. не делящихся на первые  $k$  простых). Интервал: (500, 500+200).

Расчет производится для всех  $k \leq 10$ .

3.2. Для заданного интервала:

а) рассчитать точное количество  $P_0$  простых чисел в интервале, т.е. при проверке задать только тест на делимость.

Количество первых простых чисел для деления определяется из расчета: максимальное число для деления равно квадратному корню из максимального значения интервала.

б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество  $P_1$  вероятно простых чисел, удовлетворяющих этому тесту.

в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основаниями в тесте Ферма. Вычислить количество  $P_2$  вероятно простых чисел, удовлетворяющих этому тесту.

Интервал:  $(1500, 1500 + 300)$ .

Проанализировать полученные данные.

Известно, что в заданном интервале имеются числа Кармайкла. Найти

Варианты интервалов:  $(1050, 1050 + 100)$ ,  $(1700, 1700 + 100)$ ,  $(2400, 2400 + 100)$

Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2?
2. Какова вероятность  $P(x)$  того, что наугад взятое нечетное очень большое число, не превосходящее  $x$ , окажется простым?
3. Вычислить:  $1812 \pmod{13}$ ,  $127 \pmod{7}$ .
4. Сформулируйте суть теста на простоту с использованием пробных делений.

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 6. Схема Фейстеля. Шифр DES

### 1. Цель работы

Знакомство с основными положениями федеральной целевой программы “Электронная Россия”. Ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

— ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

— Убедиться в целостности электрических розеток и разъемов.

— В лаборатории необходимо быть в сменной обуви.

— Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

— Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

— Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

— При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

— Доложить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

## **5. Аппаратное обеспечение**

Класс персональных ЭВМ, классная доска, мел (маркеры).

## **6. Программное обеспечение**

Программное обеспечение для выполнения лабораторной работы «labWork6.exe».

## **7. Описание лабораторной работы**

### **7.1 Электронная цифровая подпись**

При обмене электронными документами по сети связи существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но при этом возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе.

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является *электронная цифровая подпись (ЭЦП)*.

Первая схема ЭЦП - RSA - была разработана еще в конце 1970-х годов. Однако проблема подтверждения авторства стала актуальной настолько, что потребовалось установление стандарта, только в 1990-х годах, во время взрывного роста глобальной сети Интернет и массового распространения электронной торговли и оказания услуг. Именно по указанной причине стандарты ЭЦП в России и США были приняты практически одновременно, в 1994 году.

Из предложенных криптологами схем ЭЦП наиболее удачными оказались RSA и схема Эль-Гамала. Но первая из них была запатентована в США и ряде других стран (патент на RSA прекратил свое действие совсем недавно). Во второй же схеме существует большое количество ее возможных модификаций, и все их запатентовать весьма затруднительно. Именно по этой причине схема ЭЦП Эль-Гамала осталась по большей части свободной от патентов. Кроме того, эта схема имеет и определенные практические преимущества: размер блоков, которыми оперируют алгоритмы, и соответственно размер ЭЦП в ней оказались значительно меньше, чем в RSA, при той же самой стойкости.

Именно поэтому стандарты ЭЦП России и США базируются на схеме Эль-Гамала.

Законы об ЭЦП сегодня имеют уже более 60-ти государств. В этом списке значится и Россия. Закон «Об электронной цифровой подписи», принятый в 2001 году должен оказать стимулирующее воздействие на развитие отечественной электронной коммерции, особенно если в соответствии с ним будут своевременно приведены иные нормативно-правовые акты.

— Правительство РФ финансово поддерживает осуществление федеральной целевой программы «Электронная Россия».

— Принят закон «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации».

— Еще в январе 2001 г. правление Пенсионного фонда постановлением «О введении в системе Пенсионного фонда РФ криптографической защиты информации и электронной цифровой подписи» регламентировало регистрацию и подключение юридических и физических лиц к системе своего электронного документооборота.

— В 2003 г. вышел приказ МНС России «Об утверждении порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи», благодаря которому сегодня любое физическое или юридическое лицо может связаться с налоговой инспекцией, используя защищенную электронную почту.

— В 2004 г. были утверждены поправки к статьям 13 и 15 закона «О бухгалтерском учете», согласно которым бухгалтерская отчетность предприятия может вестись, храниться и предоставляться в контролирующие органы в электронном виде.

## 7.2 Принцип построения ЭЦП

Асимметрия ролей отправителя и получателя в схемах ЭЦП требует наличия двух тесно связанных ключей: *секретного*, или ключа подписи, и *открытого*, или ключа проверки подписи.

Любая схема ЭЦП обязана определить три следующих алгоритма:

- алгоритм генерации ключевой пары для подписи и ее проверки;
- алгоритм постановки подписи;
- алгоритм проверки подписи.

Стандарты России и США очень похожи, они различаются лишь некоторыми числовыми параметрами и отдельными деталями выработки ключевой пары, вычисления и проверки подписи. Действительно, оба стандарта являются вариантами одной и той же схемы ЭЦП Эль-Гамала.

ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает основными ее достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможность отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.
- ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом, и включает две процедуры:
  - процедуру постановки подписи, в которой используется секретный ключ отправителя сообщения;
  - процедуру проверки подписи, в которой используется открытый ключ отправителя.

### *Процедура постановки подписи*

При формировании ЭЦП, отправитель, прежде всего, вычисляет хэш- функцию  $h(M)$  подписываемого текста  $M$ . Вычисленное значения хэш-функции  $h(M)$  представляет собой один короткий блок информации  $t$ , характеризующий весь текст  $M$  в целом. Затем значение  $t$  шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста  $M$ .

### *Процедура проверки подписи*

При проверке ЭЦП, получатель сообщения снова вычисляет хэш- функцию  $t = h(M)$  принятого по каналу текста  $M$ , после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению  $t$  хэш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа.

Каждая подпись, как правило, содержит следующую информацию:

1. дату подписи;
2. срок окончания действия ключа данной подписи;
3. информацию о лице, подписавшем текст;
4. идентификатор подписавшего (имя открытого ключа);
5. собственно цифровую подпись.

### *Однонаправленные хэш-функции*

Хэш-функция предназначена для сжатия подписываемого документа  $M$  до нескольких десятков или сотен бит. Хэш-функция  $h(.)$  использует в качестве аргумента сообщение  $M$  произвольной длины и возвращает хэш-значение  $h(M)=N$  фиксированной длины. Обычно хэшированная информация является сжатым двоичным представлением

основного сообщения произвольной длины. Следует отметить, что значение хэш-функции  $h(M)$  сложным образом зависит от документа  $M$  и не позволяет восстановить сам документ  $M$ .

Хэш-функция должна удовлетворять целому ряду условий:

6. должна быть чувствительна к всевозможным изменениям в тексте  $M$ ;
7. должна обладать свойством необратимости, т.е. задача подбора документа  $M$ , который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;
8. вероятность того, что значения хэш-функции двух различных документов совпадут, должна быть ничтожно мала.

Большинство хэш-функций строится на основе однонаправленной функции  $f(.)$ , которая образует выходное значение длиной  $n$  при задании двух входных значений длиной  $n$ . Этими входами являются блок исходного текста  $M_i$  и хэш-значение  $H_{i-1}$  предыдущего блока текста, рис.6.1.

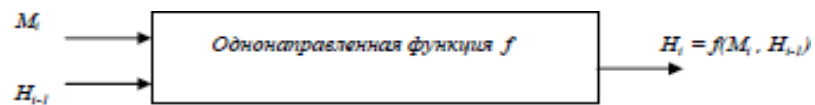


Рис. 6.1. Формирование хэш-функции

### 7.3 Алгоритм цифровой подписи DSA

Алгоритм цифровой подписи DSA (Digital Signature Authorization) предложен в 1991 году в США и является развитием алгоритма цифровой подписи Эль-Гамала.

Отправитель и получатель электронного документа используют при вычислении большие целые числа:

$G, P$  – простые числа по  $L$ -бит каждое ( $L = 512 \dots 1024$  бит);  $q$  – простое число длиной 160 бит делитель числа  $(P - 1)$ .

$G, P, q$  являются открытыми и могут быть общими для всех пользователей сети.

Описание алгоритма

1. Отправитель выбирает случайное целое число  $X$ ,  $1 < X < q$ . Число  $X$  является секретным ключом отправителя для формирования электронной подписи.

2. Отправитель вычисляет значение

$$Y = GX \bmod P.$$

Число  $Y$  является открытым ключом для проверки подписи отправителя и передается всем получателям документа.

3. Для того чтобы подписать документ  $M$ , отправитель хэширует его в целое хэш-значение  $m$ :

$$m = h(M), 1 < m < q.$$

Затем генерирует случайное целое число  $K$ ,  $1 < K < q$  и вычисляет число  $r$ :  $r = (GK \bmod P) \bmod q$ .

4. При помощи секретного ключа  $X$  отправитель вычисляет число  $s$ :

$$s = ((m + rX) / K) \bmod q.$$

Пара чисел  $r, s$  образуют цифровую подпись  $S = (r, s)$  под документом  $M$ .

5. Доставленное получателю сообщение вместе с подписью представляет собой тройку чисел  $[M, r, s]$ . Прежде всего получатель проверяет выполнение соотношений:

$$0 < r < q; 0 < s < q.$$

6. Далее получатель вычисляет значения:

$$w = 1/s \bmod q;$$

$$m = h(M) - \text{хэш-значение}; u1 = (m \cdot w) \bmod q;$$

$$u2 = (rw) \bmod q.$$

Затем при помощи открытого ключа  $Y$  вычисляется значение

$$v = ((Gu1Yu2) \bmod P) \bmod q,$$

и проверяется выполнение равенства  $v = r$ . Если оно выполняется, то подпись признается подлинной, так как можно строго математически доказать, что последнее равенство будет выполняться тогда и только тогда, когда подпись

$S = (r, s)$  под документом  $M$  получена при помощи именно того секретного ключа  $X$ , из которого был получен открытый ключ  $Y$ .

#### 7.4 Новые стандарты ЭЦП

Последние достижения криптографии показали, что общая проблема логарифмирования в дискретных полях, являющаяся базой указанной схемы ЭЦП, не может считаться достаточно прочным фундаментом. Например, размеры блоков, считающиеся "безопасными", растут сравнительно быстрыми темпами. В результате это привело к тому, что стандарты ЭЦП России и США в 2001 году были обновлены: переведены на эллиптические кривые. Схемы ЭЦП при этом остались прежними, но в качестве чисел, которыми они оперируют, теперь используются не элементы конечного поля  $GF(2n)$  или  $GF(p)$ , а эллиптические числа - решения уравнения эллиптических кривых над указанными конечными полями. Роль операции возведения числа в степень в конечном поле в обновленных стандартах выполняет операция взятия кратной точки эллиптической кривой – “умножение” точки на целое число.

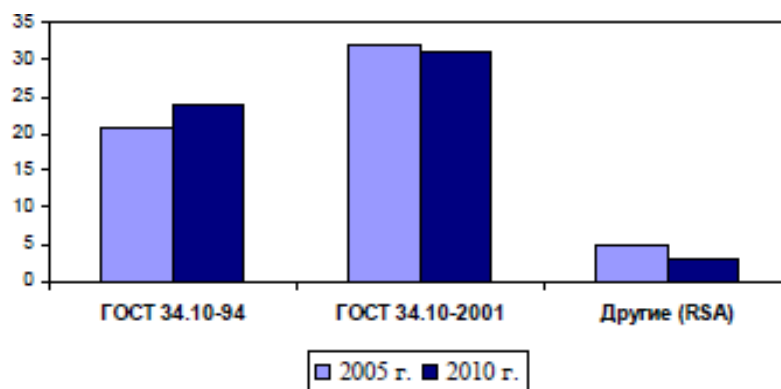


Рис. 6.2. Алгоритмы ЭЦП, используемые в РФ

Надлежащий выбор типа эллиптической кривой позволяет многократно усложнить задачу взлома схемы ЭЦП и уменьшить рабочий размер блоков данных. Старый российский стандарт ЭЦП оперирует 1024-битовыми блоками, а новый, основанный на эллиптических кривых, - 256-битовыми, и при этом обладает большей стойкостью.

Стойкость схемы подписи ГОСТ Р34.10-94 базируется на сложности решения задачи дискретного логарифмирования в простом поле. В настоящее время наиболее быстрым алгоритмом ее решения для общего случая является алгоритм обобщенного решета числового поля.

В ГОСТ Р34.10-2001 стойкость схемы ЭЦП основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой. При правильном выборе параметров кривой самыми эффективными методами ее решения являются более трудоемкие  $r$ - и  $l$ -методы Полларда. Так, по разным оценкам специалистов, трудоемкость взлома старого и нового стандартов ЭЦП России составляет величину порядка 1026 и 1038 операций умножения в базовом поле  $GF(p)$  соответственно. Очевидно, что новый стандарт более стойкий.

#### 8. Задания

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы “Электронная Россия”, а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой, изложенными в параграфе 1.

Запустить программу *labWork6.exe*, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.

2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.

5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.

6. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы. Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭЦП?

2. Перечислите стандарты хэш-функций, действующие в Российской Федерации.

3. Опишите процедуры постановки и проверки ЭЦП.

4. Какая информация содержится в ЭЦП?

5. Перечислите стандарты ЭЦП, действующие в Российской Федерации.

6. На каких принципах основана криптостойкость современных алгоритмов ЭЦП?

7. Приведите пример реализации алгоритма ЭЦП (*RSA*, *El-Gamal*, *DSA*)

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.

2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.

3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.

4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 7. Шифр ГОСТ 28147-89. Шифр Blowfish

### 1. Цель работы

Исследование шифра скользящей перестановки с использованием программной реализации XY-Mover.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы программный модуль XY-Mover.

## 7. Описание лабораторной работы

### 7.1 Устойчивые закономерности открытого текста и их использование при дешифровании шифров простой замены и перестановки

Возможность дешифрования какого-либо шифра в значительной мере зависит от того, в какой степени криптографические преобразования разрушают вероятностно-статистические закономерности, присутствующие в открытом содержательном тексте. Так в осмысленных текстах любого естественного языка различные буквы встречаются с разной частотой, при этом относительные частоты букв в различных текстах одного языка близки между собой. То же самое можно сказать и о частотах пар, троек букв открытого текста. Кроме того, любой естественный язык обладает так называемой избыточностью, что позволяет с большой вероятностью “угадывать” смысл сообщения, даже, если часть букв в сообщении не известна.

Таблица относительных частот букв алфавита русского языка

|    |              |    |           |    |              |
|----|--------------|----|-----------|----|--------------|
| 1  | а - 0,062    | 12 | л - 0,035 | 23 | п - 0,004    |
| 2  | б - 0,014    | 13 | м - 0,026 | 24 | ч - 0,012    |
| 3  | в - 0,038    | 14 | н - 0,053 | 25 | ш - 0,006    |
| 4  | г - 0,013    | 15 | о - 0,090 | 26 | щ - 0,003    |
| 5  | д - 0,025    | 16 | п - 0,023 | 27 | ы - 0,016    |
| 6  | е, е - 0,072 | 17 | р - 0,040 | 28 | ъ, ъ - 0,014 |
| 7  | ж - 0,077    | 18 | с - 0,045 | 29 | э - 0,003    |
| 8  | з - 0,016    | 19 | т - 0,053 | 30 | ю - 0,006    |
| 9  | и - 0,062    | 20 | у - 0,021 | 31 | я - 0,018    |
| 10 | й - 0,010    | 21 | ф - 0,002 | 32 | - 0,175      |
| 11 | к - 0,028    | 22 | х - 0,009 |    |              |

Подобные таблицы приводятся в разных книгах. Они получены на основе подсчетов частот на больших объемах открытого текста. Учитывая, что для экспериментов берется различный исходный материал, значения вероятностей несколько отличаются между собой.

Если упорядочить буквы по убыванию вероятностей, то мы получим следующий вариационный ряд:

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

Например, в слове **СЕНОВАЛИТР** содержатся 10 наиболее часто встречающихся букв.

Частоты знаков алфавита зависят не только от языка, но и от характера текста. Так в тексте по криптографии будет повышена вероятность букв Ф, Ш (из-за часто встречающихся слов “шифр”, “криптография”). В некоторых математических текстах может быть завышена частота буквы Ф (из-за слов “функция”, “функционал” и т.п.). В стандартных текстовых файлах наиболее частым является символ “пробел”. Частотная диаграмма содержательных текстов является устойчивой характеристикой текста. Из теории вероятностей следует, что при достаточно слабых ограничениях на вероятностные свойства случайного процесса справедлив закон больших чисел, т.е. относительные частоты знаков сходятся по вероятности к значениям их вероятностей

$$P\left\{\left|\frac{g_k}{N} - p_k\right| > \varepsilon\right\} \xrightarrow{N \rightarrow \infty} 0.$$

Шифры перестановки и простой замены не полностью разрушают вероятностно-статистические свойства, имеющиеся в открытом сообщении.

При дешифровании текста, зашифрованного шифром простой замены, используют

частотные характеристики открытого текста. Именно, если подсчитать частоты встречаемости знаков в зашифрованном тексте, упорядочить их по убыванию, и сравнить с вариационным рядом вероятностей открытого текста, то эти две последовательности будут близки.

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| п | а | я |   | в |   | и | м |
| о | ч | ш | г |   | у |   | е |
| е | б | ж | л |   | е |   | о |
| м |   | ч |   | о | т | о | я |
|   | е | г | е |   | у | с | ш |
|   | а | к | ь | з | а | т | т |
| я | р | е |   | е | п |   | ь |
|   | ю | з | в | а | н | в |   |
| о | й | а | в | е | ш | л |   |
|   | е | е | я | м |   | п | н |
| ь | р | р | н | з | е | е | е |
| з | а | м | а | н |   | а | к |
| ч | с | т | а |   | ь | а | н |
| о | я | л | м |   | а | л |   |
| о | ь | ч | х | т | а | т |   |
| в |   | е | о | а | л | е | п |
| о | е | р | м | т | ь | е |   |
| д | с | г | ы |   | о | а | т |
| е | б | в | н |   | ы |   |   |
|   | а | у | и | н | з | н | л |
|   | г | и | а | о | к | к | д |
|   | а | о | б | д | г | н |   |
|   | ж | а | у | е | д | я | д |
| х | л | и |   | е | м | о | а |
| к | р | т | д |   | ь | о | е |
|   | ь | х | в | т | о | н |   |
| р | л | е |   | е | д | а | ю |
| р |   | з | е | в |   | е | д |
| ш |   | в | а | е | н | е | н |
| т | и | й | е | в |   |   | д |
|   |   | в |   | с | д |   |   |

Скорее всего на первом месте окажется пробел, далее будут следовать буквы О, Е, А, И.

Конечно, если текст не очень длинный, то не обязательно полное совпадение. Может оказаться на втором месте О, а на третьем Е, но в любом случае в первых и вторых рядах одинаковые буквы будут располагаться недалеко друг от друга, и чем ближе к началу (чем больше вероятность знаков), тем меньше будет расстояние между знаками.

Аналогичная картина наблюдается и для пар соседних букв (биграмм) открытого текста (наиболее частая биграмма русского открытого текста - СТ). Однако для получения устойчивой картины длина анализируемой последовательности должна быть достаточно большой. На сравнительно небольших отрезках открытого текста эта картина как-то смазана. Более устойчивой характеристикой биграмм является отсутствие в осмысленном тексте некоторых биграмм, как говорят, наличие запретных биграмм, имеющих вероятность равную практически 0.

Видели ли вы когда-нибудь в открытом тексте биграмму ЪЪ, или биграммы вида: “гласная” Ъ; “пробел” Ъ? Знание и использование указанных особенностей открытого текста значительно облегчает дешифрование шифра перестановки и замены.

**Шифр перестановки.** Положим  $X$  – множество открытых (содержательных) текстов в алфавите  $I$ . Длины всех возможных открытых текстов кратны величине  $T$ . Множеством ключей является симметрическая группа подстановок  $ST$  степени  $T$ , для  $g \in ST$  определим функцию шифрования  $fg$  положив для  $(i_1, i_2, \dots, i_T) \in X$

$$fg(i_1, i_2, \dots, i_T) = (ig(1), ig(2), \dots, ig(T));$$

доопределим  $fg$  на остальных элементах из  $X$  по правилу: текст  $x \in X$  делится на отрезки длины  $T$  и каждый отрезок длины  $T$  шифруется на ключе  $g$  по указанному выше закону шифрования. Последовательность, составленная из букв образов зашифрованных слов, является зашифрованным текстом, соответствующим открытому тексту  $x$  и ключу  $g$ .

Для шифрования текста длины не кратной  $T$  его дополняют буквами до длины кратной  $T$ .

**Дешифрование шифра перестановки.** Шифрованный текст записывается в таблицу с  $T$  столбцами. Для восстановления открытого текста шифра перестановки нам необходимо переставить колонки таким образом, чтобы в строках появился осмысленный текст.

Рассмотрим пример дешифрования шифра перестановки восьми столбцов (Учебное пособие «Принципы и методы защиты информации» Проскурин Г.В.). Пусть шифротекст имеет следующий вид:

Сопоставим перестановке столбцов таблицу  $8 \times 8$ , при этом поставим на пересечении  $i$ -той строки и  $j$ -ого столбца единицу, если  $j$ -ая колонка после обратной перестановки должна следовать за  $i$ -ой. Наша задача восстановить таблицу, отвечающую правильной перестановке столбцов.

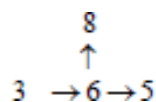
Давайте теперь попарно пристраивать один столбец к другому. Если при этом в некоторых строках появляются запретные биграммы, то столбцы не могут в открытом тексте следовать друг за другом, и соответствующая клеточка зачеркиваются. В нашем примере 6-ой столбец не может следовать за 4-ым, т.к. иначе в тексте в первой строке будет подряд два пробела. Посмотрим, например, 6-ую строку. Если бы 4-ый столбец следовал за 1-ым, то в тексте были бы слова, начинающиеся с Ъ.

После просмотра всех строк мы получим следующую таблицу:

|   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | x | x |   | x | x | x |   | x |
| 2 |   | x |   | x |   | x |   |   |
| 3 |   |   | x |   |   |   |   | x |
| 4 | x | x |   | x |   | x | x | x |
| 5 | x |   |   |   | x | x | x | x |
| 6 | x | x |   | x |   | x | x |   |
| 7 | x |   |   | x | x | x | x | x |
| 8 | x | x |   |   | x | x | x | x |

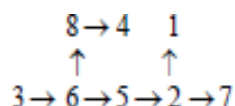
Если бы текст был подлиннее и строк было бы побольше, то в каждой строке и в каждом столбце осталось бы ровно по одной не зачеркнутой клеточке и перестановка была бы восстановлена.

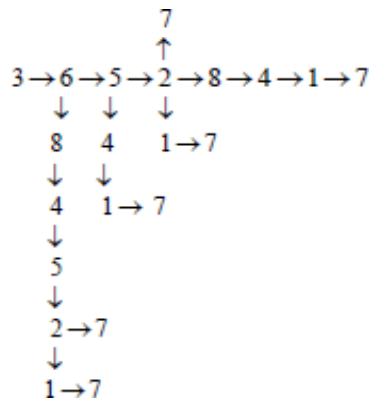
В нашей таблице мы только можем утверждать, что 6-ой столбец следует за 3-им (обозначим это событие следующим образом 3 6), если 6-ой столбец не является последним. Для 6-го столбца может быть два варианта продолжения



Нам надо рассмотреть оба и постараться отсеять ложный вариант. Если отсеять ложный вариант не удастся, то надо продолжать оба варианта

В итоге получаем некоторое дерево возможного следования столбцов в открытом тексте.





Каждой ветви дерева соответствует некоторая перестановка столбцов. Далее проверяем каждый вариант на осмысленность и получаем правильный вариант.

3 → 6 → 5 → 2 → 8 → 4 → 1 → 7

Заметим, что не обязательно было строить дерево до конца. Например, ветвь можно было отсечь сразу. Разве можно признать осмысленным следующий фрагмент текста.

|   |   |   |   |   |
|---|---|---|---|---|
| 3 | 6 | 8 | 4 | 5 |
| я |   | м |   | в |
| ш | у | е | г |   |
| ж | е | о | л |   |
| ч | т | я |   | о |
| г | у | ш | е | з |
| к | а | т | ь | е |
| е | а | т |   | а |

Такая процедура отсечения ветвей была бы просто необходима, если бы строк было поменьше, и дерево было бы соответственно гораздо ветвистей.

Предложенную процедуру легко автоматизировать и сделать пригодной для реализации на ЭВМ. Алгоритм дешифрования должен состоять из следующих этапов.

1. Предварительная работа. Анализируя достаточный представительный объем открытых текстов построить множество запрещенных биграмм.

2. Предварительная работа. Составить словарь всех возможных  $v$ -грамм для  $v=2,3,\dots,d$ , которые могут встретиться в открытом тексте. Число  $d$  выбирается, исходя из возможностей вычислительной техники.

Построить таблицу  $8 \times 8$ . При этом перебираются последовательно все запрещенные биграммы и для каждой опробуемой биграммы – последовательно все строки. Если хотя бы в одной строке первый символ биграммы встречается в  $i$ -том столбце, а второй в  $j$ -ом, то клеточка  $i, j$  таблицы зачеркивается.

3. Выбрать некоторый столбец в качестве начального столбца.

4. Начать процедуру построения дерева путем пристраивания к исходному столбцу всех вариантов столбцов.

5. Для каждого полученного варианта добавить еще один из оставшихся столбцов. Если хотя бы в одной из строк таблицы встретится 3-грамма, которая отсутствует в словаре размещенных 3-грамм, то вариант отсеивается.

6. Для каждого из не отсеянных вариантов добавляем еще один столбец и проводим отсев ложных вариантов по словарю разрешенных 4-грамм.

Если словарь был построен только для  $d$ , то отсев проводится путем проверки на допустимость 3-грамм, встретившихся в последних 3-х столбцах каждой строки. Продолжаем этот процесс до получения полной перестановки.

Ниже, в таблице, приведен восстановленный для нашего примера текст.

|    | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|----|---|---|---|---|---|---|---|---|
| 1  | я |   | в | а | м |   | п | и |
| 2  | ш | у |   | ч | е | г | о |   |
| 3  | ж | е |   | б | о | л | е |   |
| 4  | ч | т | о |   | я |   | м | о |
| 5  | г | у |   | е | щ | е |   | с |
| 6  | к | а | з | а | т | ь |   | т |
| 7  | е | п | е | р | ь |   | я |   |
| 8  | з | н | а | ю |   | в |   | в |
| 9  | а | ш | е | й |   | в | о | л |
| 10 | е |   | м | е | н | я |   | п |
| 11 | р | е | з | р | е | н | ь | е |
| 12 | м |   | н | а | к | а | з | а |
| 13 | т | ь |   | с | н | а | ч | а |
| 14 | л | а |   | я |   | м | о | л |
| 15 | ч | а | т | ь |   | х | о | т |
| 16 | е | л | а |   | п | о | в | е |
| 17 | р | ь | т | е |   | м | о | е |
| 18 | г | о |   | с | т | ы | д | а |
| 19 | в | ы |   | б |   | н | е |   |
| 20 | у | з | н | а | л | н |   | н |
| 21 | е | к | о | г | д | а |   | к |
| 22 | о | г | д | а |   | б |   | н |
| 23 | а | д | е | ж | д | у |   | я |
| 24 | и | м | е | л | а |   | х | о |
| 25 | т | ь |   | р | е | д | к | о |
| 26 | х | о | т | ь |   | в |   | н |
| 27 | е | д | е | л | ю |   | р | а |
| 28 | з |   | в |   | д | е | р | е |
| 29 | в | н | е |   | н | а | ш | е |
| 30 | й |   | в | н | д | е | т | ь |
| 31 | в | а | с |   |   |   |   |   |

Дальнейшее развитие шифры перестановки получили при осуществлении идеи непрерывной локальной перестановки символов

открытого текста под действием управляющей последовательности. Для осуществления перемешивания знаков открытого текста в памяти шифратора запоминаются отдельные знаки текста и проводится задержка их передачи в дискретном времени. Введем параметры  $n_1$  и  $n_2$ , так, что  $n = n_1 + n_2$ . В этих шифрах  $i$ -й знак передаваемого сообщения переставляется в зашифрованном сообщении на  $j$ -е место, где  $i - n_1 \leq j \leq i + n_2$ .

Управляющую последовательность временем задержки стараются выбрать так, чтобы время задержки каждого символа было случайной величиной с равномерным распределением, то есть вероятность каждого фиксированного значения времени задержки должна быть близка к  $1/n$ .

## 7.2 Шифрующий автомат скользящей перестановки

Рассмотрим схему шифрующего автомата, позволяющего при подходящей управляющей последовательности реализовать произвольный шифр скользящей перестановки, рис.7.1.

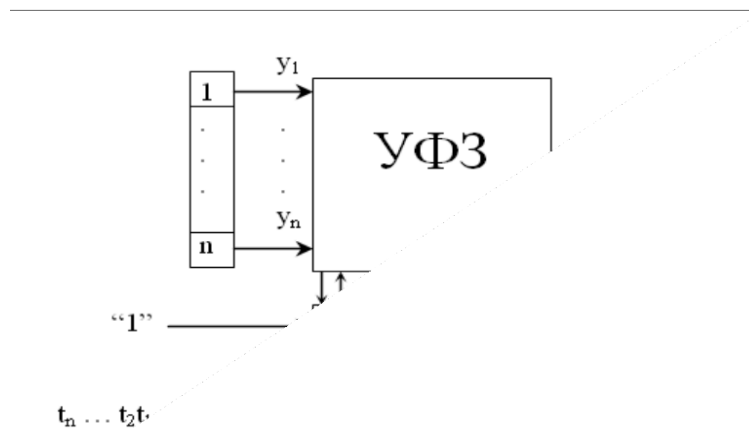


Рис. 7.1. Схема реализации шифрующего автомата скользящей перестановки

На вход узла формирования задержки (УФЗ) в каждом такте  $t$  подается вектор  $\vec{y} = (y'_1, \dots, y'_n)$ .

Узел формирования задержки является конечным автоматом

$$y'_i \in \{0,1\}, i = \overline{2, n-1}, y'_1 = y'_n = 1.$$

$$(F_1^n, F_2^n, \{1, \dots, n\},$$

$\mathcal{S}, \lambda$ ) множеством состояний которого является множество

все возможных двоичных векторов - заполнений  $\vec{x}(t) = (x'_1, \dots, x'_n)$  нижнего накопителя. В такте  $t$  вырабатывается натуральное число – значение  $\gamma$  задержки.

При этом автомат переходит в следующее состояние:

$$\gamma_t = \max j : \{x'_j = y'_j = 1, j = \overline{1, n}\},$$

$$\vec{x}(t+1) = (x_1^{t+1}, \dots, x_n^{t+1}),$$

где

$$x_1^{t+1} = 1,$$

$$x_i^{t+1} = \begin{cases} 0, & i = \gamma_t + 1 \\ x_{i-\gamma_t}^t, & i \in \{2, \dots, \gamma_t, \gamma_t + 2, \dots, n\} \end{cases}$$

Знаки открытого текста записываются на нижний накопитель. В линию в  $t$ -ом такте посылается знак открытого текста, записанный в ячейке с номером  $\gamma_t$ . Состояния автомата  $x(t)$  являются индикаторами, показывающими какие из знаков открытого текста еще не считаны с нижнего накопителя. Для зашифрования последовательности  $tN, \dots, t2, t1$  поступают следующим образом.

Сначала записываем в нижний накопитель первые  $n1$  знаков открытого текста

$(tn1, \dots, t1, 0, \dots, 0)$

Одновременно автомат устанавливается в начальное состояние

$$\vec{x}(1) = (0, \dots, 0).$$

После этого автомат УФЗ начинает работать по описанному выше закону до тех пор, пока в накопитель не поступит последний знак  $tN$  открытого текста. С прекращением подачи на накопитель знаков открытого текста происходит прекращение подачи единиц на накопитель-индикатор. В оставшиеся  $n1$  тактов производится считывание записанной в накопителе

информации.

При расшифровывании УФЗ работает по той же схеме, только вместо считывания необходимо организовывать

### **7.3 Особенности работы УФЗ**

В каждом такте  $t$  (за исключением последних  $n1$  тактов) в накопителе индикаторе  $x(t)$  записано ровно  $n1$  единиц. Поэтому в такте  $t$  величина задержки может принимать только одно из  $n1$  значений в интервале  $\{1, \dots, n\}$ . В частном случае, когда  $n=1$ , либо  $n1=n$  УФЗ вырабатывает постоянно значения задержки  $\gamma = 1$  и  $nt\gamma =$  соответственно. Легко видеть, что результирующее преобразование открытого текста действительно будет шифром скользящей перестановки.

Условие  $yt1=1, t=1, 2, \dots$  обеспечивает постоянное считывание во всех тактах, а условие  $yt2=1$  ограничивает величину задержки  $\gamma \leq n$ .

### **7.4 Описание программной реализации**

Для выполнения лабораторной работы на компьютере необходимо установить программный модуль **XY-Mover**.

#### **1) Строка меню**

В данной программе меню состоит из трех пунктов: Шифрование, Вид, Помощь. Необходимый пункт меню можно выбрать, щелкнув по нему левой кнопкой мыши, или с помощью кнопок клавиатуры «вправо», «влево», нажав перед этим функциональную клавишу «F10». После того как пользователь выбрал необходимый ему пункт меню, откроется ниспадающее подменю.

Рассмотрим пункты меню подробнее.

#### *Шифрование*

– Пункты ниспадающего меню можно выбрать либо левой кнопкой мыши, либо кнопками клавиатуры «вверх», «вниз». Рассмотрим подробнее пункты подменю.

– Редактирование параметров – эта функция меню позволяет задать необходимые параметры в поле окна программы «Параметры шифратора»

– Шифровать – выбор этого пункта меню запускает процесс шифрования

– Дешифрование – выбор этого пункта меню запускает процесс дешифрования

– Выход – завершение работы программы

#### *Вид*

– Этот пункт меню позволяет выбрать внешний вид программы. Ниже приводятся пункты подменю:

– Параметры – выбор этого пункта меню позволяет использовать поле «Параметры шифратора», описанную ниже.

– Схема шифратора – выбор этого пункта меню позволяет наблюдать структурную схему шифрующего автомата.

– Строка состояния – выбор этого пункта меню позволяет наблюдать строку состояния, описанную ниже.

#### **2) Панель инструментов**

Возможно, пользователю будет удобнее воспользоваться панелью инструментов (так называемыми «кнопками»), вместо работы с меню.

«Кнопки» дублируют некоторые пункты меню, но выбрать «кнопку» гораздо удобнее, чем пункт подменю. Для этого необходимо просто щелкнуть по выбранной кнопке левой кнопкой мыши. Рассмотрим «кнопки» слева направо:

– «А», выбор этой кнопки позволяет получить результат аналогичный пункту меню: Вид-Параметры;

– «Схема шифратора» – выбор этой кнопки позволяет получить результат аналогичный пункту меню Вид- Схема шифратора;

– «Строка состояния» – выбор этой кнопки позволяет получить результат аналогичный

пункту меню: Вид- Строка состояния;

- «Редактирование параметров» – выбор этой кнопки позволяет получить результат аналогичный пункту меню: Шифрование-Редактирование параметров;

- «Шифровать» – выбор этой кнопки позволяет получить результат аналогичный пункту меню Шифрование - Шифровать

- «Дешифровать» – выбор этой кнопки позволяет получить результат аналогичный пункту меню Шифрование - Дешифровать

- «Прервать» – выбор этой кнопки позволяет прервать процесс обработки данных (шифрование или дешифрование)

### 3) Строка состояния

Строка состояния находится в нижней части окна программы. На ней выводится информация о состоянии программы:

- «Шифрование методом скользящей перестановки» – это сообщение указывает на то, что программа готова к работе.

- «Завершено ... %» – индикация объема выполненной работы при зашифровании или расшифровании.

### 4) Описание полей окна программы

Параметры шифратора

- n1 – число знаков, которые записываются в нижний накопитель первыми;

- n2 – остальные знаки (всего их 127);

- отводы регистра – точки съема ЛРС;

- начальное заполнение – начальное заполнение ЛРС, которое пользователь может изменять.

Входной поток

- поле, в котором отражается имя текстового файла, содержание которого нужно шифровать/расшифровать;

- кнопка «открыть» – при нажатии на эту кнопку открывается стандартное для Windows окно «Открытие файла»;

- текст – содержимое файла, открытого для шифрования/расшифрования;

- битовый поток – побитное представление символов выбранного файла.

Выходной поток

- поле, в котором отражается имя текстового файла, содержание которого нужно расшифровать/шифровать;

- кнопка «открыть» – при нажатии на эту кнопку открывается стандартное для Windows окно «Открытие файла»;

- текст – содержимое файла, открытого для расшифрования/шифрования;

- битовый поток – побитное представление символов выбранного файла.

## 8. Задания

1. Для выполнения лабораторной работы на компьютере необходимо установить программный модуль XY-Mover.

2. Выполнить начальные установки шифратора, согласно примеру.

3. Загрузить файл для шифрования.

4. Произвести шифрование информации с использованием шифра скользящей перестановки, сохранить шифртекст в файле.

5. Описать в отчете процесс шифрования и расшифрования данных с использованием программы-эмулятора XY-Mover. Проанализировать полученные данные.

6. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные

в соответствии с номером варианта, указанным преподавателем.

#### 9. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

#### 10. Контрольные вопросы

1. Почему шифрование методом гаммирования является наиболее подходящим для высокоскоростных линий телекоммуникационной связи?

2. Какие общие требования, предъявляются к гамме шифра?

3. Приведите пример, поясняющий работу шифрующего автомата скользящей перестановки при  $n=5$ ,  $n_1=2$ ,  $n_2=3$ .

4. Кратко опишите работу схемы реализации шифра скользящей перестановки.

#### 11. Литература

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.

2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.

3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.

4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.

5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.

6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.

7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## **ЛАБОРАТОРНАЯ РАБОТА № 8. Распределение ключей по схеме Диффи-Хеллмана. Криптографическая система RSA. Криптографическая система Эль-Гамала**

### **1. Цель работы**

Ознакомление с общими принципами построения и использования PGP программных средств защиты информации, в частности с программой

Освоение средств программной системы PGP, предназначенных для:

- шифрования конфиденциальных ресурсов и разграничения доступа к ним;
- обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи;
- надежного уничтожения остаточной конфиденциальной информации;
- скрывания присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

Для выполнения лабораторной работы при отсутствии на компьютере программы PGP ее необходимо установить.

Инсталляционный файл прилагается к описанию лабораторной работы PGPfreeware602i.

Выбрать для установки только следующие компоненты:

- PGP 6.0.2 Program Files;
- PGP 6.0.2 User's Manual;
- Unconfigured PGP 6.0.2 Client Install;
- PGPdisk for Windows.

На вопрос программы установки о существовании ключей ответить «Нет», а на вопрос о необходимости перезагрузки системы – «Да».

### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### **3. Распределение времени занятия:**

Всего: 180 мин

|                                             |        |
|---------------------------------------------|--------|
| Вступительная часть                         | 2 мин  |
| Проверка готовности студентов к занятию     | 5 мин  |
| <b><i>Программа лабораторной работы</i></b> |        |
| 1.Описание лабораторной работы.             | 35 мин |
| 2.Задание.                                  | 35 мин |
| Проверка выполнения лабораторной работы     | 10 мин |
| Заключительная часть                        | 3 мин  |

### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

**ЗАПРЕЩАЕТСЯ:** переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.

– Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

– Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

– Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

– При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

– Доложить руководителю занятий или лаборанту о завершении работ.

– Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### **5. Аппаратное обеспечение**

Класс персональных ЭВМ, классная доска, мел (маркеры).

### **6. Программное обеспечение**

Программное обеспечение для выполнения лабораторной работы "**PGP 6.0**".

### **7. Описание лабораторной работы**

#### **7.1 Возможности PGP 6.0**

Основные задачи программы *PGP* – шифровать файлы и почтовые сообщения, заверять их электронными подписями, полностью уничтожать файлы на диске. Кроме этого, *PGP* предоставляет следующие возможности:

- хранение открытых ключей на удаленном сервере;
- использование трех симметричных алгоритмов шифрования и двух асимметричных;
- четыре способа запуска: *E-mail plugins*, *PGP tray*, *PGP tools*, контекстное меню;
- разделение ключей;
- установка уровня валидности ключа и доверия владельцу ключа.

**PGPkeys** - Это программа, входящая в состав *PGP 6.0*, и обеспечивающая работу с ключами, рис.8.1.

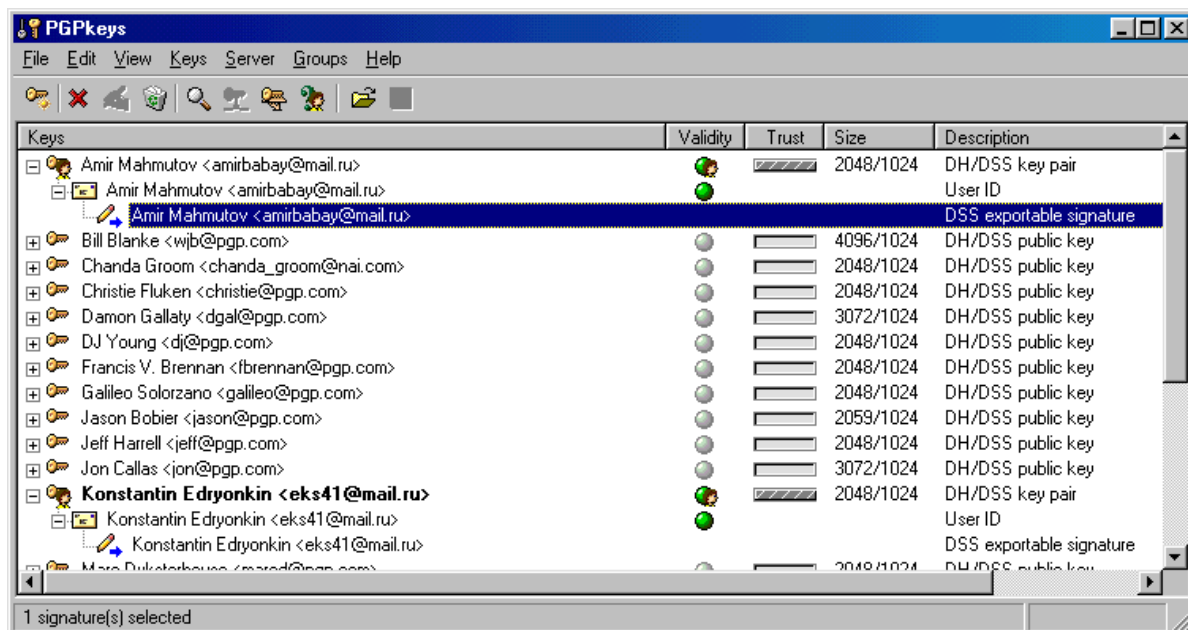


Рис. 8.1 Окно PGPkeys

В меню **File** содержатся две команды, одна из которых **Exit**, другая – **Send Key Shares** позволяет послать локальную копию разделенного ключа по сети.

Меню **Edit** кроме обычных команд содержит команду **Preferences**, которая служит для задания настроек программы, рис.8.2.

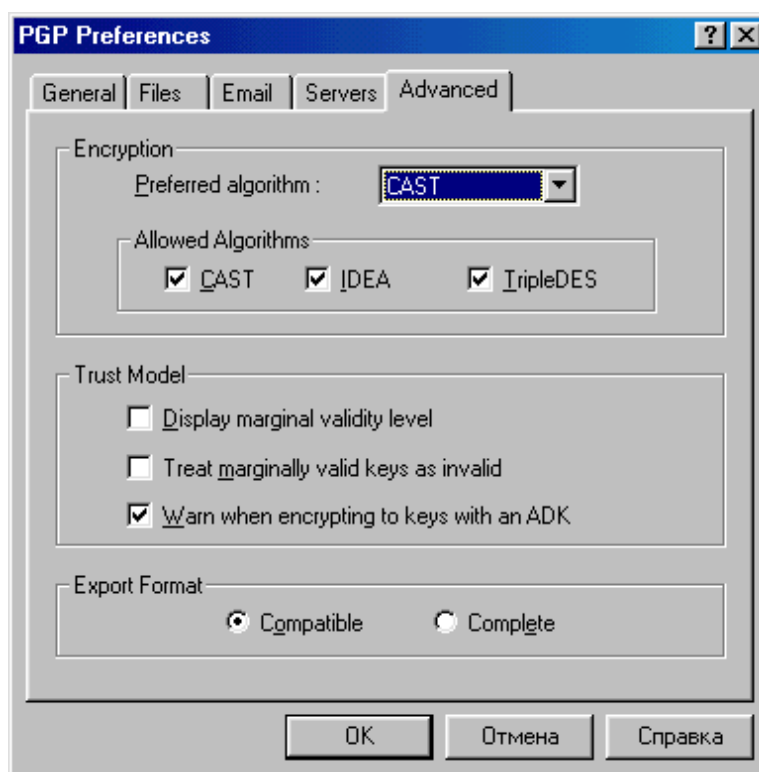


Рис. 8.2. Окно PGPPreferences

С помощью меню **View** можно задать отображаемые на экране свойства ключей.

## 7.2 Команды меню Keys

**Sign** – позволяет подписать своим закрытым ключом открытые ключи других пользователей. Тем самым вы можете показать, что доверяете владельцу используемого

ключа, то есть ключ действительно принадлежит владельцу.

При этом можно задать модификаторы: 1) *Non Exportable* – для локального набора ключей; 2) *Exportable* – заверенный ключ отсылается на сервер; 3) *Meta- introducer Non-Exportable* – доверяете не только владельцу, но и любому доверенному им ключу; 4) *Trusted Introducer Exportable* – вы доверяете владельцу подписывать ключи, рис.8.3.

**Set as Default Key** – назначить данный ключ ключом по умолчанию.

**Add Name/Photo/Revoker** – позволяет добавить к свойствам ключа имя владельца, имеющего право объявить ваш ключ недействительным.

**Revoke** – объявить ключ недействительным.

**Reverify Signatures** – проверить сигнатуру (правильность) ключа.

**New Key** – добавить новый ключ.

**Share Split** – разделить ключ между несколькими владельцами.

**Import/Export** – импортировать/экспортировать ключ из/в текстовый файл.

**Key Properties** – свойства (при этом можно задать степень доверия, валидность ключа), рис.8.4, 8.5.

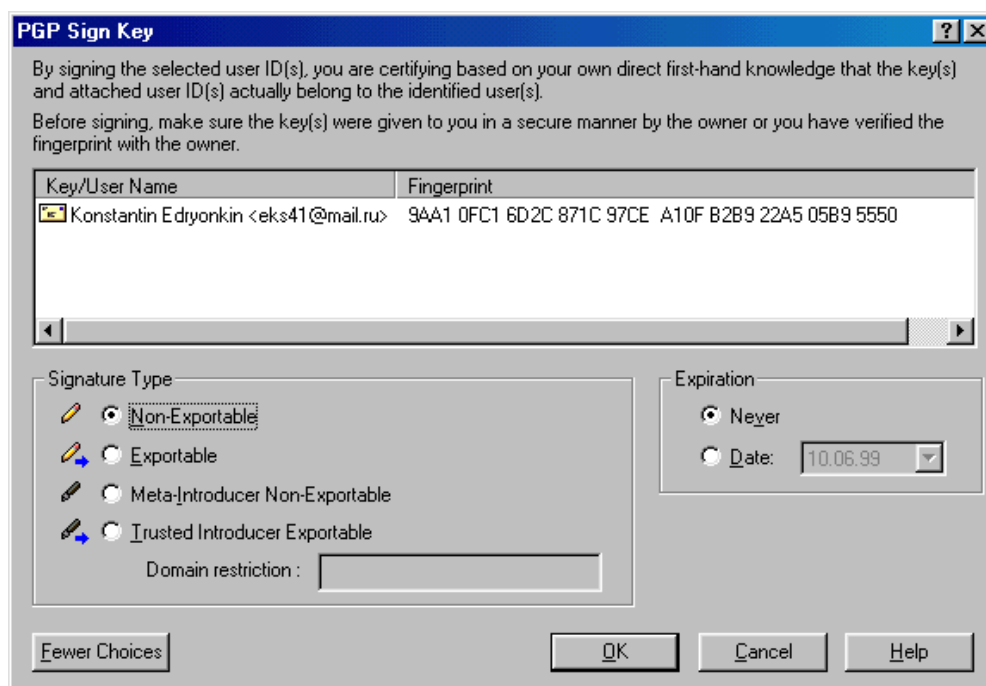


Рис.8.3. Окно PGP SignKey



Рис. 8.4. Окно Key Generation Wizard

В меню **Server** сосредоточены команды для работы с удаленным сервером ключей. Команда **Send to** позволяет послать ключи на выбираемый сервер, рис.8.6.

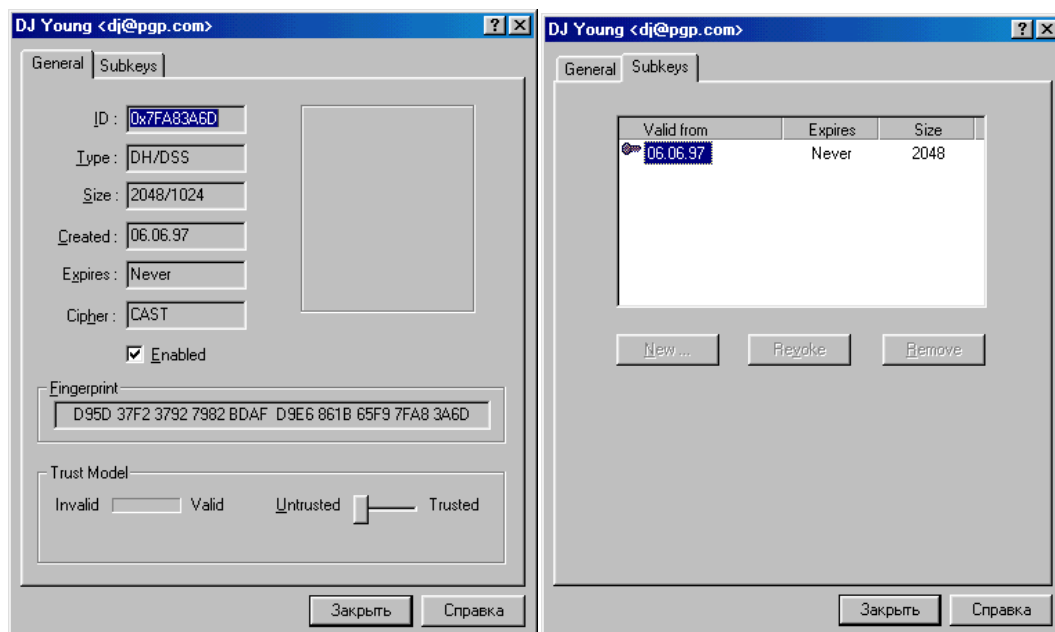


Рис. 8.5. Свойства ключа

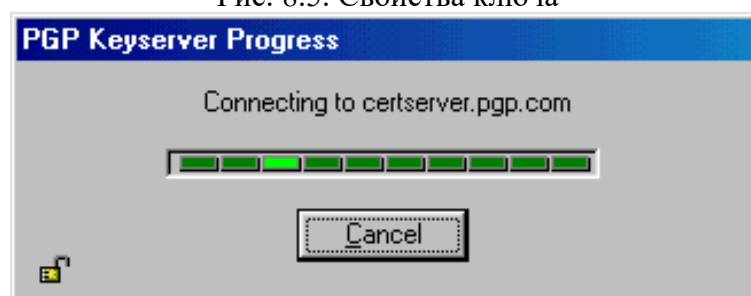


Рис.8.6. Соединение с удаленным сервером

При помощи команды **Search** можно попытаться найти на удаленном сервере ключ, задав соответствующие параметры, рис.8.7.

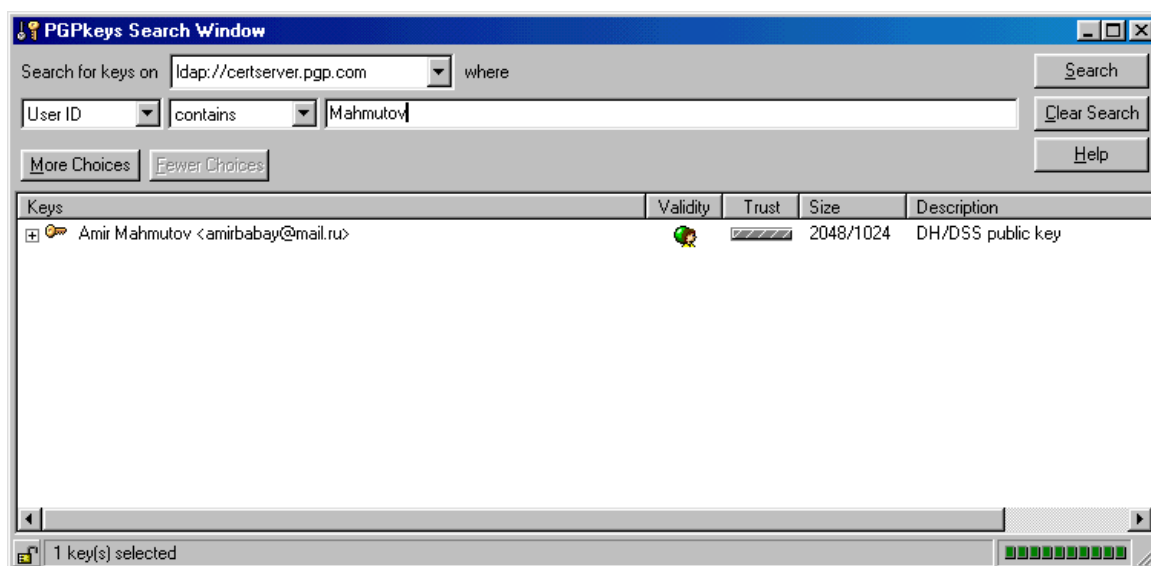


Рис. 8.7. Поиск ключа на удаленном сервере Команда **Update** позволяет обновить выбранный ключ, получив информацию с сервера

В меню **Groups** содержатся команды для работы с группами.

Команды **New Group**, **Show Groups**, **Import Groups** позволяют, соответственно, добавить группу, показать группы, импортировать группы из файла. Объединение владельцев ключей в группы позволяет легко и просто шифровать сообщения для отправки всем членам группы.

Наконец, меню **Help**, стандартное для *Windows*, позволяет получить справку.

### 7.3 PGPtray

Загружается при запуске *Windows*. Для активизации меню достаточно нажать кнопкой мыши на значок рядом с часами, рис.8.8.

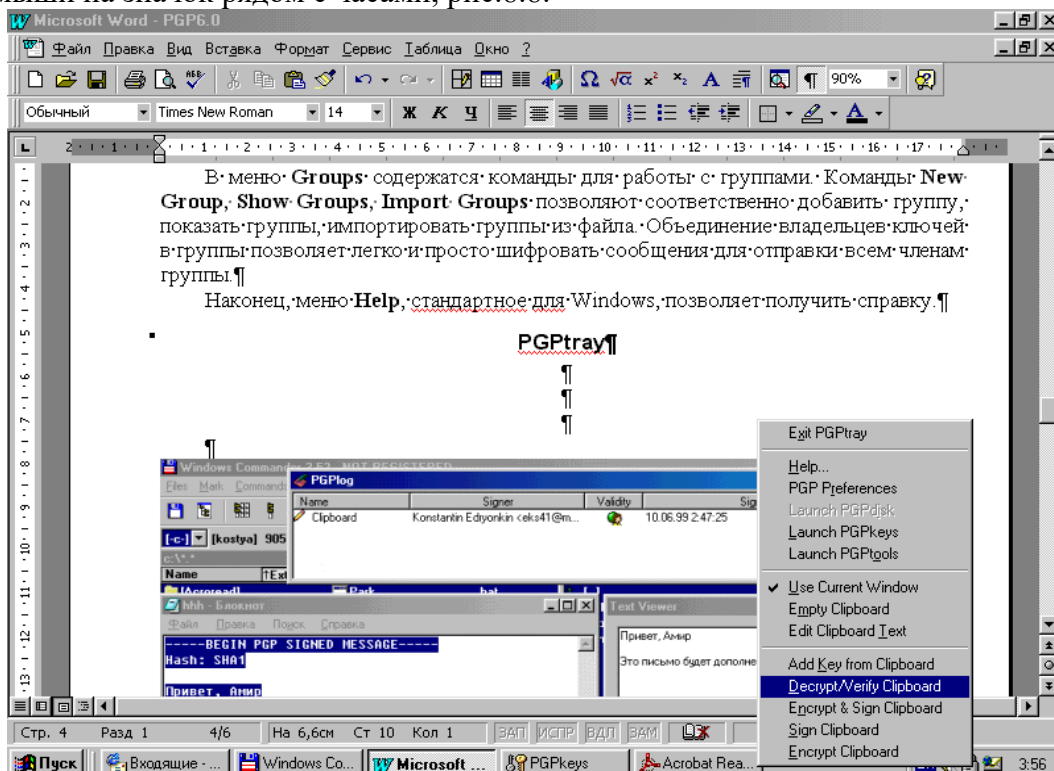


Рис. 8.8. Запуск PGP с использованием значка на панели задач

В меню содержатся команды для выхода, запуска других компонентов *PGP*, редактирования буфера обмена, работы с буфером обмена (добавление ключа, расшифрование/проверка подписи, зашифрование и подпись, просто подпись и просто зашифрование).

Если в используемом почтовом клиенте нет встроенных команд *PGP*, то можно работать с помощью *PGPtray*. Например, для подписи письма достаточно скопировать его в буфер и исполнить команду **Sign Clipboard**.

После этого достаточно вставить в тело письма уже подписанный текст, рис.8.10.

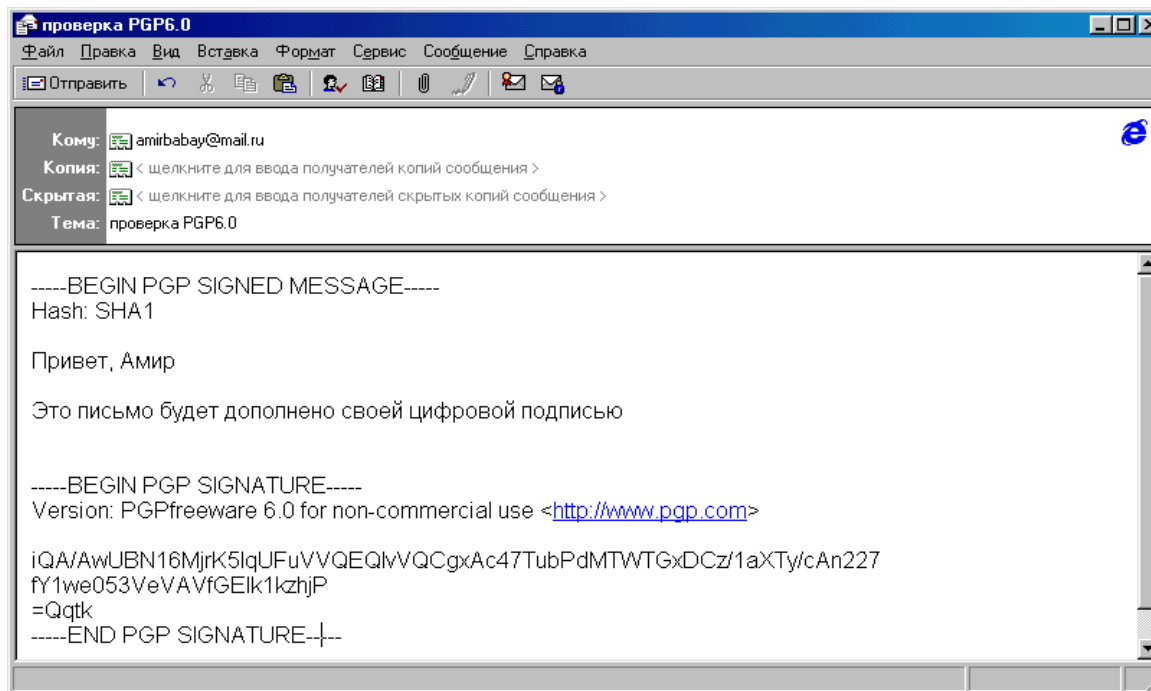


Рис. 8.10. Пример отправки письма с цифровой подписью

Аналогично получателю письма достаточно скопировать полученное письмо в буфер обмена и выбрать команду **Decrypt/Verify Clipboard**.

Естественно, в коллекции ключей должен быть открытый ключ владельца, подписавшего письмо, рис.8.11, 8.12.

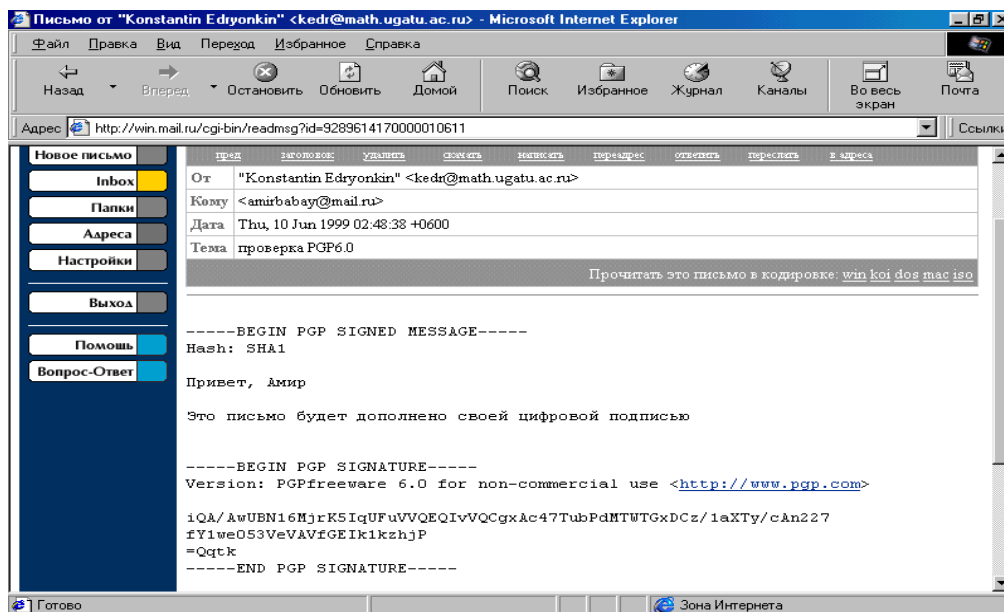


Рис. 8.11. Пример получения письма с цифровой подписью

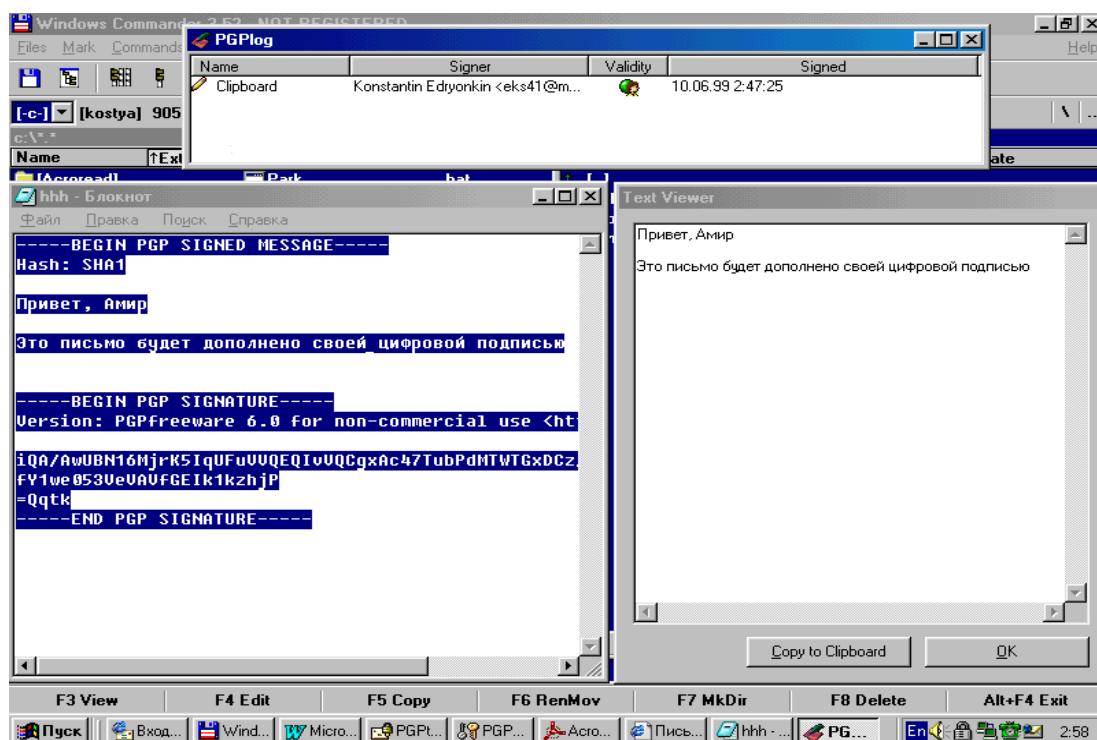


Рис. 8.12. Результаты проверки подписи

#### 7.4 PGTools

Этот компонент *PGP* представляет собой небольшую панель с кнопками, позволяющими выполнить нужное действие: открыть *PGPkeys*, зашифровать, подписать, зашифровать и подписать одновременно, расшифровать/проверить подпись, затереть файл, затереть неиспользуемое дисковое пространство, рис.8.13.

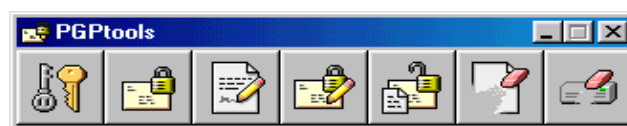


Рис. 8.13. Компоненты панели PGTools

Альтернативой *PGTools* могут служить команды, добавляющиеся при установке *PGP* в контекстное меню работы с файлами и меню **Файл** Проводника *Windows*.

#### 8. Задания

1. Ознакомиться со сведениями о программе *PGP* (см. параграф 1).
2. Запустить программу *PGTools* (с помощью меню «Пуск» или значка *PGP*tray на панели задач), ознакомиться и отразить в отчете о лабораторной работе *состав программных средств, входящих в систему PGP* (при необходимости воспользоваться справкой о системе *PGP*).

3. Создать криптографические ключи с помощью программы *PGPkeys*. Включить в отчет о лабораторной работе *сведения о порядке создания ключей шифрования в системе PGP* и включить в электронную версию отчета копии используемых при этом экранных форм, а также ответы на вопросы:

- как обеспечивается случайность выбираемых криптографических ключей в системе *PGP*;
- как и где хранится секретный ключ пользователя в системе *PGP*;
- как может быть обеспечена в системе *PGP* возможность восстановления

секретного ключа пользователя при его случайной утрате.

4. Изучить (на примере обычных текстовых файлов и файлов изображений) способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. Включить в отчет о лабораторной работе *сведения о порядке шифрования и расшифрования файлов в системе PGP*, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры шифрования могут быть использованы, в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);
- как генерируется, как и где хранится ключ симметричного шифрования файла в системе PGP;
- как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей;
- изменяется ли и как размер файла после его шифрования (привести конкретные примеры для разных типов файлов).

5. Изучить (на примере документов из своей папки) способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools. Включить в отчет *сведения о порядке обеспечения аутентичности и целостности электронных документов в системе PGP*, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры получения электронной цифровой подписи могут быть использованы, в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);
- какова реакция программы на нарушение целостности подписанного документа (обязательно проверить на примере и результаты проверки отразить в отчете).

6. Изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в отчет *сведения о порядке одновременного обеспечения конфиденциальности, аутентичности и целостности электронных документов в этой системе*, а также включить в электронную версию отчета копии используемых при этом экранных форм.

7. Изучить способы надежного удаления файлов с конфиденциальной информацией с помощью функции Wipe программы PGPtools. Включить в отчет *сведения о порядке уничтожения конфиденциальных электронных документов в системе PGP* и включить в электронную версию отчета копии используемых при этом экранных форм.

8. Изучить способы надежного уничтожения остаточной информации, которая может содержать конфиденциальные сведения, с помощью функции Freespace Wipe программы PGPtools. Включить в отчет *сведения о назначении и порядке использования этой функции программы*, копии используемых в ней экранных форм и ответы на вопросы:

- как достигается надежное уничтожение остаточной конфиденциальной информации в системе PGP;
- является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации.

9. Изучить способы быстрого выполнения функций системы PGP с помощью программы PGPtray, ярлык которой размещен в правой части панели задач. Включить в отчет *сведения о назначении и порядке использования этой программы*, а также включить в электронную версию отчета копии используемых экранных форм.

10. Изучить способы управления настройками системы PGP при ее использовании в организациях с помощью программы PGPadmin (пройти все шаги диалога с мастером вплоть до последнего, на котором вместо кнопки «Save» нажать

кнопку «Отмена»). Включить в отчет сведения о возможностях и порядке администрирования системы PGP, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

- какие функции по управлению шифрованием и обеспечением целостности информационных ресурсов предоставляет администратору программа PGPAdmin;
- какие функции по управлению криптографическими ключами пользователей PGP предоставляет администратору программа PGPAdmin;
- какие возможности предоставляет программа PGPAdmin по управлению доступными для пользователей функциями программы PGP и где сохраняется подобная информация.

11. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Как выбрать длину криптографического ключа в системе PGP?
2. В чем достоинства и недостатки криптографических методов защиты информации?
3. Какие компьютерные системы называются безопасными?
4. В чем заключаются основные требования к защищенности компьютерных систем?
5. Для выполнения каких требований к защищенности компьютерных систем могут применяться криптографические методы защиты?
6. Насколько, на Ваш взгляд, надежны методы криптографической защиты информации, используемые в программе PGP?
7. Какими основными функциями защиты информации обладает программа PGP?
8. Какой принцип лежит в основе функции надежного уничтожения остаточной конфиденциальной информации программы PGP?

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А. И., Самсонов Б. Б., Кречет Т. В., Плохов Е. М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И.Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К.Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л.Добрушина и О.Б.Лупанова. – М.: ИЛ, 2015. – 512 с.

## ЛАБОРАТОРНАЯ РАБОТА № 9. Хэш-функции без ключа. Алгоритм SHA-1. Хэш-функции с ключом

### 1. Цель работы

Ознакомление с общими принципами построения и использования корректирующих кодов для контроля целостности информации, распространяемой по телекоммуникационным каналам.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

— ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

— Убедиться в целостности электрических розеток и разъемов.

— В лаборатории необходимо быть в сменной обуви.

— Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

— Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

— Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

— При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

— Доложить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы *Hemming.exe*.

## 7. Описание лабораторной работы

Программа предназначена для кодирования символов по алгоритму Хэмминга. Процессы кодирования и декодирования представлены на рис.9.2.

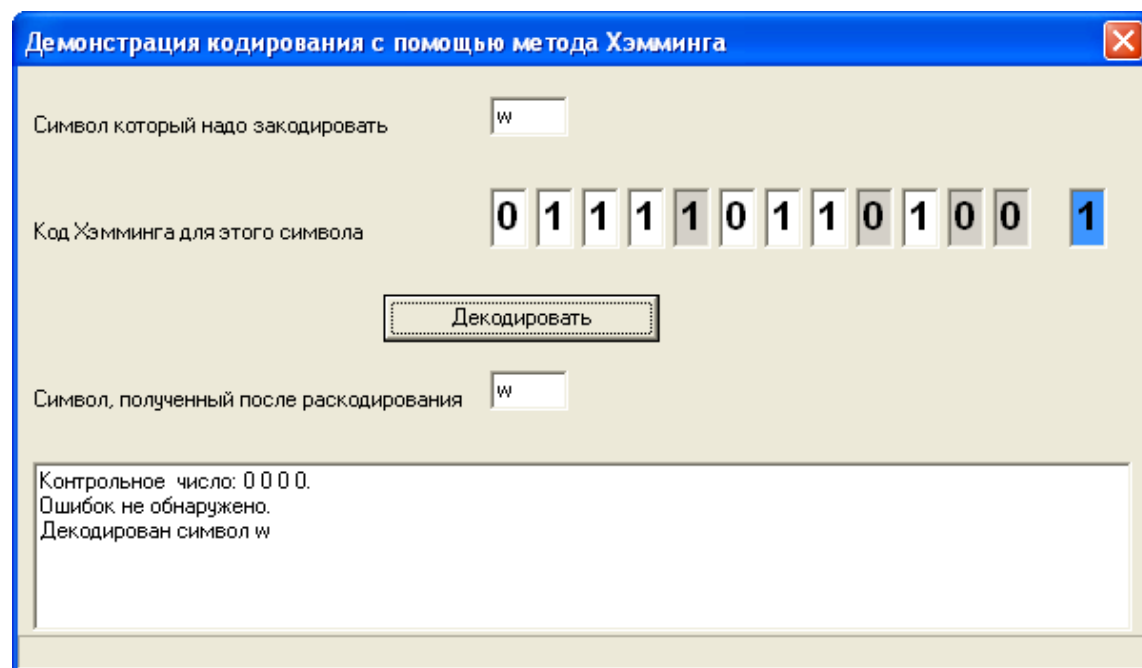


Рис. 9. 2. Процесс кодирования и декодирования Серым цветом отмечены контрольные биты, голубым – бит общей четности

В полученный код можно вносить ошибки. Одиночные ошибки могут быть исправлены, двойные – обнаруживаются без исправления. Если ошибка была исправлена, то указывается, в каком бите она была допущена. Затем символ декодируется. Процесс исправления одиночной ошибки представлен на рис. 9.3.

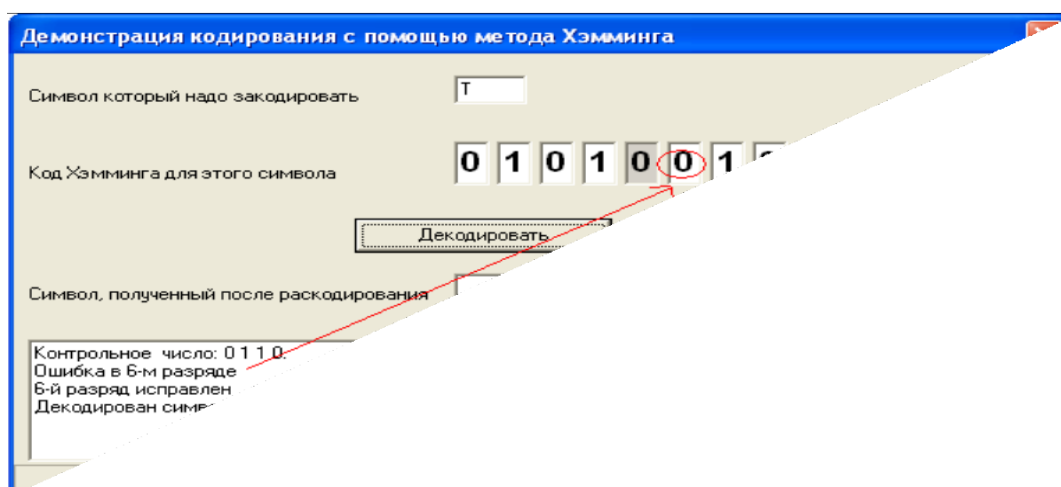


Рис. 9. 3. Процесс исправления одиночной ошибки

Если возникает ошибка двойной или более кратности – выводится сообщение о

невозможности исправления кода.

## **8. Задания**

1. Закодировать с помощью кода Хэмминга предложенный алфавит (варианты указаны в Таблице 9.1).
2. В каждую строку таблицы с закодированной информацией внести одиночную ошибку, зафиксировать в кодовой таблице результат декодирования.
3. В последние две строки таблицы с закодированной информацией внести двойные ошибки, зафиксировать в кодовой таблице результат декодирования.
4. Проанализировать полученные результаты и сформулировать аргументированные выводы.  
Описать полученный код Хэмминга:
  - количество контрольных и информационных разрядов и их номера;
  - избыточность кода;
  - относительная избыточность;
  - минимальное кодовое расстояние;
  - оценить корректирующую способность полученного кода.
5. Составить из предложенного алфавита слово длиной не менее 5 символов и закодировать его с помощью полученного кода Хэмминга.  
Подсчитать длину исходного текста (кодировка ASCII) и закодированного текста (код Хэмминга).
6. Представить краткий теоретический материал, в котором описать способ кодирования и декодирования информации с помощью кода Хэмминга.
7. Привести итоги проведенных экспериментов по кодированию с помощью программы Hemming.exe.
8. Оценить результаты обнаружения и исправления одиночных и обнаружения двойных ошибок. Сделать выводы о корректирующей способности исследуемого кода.
9. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Что представляет собой и как используется код Хэмминга?
2. Как составляется код Хэмминга?
3. Какие ошибки можно исправить с помощью кода Хэмминга?
4. От каких свойств кода зависит его корректирующая способность?
5. Какие ошибки могут возникнуть при составлении кода Хэмминга?

#### **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Методические указания**  
по выполнению практических работ  
по дисциплине «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»  
для студентов специальности 10.05.01 Компьютерная безопасность  
специализация «Информационно-аналитическая и техническая экспертиза  
компьютерных систем»

Ставрополь  
2025

## СОДЕРЖАНИЕ

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| Практическое занятие №1. Применение ИБ в прикладных задачах.....                                   | 70  |
| Практическое занятие №2. Идентификация, аутентификация.....                                        | 75  |
| Практическое занятие № 3. Информационные угрозы и их виды.....                                     | 80  |
| Практическое занятие № 4. Доктрина ИБ РФ.....                                                      | 84  |
| Практическое занятие № 5. ГОСТ Р 53114-2008.....                                                   | 88  |
| Практическое занятие № 6. ГОСТ Р ИСО/МЭК 27004-2021.....                                           | 92  |
| Практическое занятие № 7. Стандарт банка России СТО БР ИББС-1.0-2014.....                          | 94  |
| Практическое занятие № 8. ГОСТ Р ИСО/МЭК 15408-1-2012 Введение и общая модель.....                 | 98  |
| Практическое занятие № 9. ГОСТ Р ИСО/МЭК 15408-2-2013. Функциональные компоненты безопасности..... | 106 |
| Практическое занятие № 10. ГОСТ Р ИСО/МЭК 15408-3-2013. Компоненты доверия к безопасности.....     | 113 |
| Практическое занятие № 11. Принципы построения системы информационной безопасности.....            | 119 |
| Практическое занятие № 12. Модель Харрисона-Рузо-Ульмана.....                                      | 123 |
| Практическое занятие № 13. Модель Белла-ЛаПадула.....                                              | 129 |
| Практическое занятие № 14. Ролевая модель безопасности.....                                        | 130 |
| Практическое занятие №15. Основы криптографии.....                                                 | 133 |
| Практическое занятие №16. Симметричные шифры.....                                                  | 137 |
| Практическое занятие №17. Асимметричные шифры.....                                                 | 139 |
| Практическое занятие №18. Хэш-функции.....                                                         | 140 |

## Практическое занятие №1. Применение ИБ в прикладных задачах

### 1. Цель работы

Ознакомление со статистическими принципами сжатия информации с использованием методов Шеннона-Фано и Хаффмена.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

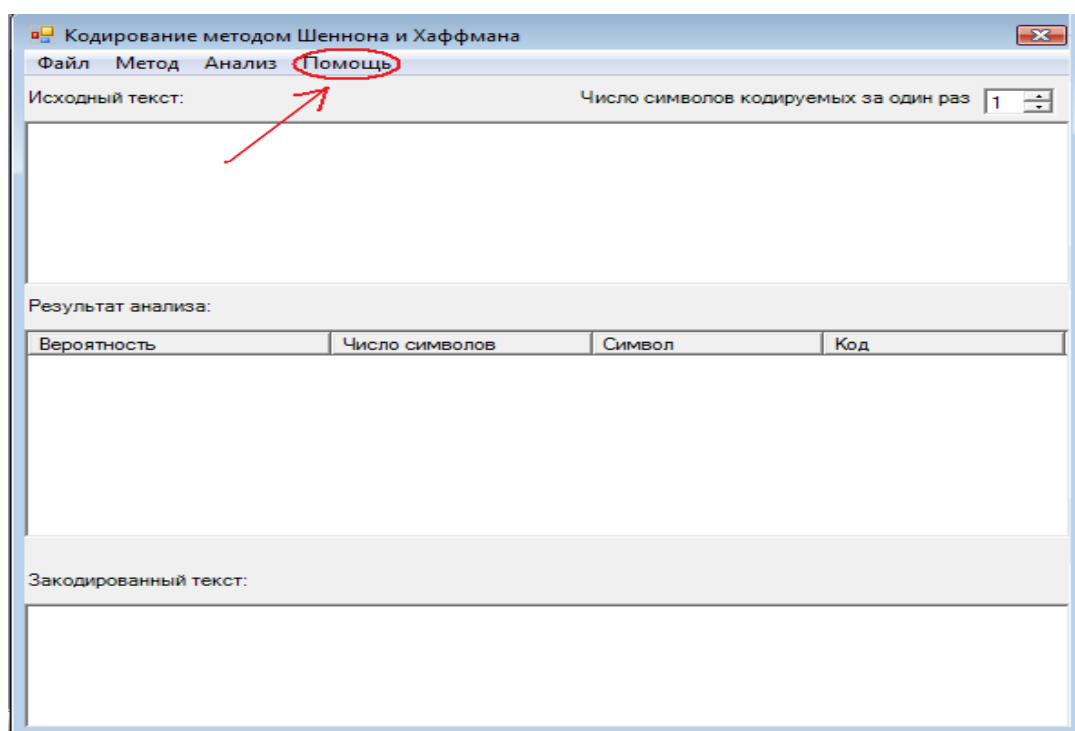
### 5. Аппаратное обеспечение

## 6. Программное обеспечение

## 7. Описание лабораторной работы

Для подсчета вероятности появления букв во введенном сообщении  $P$ , определения энтропии источника сообщений  $H$ , среднего числа символов при кодировании одной буквы сообщения  $L$ , необходимо выбрать закладку *Анализ*.

Кратко ознакомится со сведениями о программе вы можете, выбрав закладку *Помощь* (рис.11.3).



Чтобы выйти из данной программы достаточно выбрать закладку *Файл* и далее *Выход*.

Сравниваем полученные данные с результатами работы программы (рис.11.4)

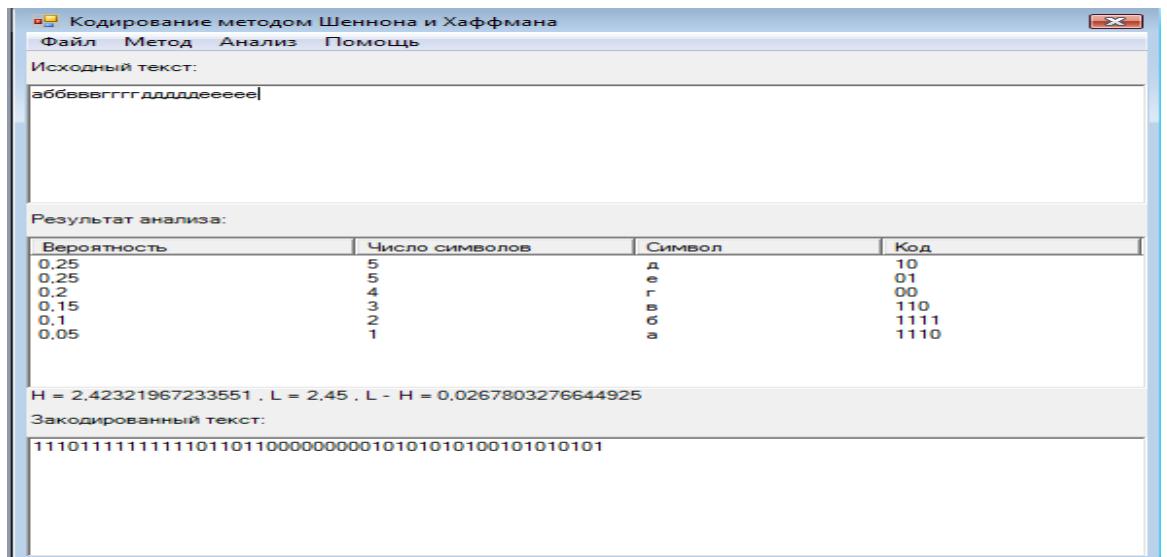


Рис. 11. 4. Пример кодирования

Сравниваем полученные данные с результатами работы программы (рис.11.5)

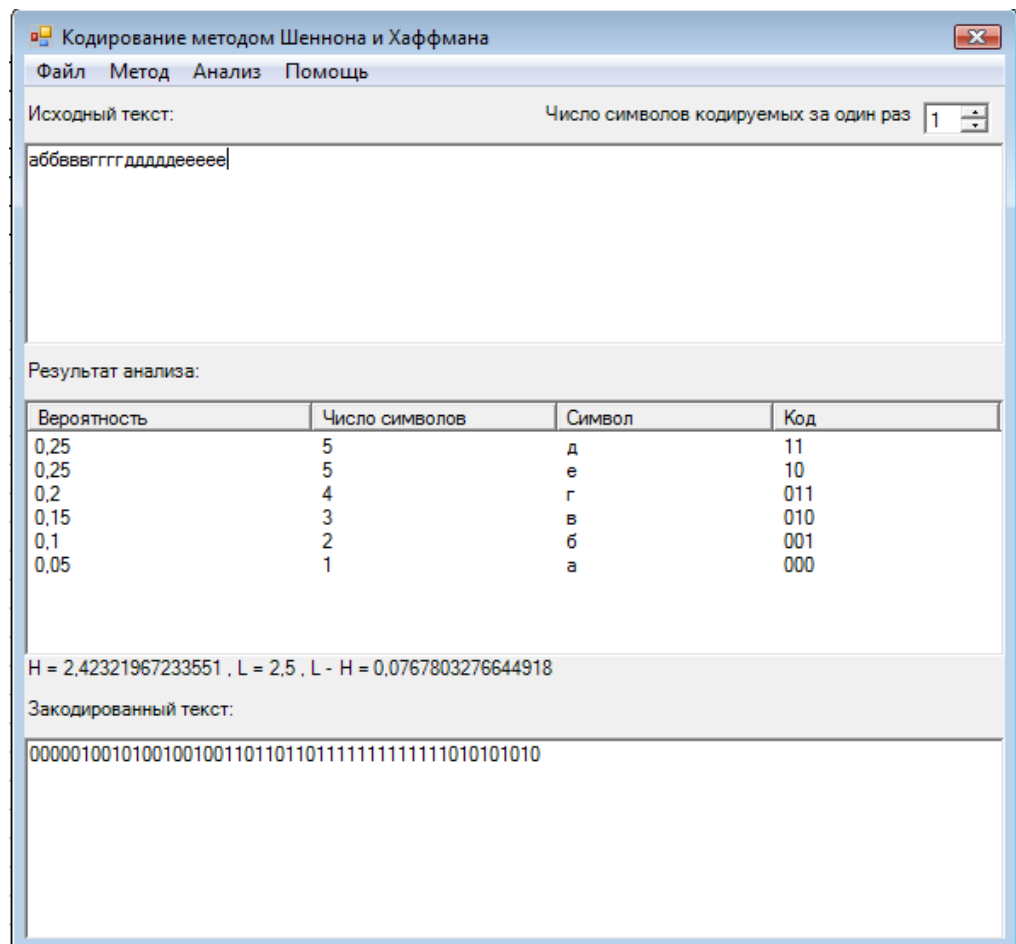


Рис. 11. 5. Пример кодирования

## 8. Задания

1. Ознакомиться со сведениями о программе *Shannon-Huffman.exe*, и рассмотреть примеры эффективного кодирования информации.
2. Запустить программу *Shannon-Huffman.exe*, предназначенную для демонстрации методов сжатия информации с использованием алгоритмов Шеннона-Фано

и Хаффмена.

3. Выполнить предложенные задания:

1). Число символов алфавита  $k = m$  ( $m$  – номер варианта). Составить такое исходное сообщение, чтобы

а) символы алфавита встречались в сообщении с равными вероятностями;

б) символы алфавита встречались в сообщении с разными вероятностями. 2).

Ввести произвольный связный текст на русском языке. Это может

быть пословица, стихотворение или произвольный текст. Используя результаты работы программы, следует проанализировать алфавит введенного сообщения: подсчитать количество символов алфавита, значение энтропии  $H$ , среднее количество символов на знак  $L$  при целочисленном кодировании.

4. Сохранить в отчете экранные формы, демонстрирующие процесс сжатия информации.

5. Отчет по лабораторной работе должен содержать результаты анализа программы *Shannon-Huffman.exe* при кодировании; алгоритм построения кода Хаффмена и Шеннона с применением знаний по данной тематике; результаты сравнения различных методов кодирования; выводы об эффективности используемых методов сжатия.

6. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

Включить в отчет о лабораторной работе выполненные задания 1, 2, 3.

## 9. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## 10. Контрольные вопросы

1. Какие коды позволяют производить однозначное декодирование даже без использования разделительного символа? Приведите примеры таких кодов.

2. Назовите условия построения оптимальных кодов.

3. С какой целью используются эффективные коды, и какие из них вам известны?

4. Перечислите основные методы сжатия информации без потерь.

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## Практическое занятие №2. Идентификация, аутентификация

### 1. Цель работы

Ознакомление с принципами сжатия информации с использованием метода *LZW* (*Lempel-Ziv-Welch*).

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

1. Описание лабораторной работы. 35 мин

2. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

— ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

— Убедиться в целостности электрических розеток и разъемов.

— В лаборатории необходимо быть в сменной обуви.

— Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

— Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

— Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

— При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

— Докладить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы *LZW.exe*.

## 7. Описание лабораторной работы

Лабораторная работа выполняется на персональном компьютере в среде программы *LZW.exe*.

При запуске программы *LZW.exe* появляется окно, рис. 12.1, содержащее следующие компоненты:

- строка текста, где вводится текст для сжатия;
- строка кода, где выводится код сжатого текста;
- строка кода, где выводится распакованный текст;
- таблица выполнения кодирования программой.

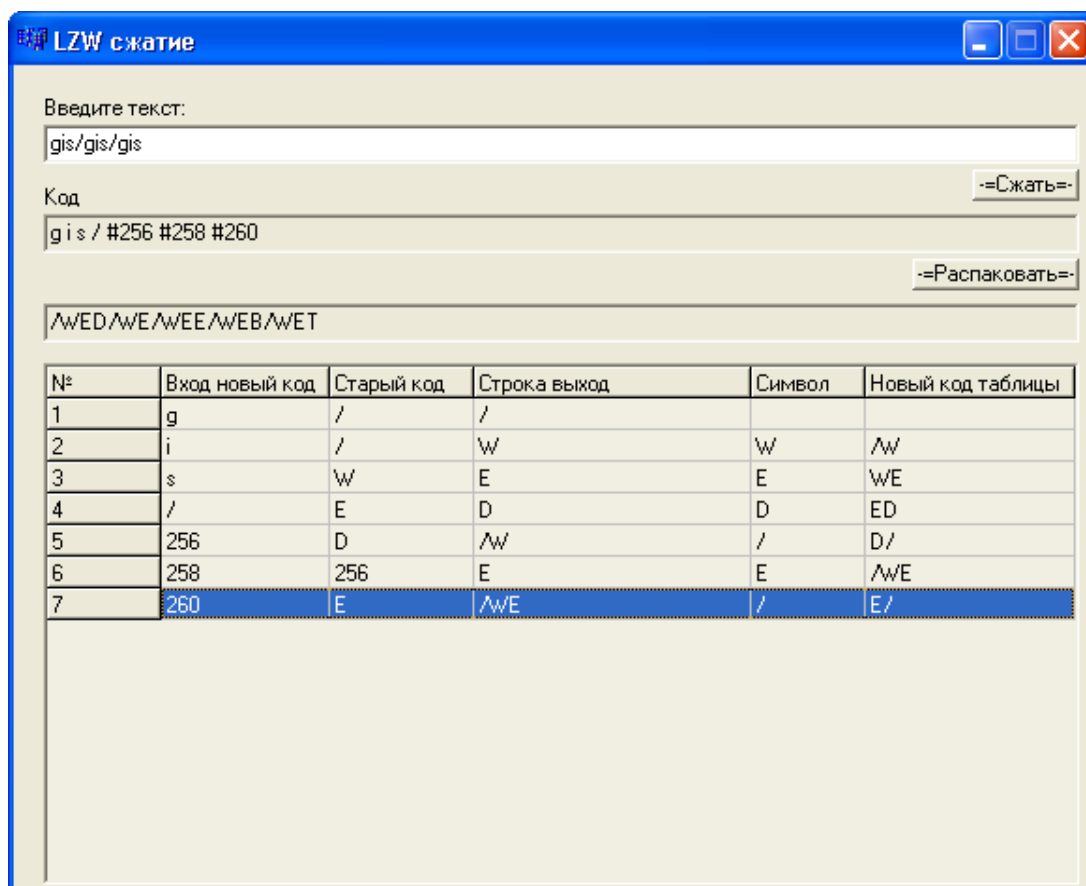


Рис. 12. 1. Главное окно программы

Программа позволяет сжимать и распаковывать текст любой длины, записанный как на кириллице, так и на латинице, а также просматривать процесс сжатия и распаковки текста.

Для сжатия какого-либо текста следует выполнить следующие действия:

1. В строку текста «Введите текст» ввести текст для сжатия.
2. Нажать кнопку «Сжать».
3. В строке «Код» появится код сжатого текста.
4. Нажать кнопку «Распаковать».
5. В следующей строке появится распакованный текст.
6. Просмотреть таблицу, выполнения программы сжатия и распаковки текста.

## 8. Задания

1. Сжать и затем распаковать исходные строки символов латинского алфавита, которые набираются непосредственно в окне программы. Сохранить в отчете экранные формы, демонстрирующие процесс сжатия и распаковки информации. Проанализировать сделанную работу и сделать выводы об эффективности алгоритма сжатия и распаковки.

2. Сжать и затем распаковать исходные строки символов кириллического алфавита, которые набираются непосредственно в окне программы. Сохранить в отчете экранные формы, демонстрирующие процесс сжатия и распаковки информации. Проанализировать сделанную работу и сделать выводы об эффективности алгоритма сжатия и распаковки.

3. Сжать и затем распаковать исходные строки чисел, которые набираются непосредственно в окне программы. Сохранить в отчете экранные формы, демонстрирующие процесс сжатия и распаковки информации. Проанализировать сделанную работу и сделать выводы об эффективности алгоритма сжатия и распаковки.

4. Сжать и затем распаковать исходные строки математических функций и формул, которые набираются непосредственно в окне программы. Сохранить в отчете экранные формы, демонстрирующие

процесс сжатия и распаковки информации. Проанализировать сделанную работу и сделать выводы об эффективности алгоритма сжатия и распаковки.

5. Сжать и затем распаковать исходные строки произвольных символов, которые набираются непосредственно в окне программы. Сохранить в отчете экранные формы, демонстрирующие процесс сжатия и распаковки информации. Проанализировать сделанную работу и сделать выводы об эффективности алгоритма сжатия и распаковки.

6. Включить в отчет:

- результаты сжатия и распаковки текстов (варианты указаны в Таблице 12.1) с помощью программы LZW-сжатия;
- сохранить в отчете кодовую таблицу в виде таблицы или рисунка;
- проанализировать полученные результаты и сформулировать аргументированные выводы.

7. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

Таблица 12.1

| № варианта | Задания к лабораторной работе |                  |           |                 |                |
|------------|-------------------------------|------------------|-----------|-----------------|----------------|
|            | № 1                           | №2               | №3        | №4              | №5             |
| 1          | Program                       | Информация       | 612534712 | $X+Y+Z-12=5$    | !!A/b/C/dE@?   |
| 2          | Processor                     | Математика       | 954723890 | $2^*X+Y+Z=2$    | ЪC<л>*ш/dE?    |
| 3          | Operation                     | Язык             | 410125935 | $X^*X+2^*Y-3$   | [4Pu/t%/3\$1\$ |
| 4          | Information                   | Вычисления       | 181952471 | $Y^*Y+Z=4^*X$   | Ё1?QяЧ*/!Д/;   |
| 5          | Mathematics                   | Общество         | 365412389 | $X+4Y+Z-2+1$    | ЙрTiV{G}%      |
| 6          | Language                      | Технология       | 113212598 | $X+2Y+5^*Z=3$   | ёЮB&<h>@       |
| 7          | Company                       | Кодирование      | 725847391 | $5^*X+Y+8Z=5$   | ЖО[Д]m/я/12    |
| 8          | Encoding                      | Информатика      | 820191856 | $X-6^*Y-3^*Z=2$ | ВН!(И)13N8     |
| 9          | Informatics                   | Обеспечение      | 100258741 | $X-2^*Y+7^*Z-9$ | Б!15fЛ2ыф»     |
| 10         | Software                      | Операция         | 101298752 | $8^*X/Y+Z/2=5$  | y4?-+/25/8?8   |
| 11         | Editor                        | Редактор         | 496123578 | $5X/2+Y/12+Z$   | уФ/z-1/2+3#    |
| 12         | Table                         | Процессор        | 123457890 | $X/5+5Y+Z/12$   | Г@14^5D/G      |
| 13         | Security                      | Таблица          | 154789123 | $7^*X>Y+2^*8Z$  | г13#&7Fоэ,     |
| 14         | Cybernetics                   | Безопасность     | 571238984 | $X^*X4^*Y<Z+5$  | ЩП/ы/45^7      |
| 15         | Knowledge                     | Знания           | 432987067 | $X+3^*Y>Z+27$   | i5(B)<px)И     |
| 16         | Computer                      | Кибернетика      | 433129851 | $X/2+2^*Y>3^*Z$ | шЁ8воп/тn5?    |
| 17         | System                        | Компьютер        | 184569347 | $7X+Y-Z/2>45$   | bPпQas156+     |
| 18         | Swindle                       | Система          | 189242578 | $Y<5^*X/3+Z-2$  | Z~+258 =fj     |
| 19         | Logic                         | Мошенничество    | 213459632 | $2^*Z>4^*X+5Y$  | C8&8вАъ/ё      |
| 20         | Programming                   | Логика           | 214357980 | $X/5+Y/4+Z=5$   | n-q6&8%^       |
| 21         | Hardware                      | Программирование | 896124587 | $Y/4-2X+3Z=6$   | S?dkошй^^      |
| 22         | Intellec                      | Техника          | 654932140 | $X+2>Z/4Y+2$    | p\$&Ghgdku     |
| 23         | Internet                      | Интеллект        | 781258743 | $X+7^*Z<2Y+3$   | j5%jkЖЕ%       |
| 24         | Translator                    | Интернет         | 834107892 | $2^*X-7Z=2+Y$   | Fd&5&%N8       |
| 25         | Driver                        | Транслятор       | 417625877 | $6X^*X+2^*Y-3$  | Dfj&5^6-2      |

## 9. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## 10. Контрольные вопросы

1. В чем состоит принцип LZW-сжатия?
2. Какие форматы файлов наиболее эффективно архивировать с помощью LZW-сжатия ?

3. В чем особенность процесса распаковки при использовании алгоритма LZW?
4. Какими достоинствами и недостатками обладает алгоритм LZW?

### **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб. пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

### Практическое занятие № 3. Информационные угрозы и их виды

#### 1. Цель работы

Целью работы является овладение практическими навыками составления шифра вручную, разработки и программирования вычислительного процесса шифрования методом моно- алфавитной подстановки, комбинированное использование нескольких различных способов шифрования.

#### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### 3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

##### ***Программа лабораторной работы***

1.Описание лабораторной работы. 35 мин

2.Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

#### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### ***4.1. Требования безопасности перед началом работ***

— ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

— Убедиться в целостности электрических розеток и разъемов.

— В лаборатории необходимо быть в сменной обуви.

— Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

##### ***4.2. Требования безопасности во время работы***

— Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.

— Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.

— При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

##### ***4.3. Требования безопасности по окончании работы***

— Доложить руководителю занятий или лаборанту о завершении работ.

— Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

#### 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы ОС Windows 2000 и выше, либо XP; Turbo Pascal 7; Borland Delphi 7; Borland C++.

## 7. Краткие теоретические сведения

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу).

Показатели криптостойкости:

- Количество всех возможных ключей;
- Среднее время, необходимое для криптоанализа.

При использовании метода криптографического закрытия **шифрования** - преобразованию подвергается каждый символ защищаемого сообщения.

Самой простой разновидностью является прямая(простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита.

**Шифр Цезаря** называется циклическим потому, что при выполнении замены буквы алфавита рассматриваются как расположенные по кругу: вслед за последней буквой алфавита вновь следует первая буква алфавита.

Шифр Цезаря реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на фиксированное число букв.

**Шифр Атбаш.** Вместо первой буквы алфавита писалась последняя буква, вместо второй – предпоследняя и т. д.

**Квадрат Полибия.** Для шифрования используется таблица, представляющая собой квадрат с шестью столбцами и шестью строками, которые нумеруются цифрами от 1 до 6. В каждую клетку такой таблицы записывалась одна буква. В результате каждой букве соответствует пара чисел, и шифрование сводится к замене буквы парой цифр.

Эффективным средством повышения криптостойкости шифров является комбинированное использование нескольких различных способов шифрования с помощью двух или более методов.

Как показали исследования, стойкость комбинированного шифрования  $S_k$  не ниже произведения стойкости используемых способов  $S_i$ , т.е.  $S_k \geq \prod S_i$

Комбинировать можно любые методы шифрования и в любом количестве.

## 8. Задания

### Варианты к лабораторной работе №14.

(ваш номер по журналу соответствует номеру варианта)

*Вариант 1.*

**Составить программу, которая шифрует сообщение** Complete support of RAR and ZIP archives **следующим образом:**

#### 1 уровень

**А. Составить программу, которая используя шифр Цезаря** заменяет каждую букву в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на 3 позиции (буквы) вперед.

#### 2 уровень

**В. Дополнить полученную программу шифром Атбаш**

#### 3 уровень

**С. Дополнить полученную программу шифром Квадрата Полибия [6x6],**

расположив буквы построчно.

*Вариант 2.*

**Составить программу, которая шифрует сообщение Highly sophisticated, original compression algorithm следующим образом:**

**1 уровень**

**А. Составить программу, которая использует шифр Атбаш**

**2 уровень**

**В. Дополнить полученную программу шифром Цезаря, заменяя каждую букву в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на 2 позиции (буквы) вперед.**

**3 уровень**

**С. Дополнить полученную программу шифром Квadrата Полибия [6x6], расположив буквы по столбцам.**

*Вариант 3.*

**Составить программу, которая шифрует сообщение Recovering physically damaged archives следующим образом:**

**1 уровень**

**А. Составить программу, которая используя шифр Цезаря заменяет каждую букву в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на 2 позиции (буквы) назад.**

**2 уровень**

**В. Дополнить полученную программу шифром Атбаш**

**3 уровень**

**С. Дополнить полученную программу шифром Квadrата Полибия [6x6], расположив буквы построчно.**

*Вариант 4.*

**Составить программу, которая шифрует сообщение Special algorithms optimized for text, audio, graphics следующим образом:**

**1 уровень**

**А. Составить программу, которая использует шифр Атбаш**

**2 уровень**

**В. Дополнить полученную программу шифром Цезаря, заменяя каждую букву в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на 4 позиции (буквы) вперед.**

**3 уровень**

**С. Дополнить полученную программу шифром Квadrата Полибия [6x6], расположив буквы по столбцам.**

*Вариант 5.*

**Составить программу, которая шифрует сообщение Support for Unicode in file names следующим образом:**

**1 уровень**

**А. Составить программу, которая используя шифр Цезаря заменяет каждую букву в сообщении другой буквой этого же алфавита, отстоящей в алфавите от данной буквы на 1 позицию (буквы) назад.**

**2 уровень**

**В. Дополнить полученную программу шифром Атбаш**

**3 уровень**

**С. Дополнить полученную программу шифром Квadrата Полибия [6x6], расположив буквы построчно.**

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают

на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

## **10. Контрольные вопросы**

1. Алгоритм закрытия информации шифром Цезаря.
2. Почему шифр Цезаря называется циклическим ?
3. Алгоритм закрытия информации шифром Атбаш.
4. Алгоритм закрытия информации Квадратом Полибия.
5. Показатели криптостойкости?
6. Что называется криптостойкостью?

## **11. Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А.И., Самсонов Б.Б., Кречет Т.В., Плохов Е.М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И. Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М.: ИЛ, 2015. – 512 с.

## Практическое занятие № 4. Доктрина ИБ РФ

### 1. Цель работы

Целью работы является овладение практическими навыками составления шифра вручную, разработки и программирования вычислительного процесса шифрования методом полиалфавитной подстановки.

### 2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

### 3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

#### ***Программа лабораторной работы***

25. Описание лабораторной работы. 35 мин

26. Задание. 35 мин

Проверка выполнения лабораторной работы 10 мин

Заключительная часть 3 мин

### 4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### ***4.1. Требования безопасности перед началом работ***

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов.
- В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### ***4.2. Требования безопасности во время работы***

- Выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### ***4.3. Требования безопасности по окончании работы***

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

## 5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

## 6. Программное обеспечение

Программное обеспечение для выполнения лабораторной работы ОС Windows 2000 и выше, либо XP; Turbo Pascal 7; Borland Delphi 7; Borland C++.

## 7. Краткие теоретические сведения

**Аффинные криптосистемы.** В таких системах за счет математических преобразований буквы, заменяющие открытый текст, относительно хаотично перемешаны.

Буквы алфавита нумеруются числами, например от 0 до 26. Затем каждая буква открытого текста заменяется буквой, порядковый номер в алфавите которой вычисляется с помощью линейного уравнения.

Аффинные криптосистемы задаются при помощи двух чисел:  $a$  и  $b$ . Для английского алфавита эти числа выбираются из условия  $a \geq 0$ ,  $b \leq 25$ . Причем числа  $a$  и  $\gamma=26$  должны быть взаимно простыми. Если это условие не будет выполняться, то две разные буквы могут отобразиться в одну. Каждый код (номер в алфавите) криптограммы определяется по коду буквы открытого текста  $\mu$  по следующему правилу. Вначале вычисляется число  $\alpha = a * \mu + b$ , а затем выполняется операция целочисленного деления числа  $\alpha$  на число  $\gamma = 26$ . Математически это записывается так:

$\alpha = \beta(\text{mod}(\gamma))$ , что означает:  $\beta$  является остатком от целочисленного деления  $\alpha$  на  $\gamma$ . Число  $\beta$  используется в качестве кода буквы шифрограммы.

Повысить криптостойкость позволяют **шифры многоалфавитной, или многозначной, замены.** В таких шифрах каждому символу открытого алфавита ставят в соответствие не один, а несколько символов шифровки.

## 8. Задания

### Варианты к лабораторной работе №15.

(ваш номер по журналу соответствует номеру варианта)

#### Вариант 1.

Составить программу, которая шифрует сообщение \*(вариант задания выдается преподавателем) следующим образом:

#### 1 уровень

**А. Составить программу, которая использует Аффинные криптосистемы**

$a=3$  и  $b=5$

#### 2 уровень

**В. Дополнить полученную программу шифром по Таблице Виженера:**

#### 3 уровень

**С. Дополнить полученную программу шифром Квадрата Полибия [6x6], расположив буквы построчно.**

#### Вариант 2.

Составить программу, которая шифрует сообщение Make your own settings by modifying or creating a KBD file следующим образом:

#### 1 уровень

**А. Составить программу шифром по Таблице Виженера.**

#### 2 уровень

**В. Дополнить полученную программу, которая использует Аффинные криптосистемы  $a=5$  и  $b=3$**

#### 3 уровень

**С. Дополнить полученную программу шифром Квадрата Бьюфорта, расположив буквы построчно.**

#### Вариант 3.

**Составить программу , которая шифрует сообщение** Use Script to assign a keystroke to a script command or function следующим образом:

**1 уровень**

**А. Составить программу шифром Квadrата Бьюфорта.**

**2 уровень**

**В. Дополнить полученную программу, которая использует Аффинные криптосистемы  $a=5$  и  $v=7$**

**3 уровень**

**С. Дополнить полученную программу шифром по Таблице Виженера, расположив буквы построчно.**

**Вариант 4.**

**Составить программу , которая шифрует сообщение** You can map your keyboard the following ways следующим образом:

**1 уровень**

**А. Составить программу, которая шифрует сообщение Аффинными криптосистемами  $a=3$  и  $v=7$**

**2 уровень**

**В. Дополнить полученную программу, которая шифрует сообщение по Таблице Бьюфорта**

**3 уровень**

**С. Дополнить полученную программу, которая шифрует сообщение Квадратом Полибия [6x6]**

**Вариант 5.**

**Составить программу , которая шифрует сообщение** In the IDE, the keystroke repeat rate defaults to OFF следующим образом:

**1 уровень**

**А. Составить программу, которая шифрует сообщение Аффинными криптосистемами  $a=7$  и  $v=3$**

**2 уровень**

**В. Дополнить полученную программу, которая шифрует сообщение Таблицей Виженера**

**3 уровень**

**С. Дополнить полученную программу, которая шифрует сообщение квадратом Полибия [6x6]**

## **9. Содержание отчета о лабораторной работе**

По результатам выполнения лабораторной работы студенты оформляют и сдают на проверку отчет. Отчет по выполнению лабораторной работы должен быть сдан на проверку в письменной форме, либо в форме электронного документа. Отчет оформляется в соответствии с общими правилами оформления квалификационных работ и должен содержать:

- титульный лист;
- введение;
- основную часть;
- заключение.

Титульный лист содержит наименование вуза, наименование специальности, наименование дисциплины, наименование работы, ФИО студента, дату выполнения работы, дату защиты работы, оценку.

Во введении указывается цель работы и основные пункты задания.

В основной части приводится ход выполнения работы, расчеты, графики.

При необходимости могут быть приведены основные теоретические сведения.

В заключении указываются выводы по работе, производится теоретическое

обоснование полученных результатов и приводятся ответы на контрольные вопросы

Результаты выполненной лабораторной работы защищаются каждым студентом в индивидуальном порядке в форме беседы.

#### **10. Контрольные вопросы**

1. Алгоритм закрытия информации Квадратом Бьюфорта.
2. Алгоритм закрытия информации Таблица Виженера.
3. Отличие шифрование Квадратом Бьюфорта от Таблицы Виженера.
4. Алгоритм закрытия информации Квадратом Полибия.
5. Шифрование аффинными криптосистемами.
6. Эффективное средство повышения криптостойкости шифров?
7. Формула стойкости комбинированного шифрования.

## Практическое занятие № 5. ГОСТ Р 53114-2008

Цель занятия: приобретение практических навыков в определении классификационных индексов УДК и МПК для поиска научно-технической информации

1 Основные классификационные системы в области библиографии и научно-технической информации

Практика систематизации документов (в целях их хранения и поиска) опирается на специальные классификационные системы – библиотечно- библиографические классификации и рубрикаторы.

На основании признаков содержания, формы издания, читательского назначения и т.п. документы упорядочиваются по классам, подклассам и более дробным делениям, следующим в логической последовательности и соподчинении. Классы и отношения между классами обозначаются с помощью нотации – совокупности символов (цифр, букв, знаков) и правил их применения. Так классификационная система находит материальное воплощение в виде издаваемых и переиздаваемых классификационных таблиц.

Иерархия этих систем (основных делений) основывается на классификации наук.

Библиотечно-библиографические классификации относятся к информационно-поисковым языкам.

Существуют национальные и международные классификационные системы. Наиболее распространенными международными являются:

- Универсальная десятичная классификация (УДК)
- Международная патентная классификация (МПК)
- Библиотечно-библиографическая классификация (ББК) Государственный рубрикатор (ГРНТИ)

- Десятичная классификация Дьюи (ДКД)

- Универсальная десятичная классификация (УДК)

Универсальная десятичная классификация (УДК) была создана в 1895-1905 годах для Международного библиографического института (МБИ) бельгийскими учеными Полем Отле (1868—1944) и Анри Лафонтеном (1854-1943). В 1905 году в Брюсселе на французском языке вышло первое сводное издание таблиц УДК – «Руководство к универсальному библиографическому репертуару» (“Manuel du repertoire bibliographique universel”). Современное название УДК получила в 1927 году.

Она разработана на основе Десятичной классификации Дьюи (П. Отле и А. Лафонтен превратили перечислительную систему М. Дьюи в комбинационную, снабдив ее рядом таблиц определителей), но является значительно отличающейся от нее самостоятельной классификацией. Объем изданий УДК постоянно наращивался, и в настоящее время её эталон содержит свыше 220 тыс. делений.

Десятичной она называется потому, что в основу ее структуры положен принцип десятичных дробей. Вся сумма человеческих знаний разделена на 10 основных классов, каждый из которых дробится на более мелкие подклассы, те в свою очередь - на более мелкие и конкретные деления и т. д. Индексы классов обозначаются арабскими цифрами от 0 до 9. Чем конкретнее, уже тема индексируемого документа, тем большего уровня подробности присваивается ему классификационный индекс. Наглядно это выражается в большей длине индекса.

Ныне УДК - вторая по распространенности в мире и первая по объему содержания библиотечно-библиографическая классификация. Она переведена на 20 языков, используется в 36-ти странах, и в 21-й из них признается классификацией национальной библиографии. Таблицы УДК многократно переиздавались, обогащаясь новыми изменениями и дополнениями. В 1963-1966 годах вышло в свет первое издание таблиц УДК на русском языке, их последним законченным изданием было 3-е издание (в 1982-1987 годах).

УДК поддерживалась и распространялась МБИ (1895-1931), Международным

институтом по документации (1931-1938) и Международной федерацией по документации (1938-1990). С 1991 года образован Консорциум УДК (УДКК), дирекция которого находится в Гааге (Нидерланды). Она продает лицензии на право перевода, издания и распространения УДК. С 1993 года дирекция УДКК распространяет эталон УДК в машиночитаемой форме - Master Reference File.

С 1962 года УДК является единой классификационной системой для отечественных технических библиотек и органов научно-технической информации. С 1963 года в научно-технических издательствах и редакциях научно-технических журналов введено обязательное индексирование всех публикаций по таблицам УДК.

Исключительным правом на перевод, издание и распространение УДК на русском языке обладает Всероссийский институт научной и технической информации (ВИНИТИ).

Индекс УДК – обязательный элемент выходных сведений издания: ГОСТ 7.4-95 требует ставить его в верхнем левом углу оборота титульного листа.

Справочник по УДК на сайте исследовательской группы Центра новых информационных технологий Иркутского государственного университета. Содержит описание 126441 кода УДК.

Предисловие к официальному изданию УДК на сайте ГСНТИ.

Международная патентная классификация (МПК)

Информация о патентах позволяет проследить историю изобретений с момента выдачи первого патента в 1617 году до наших дней по любой отрасли знания, выявить современное состояние и направление развития технической мысли в различных областях знания. Основное практическое назначение – облегчение поиска аналогичных технических решений, без чего невозможно проведение патентной экспертизы. Для упорядочения патентной информации была создана специальная классификация.

В соответствии с положениями Европейской конвенции 1954 года Международная (Европейская) классификация патентов на изобретения была опубликована в 1968 году, а после подписания Страсбургского соглашения 24 марта 1971 года считается первой редакцией МПК. В России (бывшем СССР) Международная классификация изобретений введена с 1970 года.

МПК охватывает все отрасли знания, объекты которых могут быть защищены авторскими правами. Она представляет собой специальную линейную систему иерархического типа, построенную по функционально-отраслевому принципу. По своей структуре МПК представляет компромиссное решение между отраслевым принципом классификации и функциональным принципом - по функциям и применению предлагаемого изобретения. В этом ярко проявляется ее технико-прикладной характер.

Главную таблицу МПК составляют 8 разделов:

A Удовлетворение жизненных потребностей человека

B Различные технологические процессы; транспортирование

C Химия; металлургия

D Текстиль; бумага

E Строительство; Горное дело

F Механика; освещение; отопление; двигатели и насосы; оружие; боеприпасы; взрывные работы

G Физика

H Электричество

Внутри каждого раздела предусматривается возможность создания 5 подразделов, а в каждом подразделе - 20 классов. Следовательно, в составе одного раздела может быть образовано 100 классов, а в 8 разделах 800 классов.

Для облегчения ориентации специалистов в МПК разработан алфавитно-предметный указатель, в котором все технические термины расположены в алфавитном порядке.

Новая (восьмая) редакция Международной патентной классификации, вступившая

в силу 1-го января 2006 года, разделена на два уровня – базовый (укрупненный) и расширенный (более подробный). Базовый уровень включает в себя только наиболее крупные рубрики МПК: разделы, классы, подклассы и основные группы (около 18 000 рубрик). Расширенный уровень, включающий в себя полностью рубрики базового уровня, представляет собой его детализацию, включая соответственно все подгруппы МПК.

Текст МПК на русском языке издает Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент).

Библиотечно-библиографическая классификация (ББК)

Национальная классификационная система России, наиболее распространенная в ее библиотеках.

Разрабатывалась с 30-х годов XX века на протяжении нескольких десятилетий. Первое издание таблиц ББК для научных библиотек в 25 выпусках (30 книгах) было опубликовано 1960— 1968 годах. На основе полной версии созданы варианты для научных, массовых, детских библиотек и др.

Таблицы ББК достаточно глубоко отражали уровень развития классификационной теории своего времени, обладали комбинационными свойствами, развитой системой общих и специальных типовых делений. ББК получила признание как одна из крупнейших универсальных систем. В 1981 году группе разработчиков ББК была присуждена Государственная премия СССР в области науки.

Изменения в научных знаниях и обществе потребовали серьезной переработки ББК. В 2001 году начат выпуск Средних таблиц, которые сейчас являются основными.

ББК используется как основная библиотечно-библиографическая классификация в крупных универсальных, публичных библиотеках, а также в библиотеках гуманитарного профиля.

Функции федерального межведомственного координационного центра, ответственного за издание и использование ББК, возложены на Научно-исследовательский центр развития ББК (НИЦ ББК), работающий в Российской государственной библиотеке. Официальный издатель ББК – ООО «Издательство "ЛИБЕРЕЯ"».

ГОСТ 7.4-95 включает индекс ББК в число основных элементов выходных сведений, определяя ему место на обороте титульного листа издания вверху слева отдельной строкой под индексом УДК.

Основные деления ББК

Государственный рубрикатор (ГРНТИ)

Помимо собственно библиотечно-библиографических классификаций для систематизации документов и поиска в базах данных в России и государствах СНГ широко применяется Рубрикатор научно-технической информации. В основном он используется учреждениями НТИ. На основе ГРНТИ построена система локальных (отраслевых, тематических, проблемных) рубрикаторов.

ГРНТИ разработан в соответствии с " Положением о лингвистическом обеспечении Государственной автоматизированной системы научно- технической информации» (1986 год) и представляет собой универсальную классификацию областей знания и практики.

Индексы в ГРНТИ принято называть кодами. Коды начальных делений областей знаний состоят из пары цифр от 00 до 90 (первый подуровень). Дальнейшая детализация возможна до 3-го подуровня, код которого состоит из 6-ти цифр, разделенных на пары точками. (Например, 29.31.15 Излучение и волновая оптика.)

В своей кодовой части классификатор связан с Номенклатурой специальностей научных работников. (См. Базу данных «ГРНТИ» на сайте ФГУ "Научно-исследовательский институт - Республиканский исследовательский научно-консультационный центр экспертизы").

Государственный рубрикатор научно-технической информации на сайте ГСНТИ.

Гипертекстовый вариант рубрикатора на сайте ГПНТБ СО РАН.

Десятичная классификация Дьюи (ДКД)

Самой старинной и самой распространенной в мире универсальной библиотечно-библиографической классификацией является Десятичная классификация Дьюи, названная в честь ее создателя – американского библиотекаря Мелвила Дьюи (1857—1931). Он разработал ее для систематизированной расстановки книг в публичных библиотеках США. Классификация Дьюи послужила основой при разработке УДК. Первое издание таблиц ДКД вышло в 1876 году.

М. Дьюи, сторонник и пропагандист метрической системы, избрал принцип деления всей совокупности знаний на десять основных классов с последующим их делением. Определяющей явилась форма (десятичная индексация), ей подчинено содержание (классификация). Дьюи отрицал связь с классификацией наук и как основной принцип называл удобство и легкость: арабские цифры понятны во всем мире, и таким образом система не зависит от языка. Классы имели обозначение от 000 до 900.

УДК и классификация Дьюи едины в своей основе, совпадают для первых трех ступеней классификации (трехзначных индексов), т.е. для 1000 рубрик, но расходятся в дальнейших делениях, их детализации и методике составления индексов. При жизни автора ДКД выдержала 12 изданий, постоянно наращивался объем таблиц. М. Дьюи в 1922 году передал авторские права на ДКД Lake Placid Club Educational Foundation. Сейчас авторские права на ДКД принадлежат OCLC Forest Press (издательству корпорации Online Computer Library Center). Ведение ДКД с 1923 года осуществляется редакцией, находящейся в Библиотеке Конгресса США.

Ныне ДКД применяется в 135 странах, в 60-ти из них – в национальных библиографиях. Классификация Дьюи активно используется в зарубежных библиографических базах данных и электронных каталогах библиотек. Её популярности способствуют ясность самой классификационной системы и относительная компактность таблиц. В России использование ДКД разрешено ГОСТом 7.59 - 2003. Десятичная классификация Дьюи (ДКД) в переводе на русский язык на сайте ГПНТБ. Навигация с помощью УДК, ББК и ГРНТИ по базам данных и каталогам ГПНТБ.

## Практическое занятие № 6. ГОСТ Р ИСО/МЭК 27004-2021

Патентный поиск - это процесс отбора соответствующих запросу документов или сведений по одному или нескольким признакам из массива патентных документов или данных, при этом осуществляется процесс поиска из множества документов и текстов только тех, которые соответствуют теме или предмету запроса.

Патентный поиск осуществляется посредством информационно-поисковой системы и выполняется вручную или с использованием соответствующих компьютерных программ, а так же с привлечением соответствующих экспертов.

Предмет поиска определяют исходя из конкретных задач патентных исследований категории объекта (устройство, способ, вещество), а так же из того, какие его элементы, параметры, свойства и другие характеристики предполагается исследовать.

При патентном поиске сравниваются выражения смыслового содержания информационного запроса и содержания документа.

Для оценки результатов поиска создаются определенные правила-критерии соответствия, устанавливающие, при какой степени формального совпадения поискового образа документа с поисковым предписанием текст следует считать отвечающим информационному запросу. Зачем проводить патентный поиск

Среди основных целей патентного поиска можно выделить:

- Проверка уникальности изобретения
- Определение особенностей нового продукта
- Определение других сфер применения нового продукта
- Поиск изобретателей или компании, получивших патенты на изобретения в той же области
- Поиск патентов на какой-либо продукт
- Найти последние новинки в исследуемой области
- Поиск патентов на изобретения в смежных областях
- Определение состояния исследований в интересующем технологическом поле
- Выяснить, не посягает ли ваше изобретение на чужую интеллектуальную собственность
- Получить информацию по конкретной компании или состоянию сектора рынка в целом
- Получить информацию о частных лицах, имеющих патенты на схожие изобретения
- Поиск потенциальных лицензиаров
- Поиск дополнительных информационных материалов

Патентный поиск является трудоёмким, но необходимым мероприятием. Он необходим не только лицам или организациям, желающим запатентовать изобретение, но и промышленным предприятиям, желающим это изобретение использовать.

Например, использование запатентованных изобретений другими юридическими и физическими лицами приводит к огромным штрафам и возможным разорением предприятий.

Существует два способа проведения патентного поиска: поручить его специализирующейся на этом фирме или проводить самому, в последнем случае вся ответственность за результат будет лежать только на вас.

Патентный поиск является трудоёмким и недешёвым процессом, кроме того, результата напрямую зависит от добросовестности и квалификации экспертов, его осуществляющих.

Последовательность самостоятельного проведения патентного поиска:

- Подготовить полное описание изобретения;
- Вести подробные записи на всём протяжении проведения патентного поиска;

- Изучить информационные источники, не связанные с патентованием, но имеющие отношение к области применения вашего изобретения;
- Провести небольшое исследование рынка для выявления изобретений, схожих с вашим.

Первичный патентный поиск может быть проведён через сеть Интернет. Кроме того, могут потребоваться:

- сотрудники, эксперты, знающие суть патентного поиска и обученные работе с соответствующими БД;
- печатные источники, материалы, каталоги и т.п. по патентам;
- патентные БД;
- дополнительная научно-техническая информация, книги, материалы.

По законодательству Российской Федерации, патентный поверенный – гражданин, которому в соответствии с Патентным законом Российской Федерации, Законом Российской Федерации "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров" и "Положением о патентных поверенных" предоставлено право на представительство физических и юридических лиц перед Федеральной службой по интеллектуальной собственности, патентам и товарным знакам (РОСПАТЕНТ) и организациями, входящими в единую государственную патентную службу.

В качестве патентного поверенного, согласно Положению о патентных поверенных, может быть аттестован и зарегистрирован гражданин Российской Федерации, который имеет постоянное место жительства в Российской Федерации, высшее образование и не менее чем 4-х летний опыт практической работы в области охраны промышленной собственности или профессионального правового представительства (адвокат или иное лицо, получившее разрешение на занятие правоприменительной деятельностью); обладает знанием законодательных и иных нормативных актов Российской Федерации, международных договоров и соглашений, необходимых для осуществления деятельности по защите прав на объекты промышленной собственности, в объеме, определяемом Роспатентом, и соответствующими навыками их практического применения, подтвержденным результатами квалификационного экзамена.

### **Задания**

1. Расшифровать индекс ББК и УДК для учебного пособия Тоискин В.С., Жук А.П. Системы документальной электросвязи. –М.: Инфра-М, 2011.
2. Найти описание изобретения из области информационных систем и технологий, определить и расшифровать для него индекс МПК.

### **Литература:**

1. Гиляревский Р.С. Рубрикатор как инструмент информационной навигации / Р.С. Гиляревский, А.В. Шапкин, В.Н. Белоозеров. – СПб.: Профессия, 2014. – 352 с.: табл. - Прил.: с. 338 - 350. - ISBN 978-5-93913-168-1.
2. Паршукова Г.Б. Методика поиска профессиональной информации: Учебно-методическое пособие для студентов высших учебных заведений / Паршукова Галина Борисовна. - СПб. : Профессия, 2013. – 224 с.:

## Практическое занятие № 7. Стандарт банка России СТО БР ИББС-1.0-2014

**Право** – это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Законодательство Российской Федерации представляет собой совокупность Конституции и принимаемых в соответствии с ней законов и подзаконных актов.

Внутреннее строение системы права РФ можно представить в вертикальном и горизонтальном срезам.

**Вертикальное строение права** – совокупность элементов, включающих: отрасль, подотрасль, институт, субинститут и правовое предписание.

**Горизонтальное строение права** позволяет увидеть все отрасли, его составляющие. Если их классифицировать, то можно выделить две группы отраслей.

В первую группу объединяются **регулятивные отрасли права**, т. е. отрасли, в которых основной упор делается на установление прав и обязанностей участников правоотношений.

Вторую группу отраслей составляют **охранительные отрасли права**, основной задачей которых является защита правоотношений.

**Структура правоотношений и виды юридической ответственности**  
**Правоотношение** – это такое общественное отношение, в котором стороны

связаны между собой взаимными юридическими правами и обязанностями, охраняемыми государством. Правоотношение есть та мера внешней свободы, которая предоставляется его участникам нормами позитивного (писаного) права.

*Структура правового отношения имеет четыре необходимых элемента: субъекты, объект, право и обязанность:*

**Субъекты правоотношений** – это отдельные индивиды и организации, которые в соответствии с нормами права являются носителями юридических прав и обязанностей. В реальной жизни не все индивиды и организации могут быть субъектами правоотношений, например, малолетние дети, душевнобольные, организации, прекратившие свое существование, фактически не могут участвовать в правоотношениях по понятным причинам.

Мера участия субъектов в правовых отношениях определяется их правоспособностью и дееспособностью.

**Правоспособность** – это способность субъекта иметь юридические права и нести юридические обязанности. Она начинается с момента рождения индивида и прекращается смертью. Однако, чтобы стать реальным участником правоотношения, правоспособный субъект должен быть дееспособным.

**Дееспособность** – это способность субъекта самостоятельно, своими действиями осуществлять юридические права и нести обязанности.

1. **Объект правоотношений** – это то, на что воздействует правоотношение. Объектом правоотношения является фактическое поведение его участников. В соответствии с содержанием субъективного права и юридической обязанности участники правоотношения строят свое поведение. Вступая в правоотношения, субъекты удовлетворяют определенные материальные, духовные и иные потребности (например, приобретают вещи, пользуются авторскими правами, правами изобретателя). Объектом правоотношений выступает поведение людей, которое может быть различным по содержанию.

2. **Субъективное право** – это предоставляемая и охраняемая государством возможность (свобода) субъекта по своему усмотрению удовлетворять те интересы, которые предусмотрены позитивным правом. Право, принадлежащее субъекту, называется субъективным потому, что только от воли субъекта зависит, как им

распорядиться. Это возможность не произвольная, а правовая, устанавливающая меру дозволенного поведения.

3. **Юридическая обязанность** – это предусмотренная законодательством и охраняемая государством необходимость должного поведения участника правового отношения в интересах управомоченного субъекта (индивида, организации, государства в целом). Если содержание субъективного права образует мера дозволенного поведения, то содержание обязанности – мера должного, необходимого поведения в правоотношении.

**Юридическая ответственность** – это применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера. Фактическим основанием для юридической ответственности является правонарушение. Лицо может быть привлечено к ответственности только при наличии в его действии всех элементов состава правонарушения.

*Состав правонарушения состоит из четырех составляющих:*

- **объект правонарушения** – область общественных отношений, регулируемых и охраняемых правом, в котором произошло деяние и (или) которой данным деянием причинен вред;

- **объективная сторона** – характеристика деяния, способа его совершения (группой, с применением оружия, систематически, повторно), обстоятельств (во время военных действий, стихийных бедствий и т. п.);

- **субъект** – лицо, которое совершило правонарушение, характеристика правонарушителя;

- **субъективная сторона** – форма вины (умысел или неосторожность).

Само по себе правонарушение не порождает автоматически возникновения ответственности, а является лишь основанием для такого применения. Для реального же осуществления юридической ответственности необходим **правоприменительный акт** – решение компетентного органа, который возлагает юридическую ответственность, устанавливает объем и форму принудительных мер к конкретному лицу. Это может быть приговор суда, приказ администрации и т. п. Наибольшее распространение получило деление юридической ответственности по отраслевому признаку. По данному основанию различают ответственность *уголовную, административно-правовую, гражданско-правовую, дисциплинарную и материальную.*

**Уголовная ответственность** наступает за совершение преступлений и в отличие от других видов ответственности устанавливается только уголовным законом. Никакие иные нормативные акты не могут определять общественно опасные деяния как преступные и устанавливать за них меры ответственности. В Российской Федерации исчерпывающий перечень преступлений зафиксирован в Уголовном кодексе. Порядок привлечения к уголовной ответственности регламентируется Уголовно-процессуальным кодексом. Полномочиями привлечения к уголовной ответственности обладает только суд.

**Административно-правовая ответственность** наступает за совершение административных проступков, предусмотренных Кодексом об административных правонарушениях. Кроме того, этот вид ответственности может устанавливаться указами Президента Российской Федерации, постановлениями Правительства Российской Федерации и нормативными актами субъектов Федерации. Дела об административных правонарушениях рассматриваются компетентными органами государственной власти, круг которых закреплен в кодексе. Меры административного принуждения – предупреждение, штраф, лишение специального права, административный арест.

**Гражданско-правовая ответственность** наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. Ее сущность состоит в принуждении лица нести отрицательные имущественные последствия. Полное возмещение вреда основной принцип гражданско-правовой ответственности (статья 1064 ГК). Возмещение убытков в некоторых случаях

дополняется штрафными санкциями, например, выплатой неустойки. **Дисциплинарная ответственность** возникает вследствие совершения дисциплинарных проступков. Привлекать к дисциплинарной ответственности может руководитель, осуществляющий распорядительно-дисциплинарную власть над конкретным работником. Меры дисциплинарной ответственности – выговор, строгий выговор, отстранение от занимаемой должности и т. п.

**Материальная ответственность** рабочих и служащих за ущерб, нанесенный предприятию, учреждению, заключается в необходимости возместить ущерб в порядке, установленном законом. Основанием этого вида ответственности является нанесение ущерба во время работы предприятию, с которым работник находится в трудовых отношениях. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

**Информационное законодательство** – это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предметом правового регулирования в информационной сфере являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация права на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают гарантии, обязанности, механизмы защиты и ответственность.

*Информационное законодательство имеет вертикальную (по видам правовых актов) и горизонтальную (по отраслям законодательства) структуру.* Вертикальная структура строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов.

Структура информационного законодательства как комплексной отрасли включает в себя:

- Международные акты информационного законодательства.
- Информационно-правовые нормы Конституции РФ.
- Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.
- Отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

Совокупность вышеперечисленных документов составляет правовую базу, обеспечивающую нормативное регулирование процессов информационного обмена, в том числе и защиту информации.

Информация имеет ряд особенностей, отличающих ее от других видов товаров:

- нематериальность (идеальность) информации;
- информационный продукт подвергается только моральному износу;
- информация находится на материальном носителе;
- информация не исчезает при потреблении и может быть использована многократно;
- производство информации требует значительных затрат по сравнению с затратами на тиражирование;
- при копировании количество информации не изменяется, а цена снижается.

Основные определения в области информационного права:

**Информация** – это сведения о лицах, предметах, фактах, явлениях, процессах независимо от формы их представления.

**Документированная информация** – это зафиксированная на материальном

носителе информации с реквизитами, позволяющими ее идентифицировать.

**Объект правоотношений** – это то, на что воздействуют правоотношения.

**Субъект правоотношений** – предоставленная и охраняемая государством возможность субъекта по своему усмотрению удовлетворять потребности, предусмотренные позитивным правом.

**Юридическая ответственность** – применение предусмотренных санкций, юридических норм, мер государственного принуждения.

**Юридические обязанности** – предусмотренная законодательством и охраняемая государством необходимость должностного поведения участника правоотношений.

*Правовые принципы защиты информации:*

- полнота правового регулирования;
- принципы единства нормативно-правовой базы;
- непротиворечивость законодательной базе;
- принцип соблюдения рациональных пропорций между правовыми и технико-юридическими нормами;
- нормативно-правовые акты должны предусматривать развернутую защиту прав граждан.

**Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

**Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

**Контрольные вопросы**

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.

## **Практическое занятие № 8. ГОСТ Р ИСО/МЭК 15408-1-2012 Введение и общая модель**

В настоящее время с учетом сложившейся практики обеспечения информационной безопасности принято выделять следующие направления защиты информации:

- правовая защита – это специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

Правовое обеспечение информационной безопасности любой страны содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения информационной безопасности составляют Конституция РФ, Законы РФ, Кодексы, Указы и другие нормативные акты, регулирующие отношения в области информации.

Правовая защита информации как ресурса признана на международном уровне и определяется межгосударственными договорами, конвенциями, декларациями, реализуется правовыми механизмами защиты патентных и авторских прав.

В реализации государственной политики в сфере информатизации участвуют следующие структуры власти:

- Президент Российской Федерации;
- Совет Федерации;
- Государственная дума Федерального собрания Российской Федерации;
- Правительство Российской Федерации;
- Совет безопасности Российской Федерации;
- федеральные органы исполнительной власти;
- органы государственной власти Российской Федерации;
- органы местного самоуправления.

Совет безопасности Российской Федерации рассматривает наиболее важные вопросы, связанные с безопасностью Российской Федерации в современном мире, в том числе и вопросы информационной безопасности.

Структуру аппарата системы безопасности Российской Федерации составляют:

- Управление информационной безопасности и стратегического прогнозирования;
- Межведомственная комиссия Совета безопасности Российской Федерации по информационной безопасности.

В Государственной думе Российской Федерации функционируют:

- Комитет по информационной политике и связи;
- Комитет по безопасности, составной частью которого является комитет по информационной безопасности.

На внутригосударственном уровне правовая защита регулируется государственными и ведомственными актами. Государственными актами являются Конституция РФ, законы РФ, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями.

**Информационное законодательство** – совокупность норм права, регулирующих общественные отношения в информационной среде. Предметом правового регулирования в информационной среде являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация прав граждан на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

Таким образом, законодательство по информационной безопасности является неотъемлемой частью всей системы законов Российской Федерации.

### **Федеральный закон «Об информации, информационных технологиях и о защите информации»**

Со дня вступления в силу Федерального закона от 27 июля 2006 года

№ 149-ФЗ «Об информации, информационных технологиях и о защите информации» утратили силу Федеральный закон от 20 февраля 1995 года

№ 24-ФЗ «Об информации, информатизации и защите информации» и Федеральный закон от 04 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене».

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

*Термины, используемые в законе, их определения*

**Информация** – сведения (сообщения, данные) независимо от формы их представления.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Доступ к информации** – возможность получения информации и ее использования.

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**Распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

**Электронное сообщение** – информация, переданная или полученная

пользователем информационно-телекоммуникационной сети.

**Документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель.

**Оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

### **Доктрина информационной безопасности Российской Федерации**

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Важнейшие задачи обеспечения информационной безопасности Российской Федерации:

1. Противодействие угрозе развязывания противоборства в информационной сфере.
2. Реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности.
3. Совершенствование и защита отечественной информационной структуры, интеграция России в мировое информационное пространство.

Доктрина информационной безопасности РФ развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для:

- 1) формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- 2) подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- 3) разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под *информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы *личности* в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы *общества* в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы *государства* в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

*Первая* составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

*Вторая* составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

*Третья* составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

*Четвертая* составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

## **Федеральный закон «О техническом регулировании»**

Федеральный закон «О техническом регулировании» от 27 декабря 2002 года № 184-ФЗ регулирует отношения, возникающие при:

- 1) разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- 2) разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- 3) оценке соответствия продукции установленным законодательством требованиям.

Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

Действие закона не распространяется на государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

*Термины, используемые в законе, их определения*

**Аккредитация** – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

**Безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации** – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

**Декларирование соответствия** – форма подтверждения соответствия продукции требованиям технических регламентов.

**Декларация о соответствии** – документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

**Заявитель** – физическое или юридическое лицо, осуществляющее обязательное подтверждение соответствия.

**Знак обращения на рынке** – обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов.

**Знак соответствия** – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

**Идентификация продукции** – установление тождественности характеристик продукции ее существенным признакам.

**Контроль (надзор) за соблюдением требований технических регламентов** – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки.

**Международный стандарт** – стандарт, принятый международной организацией.

**Национальный стандарт** – стандарт, утвержденный национальным органом Российской Федерации по стандартизации.

**Орган по сертификации** – юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации.

**Оценка соответствия** – прямое или косвенное определение соблюдения требований, предъявляемых к объекту.

**Подтверждение соответствия** – документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

**Продукция** – результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях.

**Риск** – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда.

**Сертификация** – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

**Сертификат соответствия** – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

**Система сертификации** – совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом.

**Стандарт** – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

**Стандартизация** – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

**Техническое регулирование** – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.

**Технический регламент** – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

**Форма подтверждения соответствия** – определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или

условиям договоров.

### **Закон Российской Федерации «О безопасности»**

Закон РФ «О безопасности» от 5 марта 1992 года № 2446-1 закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

*Термины, используемые в законе, их определения*

**Безопасность** – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся:

- 1) личность – ее права и свободы;
- 2) общество – его материальные и духовные ценности;
- 3) государство – его конституционный строй, суверенитет и территориальная целостность.

**Субъект обеспечения безопасности** – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

**Угроза безопасности** – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

*Принципы обеспечения безопасности*

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов,

обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

### **Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

### **Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

### **Контрольные вопросы**

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.
12. Назовите и охарактеризуйте направления защиты информации.

## **Практическое занятие № 9. ГОСТ Р ИСО/МЭК 15408-2-2013. Функциональные компоненты безопасности**

Информация ограниченного доступа, включающая государственную тайну и конфиденциальную информацию, имеет особую важность для государства и общества. В той или иной мере правовые институты тайн есть во всех развитых демократиях мира.

Опыт показывает, что с ростом значимости информации в общей системе государственного и муниципального управления (ГМУ) наиболее важным элементом с годами становится достижение превосходства в информационной сфере. Этим обстоятельством и определяется существование институтов тайн, создающих возможность для ГМУ проводить независимую информационную политику, защищать свои интересы, осуществлять управление обществом, регионом, муниципальным образованием.

Система секретной и конфиденциальной информации – наиболее сильное звено регулирования общественных отношений в информационной сфере. Вследствие возможного существенного ущерба от ее разглашения информация ограниченного доступа занимает особое место в системе управления. Институт тайн – важнейший элемент системы государственного и муниципального управления.

Основу нормативно-правового обеспечения защиты информации ограниченного доступа в России составляют Конституция РФ, законы «О безопасности» от 5 марта 1992 года № 2446-1, «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ и другие.

В условиях сегодняшней России (расширяющееся международное сотрудничество, либерализация экономики, увеличение количества объектов иностранных инспекций, свободное перемещение иностранцев по большей части территории страны, внедрение компьютерной техники иностранного производства) значительной возросла опасность утечки сведений, составляющих информацию ограниченного доступа. Вследствие этого важнейшими задачами органов ГМУ являются обеспечение необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями на ее распространение, а также развитие и защита государственного и муниципального ресурса.

В действующем законодательстве РФ встречается упоминание более чем о 30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная, тайна следствия, связи, почтовых отправок и другие).

Приведем наиболее важные определения в этой области и дадим необходимую классификацию.

**Защищаемой информацией** называется информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации относится информация с ограниченным доступом, а также открытая информация, представляющая ценность.

**Информацией с ограниченным доступом** называется информация, доступ к которой ограничен в соответствии с Законом с целью защиты прав и законных интересов субъектов права на тайну. Она состоит из государственной тайны и конфиденциальной информации.

Конфиденциальная информация в свою очередь включает множество видов тайны, которые сводятся к шести основным видам:

- 1) персональные данные;
- 2) тайна следствия и судопроизводства;

- 3) служебная тайна;
- 4) профессиональная тайна;
- 5) коммерческая тайна;
- 6) тайна изобретения, полезной модели и промышленного образца.

Особую важность с точки зрения безопасности государства имеет защита информации, составляющей государственную и служебную тайну.

**Государственная тайна** – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

**Конфиденциальная информация** – информация, не составляющая государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

**Персональные данные** – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

**Тайна следствия и судопроизводства** – защищаемая по закону конфиденциальная информация, ставшая известной в органах следствия и судопроизводства только на законных основаниях в ходе следствия и судопроизводства, а также служебная информация о деятельности органов следствия и судопроизводства, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

**Служебная тайна** – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

**Профессиональная тайна** – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, банковская тайна и т. д.).

**Коммерческая тайна** – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности меры охраны.

**Тайна изобретения, полезной модели или промышленного образца** – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Согласно законодательству обязательными признаками информации с ограниченным доступом должны быть:

1. Информация имеет действительную или потенциальную ценность для ее обладателя в силу неизвестности ее третьим лицам. Такими лицами могут быть государство, юридические или физические лица.

2. К информации нет свободного доступа на законном основании. Возможность сохранения ее неизвестной для третьих лиц установлена законом.

3. Обладатель информации принимает меры по ее защите.

К государственной тайне относятся сведения, удовлетворяющие следующим признакам:

1. Сведения в строго установленных сферах деятельности государства (военной, внешнеполитической, экономической, разведывательной,

контрразведывательной и оперативно розыскной деятельности) и ни в каких других.

2. Сведения, не известные широкому, точнее – неопределенному неконтролируемому кругу лиц, и представляющие ценность именно в силу такой неизвестности.

3. Сведения, распространение которых может нанести ущерб безопасности РФ. При этом величина ущерба такова, что влияет на безопасность государства.

4. Сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

#### **Система документов по защите государственной тайны**

Документы по защите государственной тайны по функционально-целевому назначению подразделяются на следующие основные классы:

- нормативные правовые;
- организационно-распорядительные;
- нормативные;
- плановые;
- информационные.

**Нормативные правовые акты** в области защиты государственной тайны включают:

- федеральные законы;
- указы и распоряжения Президента РФ;
- постановления и распоряжения высших органов исполнительной и судебной властей РФ.

Базовыми законами в области защиты государственной тайны являются специальные законы «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, а также нормативные правовые акты более общего характера: Конституция РФ, Гражданский и Уголовный кодексы РФ и др.

На их основе **организационно-распорядительные документы** определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны. Эти документы по характеру регламентируемых вопросов (решаемых задач) и продолжительности действия подразделяют на два вида:

- основополагающие (руководящие) документы;
- распорядительные документы (документы оперативного управления).

Основополагающие (руководящие) документы помимо самостоятельного использования служат основой при разработке нормативных, плановых и информационных документов. Они являются подзаконными актами, детализирующими и раскрывающими положения нормативных правовых актов, и устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их задач, функций, прав, обязанностей и мер ответственности.

Положения по защите государственной тайны издаются на основе нормативных правовых актов и принятых концепций и детализируют указные документы, в основном по вопросам организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

- основные направления работ по защите государственной тайны;
- структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;
- порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;
- финансово-экономические вопросы обеспечения работ по защите государственной тайны;

– вопросы государственного лицензирования в области защиты государственной тайны.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие руководства, наставления, инструкции и правила.

**Распорядительные документы** – документы текущего (оперативного) управления издаются во исполнение или в дополнение к основополагающим документам. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

**Нормативные документы** устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну, обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых регламентируются вопросы защиты государственной тайны, являются:

- специальные нормативные документы федеральных органов исполнительной власти, ответственных за обеспечение защиты государственной тайны;
- нормативные документы государственной системы стандартизации. К специальным нормативным документам относятся:
  - требования и нормы по защите государственной тайны;
  - методики проведения работ в области защиты государственной тайны;
  - лицензии предприятиям на право осуществления работ в области защиты государственной тайны;
  - сертификаты соответствия средств защиты информации;
  - аттестаты на объекты защиты.

**Плановые документы** включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

**Информационные документы** служат для информационного обеспечения решения задач организации и осуществления защиты государственной тайны.

По форме представления информационные документы могут быть следующих видов:

- справочные документы;
- отчетная научно-техническая документация;
- учебная и научная литература;
- формы документов служебного делопроизводства.

#### **Федеральный закон «О государственной тайне»**

Положения федерального закона «О государственной тайне» от 21 июля 1993 года № 5485-1 обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

*Термины, используемые в законе, их определения*

**Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

**Носители сведений, составляющих государственную тайну** – материальные объекты, в том числе физические поля, в которых сведения, составляющие

государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов.

**Система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

**Допуск к государственной тайне** – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а также предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

**Доступ к сведениям, составляющим государственную тайну** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

**Гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

**Средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

**Перечень сведений, составляющих государственную тайну**, совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

#### **Правовой режим защиты государственной тайны**

##### *Перечневый подход к организации защиты государственной тайны*

В настоящее время в России существуют как открытые, так и закрытые перечни сведений. Открытыми перечнями являются приведенный в Законе «О государственной тайне» перечень сведений, составляющих государственную тайну, а также утверждаемый Указом Президента РФ перечень сведений, отнесенных к государственной тайне. Кроме того, существуют ведомственные перечни сведений, подлежащих засекречиванию, которые могут быть как открытыми, так и закрытыми.

С их помощью реализуется подход к организации защиты государственной тайны в виде системы перечней, включающей:

- перечень сведений, составляющих государственную тайну (определен в Законе «О государственной тайне»);
- перечень сведений, отнесенных к государственной тайне (утверждается Указом Президента РФ);
- развернутый перечень сведений, подлежащих засекречиванию в органе государственной власти (утверждается руководителями органов власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне);
- перечни сведений, подлежащих засекречиванию, на предприятии, в учреждении и организации (представляют собой выписки из развернутых перечней сведений, подлежащих засекречиванию).

**Перечень сведений, составляющих государственную тайну** – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделяемых полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут

персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Перечень не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Такой подход должен позволить системе засекречивания адаптироваться к динамичному развитию нашего общества, ослабить искусственную секретность, наносящую ущерб экономическим интересам РФ.

Установлена персональная ответственность конкретных должностных лиц за принятие решения по отнесению сведений к государственной тайне. Именно за ними сохраняется ответственность за обоснованность, в том числе экономическую, установленной степени секретности конкретных сведений. Именно на них возложена функция гибкого и своевременного реагирования на внешние условия изменения режима секретности, чтобы последний не превращался в фактор, тормозящий развитие экономики, науки и межгосударственных отношений.

*Сведения, не подлежащие отнесению к государственной тайне и засекречиванию*

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- 1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- 2) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- 3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- 4) о фактах нарушения прав и свобод человека и гражданина;
- 5) о размерах золотого запаса и государственных валютных резервах РФ;
- 6) о состоянии здоровья высших должностных лиц РФ;
- 7) о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

### **Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

### **Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

### **Контрольные вопросы**

1. Перечислите основные виды тайн. Охарактеризуйте каждый вид.
2. Назовите обязательные признаки информации с ограниченным доступом.
3. На какие классы по функциональному назначению подразделяются документы по защите государственной тайны?
4. Дайте определение понятию «гриф секретности».
5. Какие сведения не относятся к государственной тайне и не подлежат

засекречиванию?

6. Перечислите органы защиты государственной тайны.
7. Какие существуют методы защиты сведений, составляющих государственную тайну?
8. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.

## **Практическое занятие № 10. ГОСТ Р ИСО/МЭК 15408-3-2013. Компоненты доверия к безопасности**

**Система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны), Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне.

Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом РФ.

Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны, Служба внешней разведки РФ, Государственная техническая комиссия при президенте РФ и их органы на местах организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Защита государственной тайны является основным видом деятельности органов государственной власти, предприятий, учреждений или организаций.

Цель защиты государственной тайны заключается в предотвращении или снижении величины ущерба безопасности государства путем исключения (существенного затруднения) утечки информации по всем возможным каналам.

Методы защиты сведений, составляющих государственную тайну, подразделяются на правовые, организационно-технические и экономические.

К **правовым методам** обеспечения защиты сведений, составляющих государственную тайну, относится разработка нормативных правовых актов, регламентирующих отношения в области защиты государственной тайны, и нормативных методических документов по вопросам обеспечения защиты государственной тайны.

**Организационно-техническими методами** обеспечения защиты сведений, составляющих государственную тайну, являются:

- создание и совершенствование системы защиты государственной тайны в РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, включая предупреждение и пресечение правонарушений в области защиты государственной тайны, а также выявление, изобличение и привлечение

к ответственности лиц, совершивших преступления в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;

- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах жизни и деятельности общества и государства, в том числе и по вопросам обеспечения защиты государственной тайны.

**Экономические методы** обеспечения защиты государственной тайны включают в себя:

- разработку федеральных программ в области защиты государственной тайны и определение порядка их финансирования;

- установление и наложение штрафов на должностных и юридических лиц за нарушения требований по защите государственной тайны.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов:

- бумажные документы;
- магнитные носители информации в электронно-вычислительных машинах;
- электромагнитные поля, создаваемые радиоэлектронными средствами при передаче информации;

- физические проявления объектов (органов управления, промышленных предприятий и др.), сведения о которых составляют государственную тайну, в виде разнообразных полей и следов деятельности.

Как носители сведений в современных условиях особую роль имеют технические средства сбора, передачи, хранения и обработки информации. С их использованием обрабатывается основной объем информации, составляющей государственную тайну. Их недостатком является уязвимость для широкого спектра угроз несанкционированного распространения защищаемой информации. защите информации на таких носителях уделяется особое внимание.

Человек в действующем Законе РФ «О государственной тайне» не рассматривается как специфический носитель сведений, хотя он в своей памяти может

хранить эти сведения. Тем самым человек не ставится на один уровень с техническими носителями. Он в проблеме защиты государственной тайны рассматривается как субъект общественных отношений, возникающих в процессе защиты государственной тайны.

### **Полномочия органов государственной власти и должностных лиц в области защиты государственной тайны**

Палаты Федерального собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны;
- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- определяют полномочия должностных лиц в аппаратах палат Федерального собрания по обеспечению защиты государственной тайны.

Президент РФ:

- утверждает государственные программы в области защиты государственной тайны;
- утверждает по представлению Правительства РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства РФ перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры РФ о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

Правительство РФ:

- организует исполнение Закона РФ «О государственной тайне»;
- представляет на утверждение Президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает порядок разработки Перечня сведений, отнесенных к государственной тайне;
- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства РФ;
- устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;
- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или

рассекречиванием и их защитой.

Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства РФ;
- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;
- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;
- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства РФ о государственной тайне;
- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;
- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;
- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

#### **Допуск должностных лиц и граждан к государственной тайне**

**Допуск к государственной тайне** – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

Принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частные, временные ограничения их прав в соответствии со статьей 24 Закона «О государственной тайне»;
- письменное согласие на проведение в отношении их полномочий органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом «О государственной тайне»;
- ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на

работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и/или штатных мероприятий.

Основанием для отказа гражданину в допуске к государственной тайне в соответствии со статьей 22 Закона «О государственной тайне» могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное место жительства в другое государство;
- выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;
- уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

- **первая форма** – для граждан, допускаемых к сведениям особой важности;
- **вторая форма** – для граждан, допускаемых к совершенно секретным сведениям;
- **третья форма** – для граждан, допускаемых к секретным сведениям.

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Основными **целями** контроля и надзора являются:

- обеспечение выполнения единых правил и норм в организации работ по защите государственной тайны;
- своевременное выявление предпосылок к утечке информации, составляющей государственную тайну.

Основными **задачами** контроля и надзора являются:

- оценка полноты и качества выполнения органами, организациями и должностными лицами, осуществляющими деятельность в области защиты государственной тайны, возложенных на них обязанностей и функций;
- оценка целесообразности и обоснованности принимаемых управленческих решений и мер по защите государственной тайны с целью предупреждения возможных неблагоприятных последствий их выполнения;
- выявление нарушений установленных требований или норм по защите

государственной тайны, установление их причин, подготовка в необходимых случаях материалов для привлечения виновных к ответственности;

- профилактика различных видов нарушений;
- выявление нерешенных проблем и противоречий в правовом, организационном, научно-техническом, информационном и других видах обеспечения эффективной защиты государственной тайны.

Рассмотрим основные термины в области контроля и надзора за обеспечением защиты государственной тайны.

**Контроль состояния защиты государственной службы** – проверка соответствия организации и эффективности защиты информации, составляющей государственную тайну, установленным требованиям и/или нормам по защите государственной тайны.

**Контроль организации защиты информации** – проверка соответствия организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов в области защиты информации.

**Контроль эффективности защиты информации** – проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации.

**Надзор** – наблюдение, разновидность контроля, одна из форм деятельности различных государственных органов по обеспечению законности. Надзор – это контроль в форме правового регулирования. Эта форма применяется, прежде всего, для осуществления контроля за соблюдением законов, установленных норм, требований, стандартов. Органы надзора вправе при соответствующих обстоятельствах применять к объектам надзора меры административного принуждения. Необходимым условием надзора является отсутствие между субъектами и объектами надзора организационной соподчиненности.

### **Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

### **Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

### **Контрольные вопросы**

Перечислите органы защиты государственной тайны.

1. Какие существуют методы защиты сведений, составляющих государственную тайну?
2. Перечислите органы защиты государственной тайны.
3. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
4. Назовите цели и задачи контроля и надзора за обеспечением защиты государственной тайны.
5. Поясните сущность ведомственного контроля над обеспечением защиты государственной тайны.

## **Практическое занятие № 11. Принципы построения системы информационной безопасности**

**Банковская тайна** – защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов. К основным объектам банковской тайны относятся: тайна банковского счета, тайна операций по банковскому счету, тайна банковского вклада, тайна частной жизни клиента.

Банковская тайна является видом конфиденциальной информации или видом сведений, перечень которых достаточно четко определен законом. Статья 857

«Гражданского кодекса РФ (Часть вторая)» от 26 января 1996 года № 14-ФЗ «Банковская тайна» содержит следующие нормы:

- 1) банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;
- 2) сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренном законом;
- 3) в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 года № 395-1 содержит более расширенную группу норм (статья 26):

Кредитная организация. Банк России гарантирует тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям). Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия прокурора – органами предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность,

включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

Таким образом, сведения, составляющие банковскую тайну, не устанавливаются по волеизъявлению субъекта предпринимательской деятельности – банка или иной кредитной организации, а это определенные законом сведения, которые принадлежат клиентам банка (банковский счет, банковский вклад, операции по счету, сведения о клиенте). При этом обязанность сохранять эти сведения является односторонней обязанностью банка – клиент не связан этими обязательствами. Вторым отличием банковской тайны, выводящим ее за пределы частного случая коммерческой тайны, является тот факт, что банковская тайна может выступать как охранительный институт для личной и семейной тайны, если граждане желают сохранять в тайне свое финансовое положение.

### **Пользование информацией, составляющей профессиональную тайну**

В сфере ГМУ широко распространена **профессиональная тайна**, которая представляет собой одну из самых специфических систем ограничений на доступ к информации. Профессиональная тайна чаще всего имеет дело с информационными блоками, защита от несанкционированного распространения которых является обязанностью субъекта в силу выполняемых им профессиональных функций. При этом в качестве субъекта, на который возлагается обязанность сохранения профессиональной тайны, может выступать как физическое, так и юридическое лицо. Соблюдение тайн представителями определенных профессий является их обязанностью, возникающей вне зависимости от того, урегулирована она какими-либо юридическими нормами либо нет. В этом случае обязательства по нераспространению сведений являются неотъемлемой частью самой профессии. Гражданин не обратился бы к адвокату, нотариусу или частнопрактикующему врачу, если бы не был уверен, что доверенные этому лицу сведения не будут сохранены в тайне от посторонних, которыми в данном случае являются любые третьи лица.

Система исходящих от государства норм поведения также не может оставаться в стороне от регулирования этой группы общественных отношений.

Нормы законодательства, регулирующие данные отношения, характеризуются в целом двумя моментами:

- данные нормы содержатся в соответствующих профильных законах;
- как правило, эти нормы содержат только запреты на распространение определенных категорий сведений, не описывая механизма их защиты.

Объектом профессиональной тайны является, прежде всего, информация, принадлежащая гражданам, обращающимся за профессиональными услугами (нотариальными, страховыми, медицинскими и др.). С развитием рыночных отношений и появлением большого числа субъектов предпринимательской деятельности в России юридические лица также стали полноправными участниками этих отношений. Нотариальная тайна, тайна связи, адвокатская тайна – действие этих правовых институтов в равной степени распространяется и на сведения, обладателями которых являются юридические лица.

Профессиональная тайна является неотъемлемой частью определенных видов профессиональной деятельности вне зависимости от того, ведется она от имени государства или от частного лица. И даже если она ведется от имени государства, это не значит, что государство в лице других органов ГМУ может без ограничений получать доступ к таким сведениям.

К примеру, по действующему законодательству РФ информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при обследовании и лечении, составляют **врачебную (медицинскую) тайну**.

Включаемый в данный институт перечень сведений достаточно подробно

представлен в действующем законодательстве РФ. Прежде всего следует отметить нормы статьи 61 «Основ законодательства РФ об охране здоровья граждан», утвержденные ВС РФ 22 июля 1993 года № 5487-1, которая именуется «Врачебная тайна». На основе этих норм к медицинской тайне относятся:

- факт обращения гражданина за медицинской помощью;
- состояние здоровья гражданина;
- диагноз заболевания;
- иные сведения, полученные при обследовании и лечении.

Допускается предоставление сведений, составляющих медицинскую тайну, без согласия гражданина или его законного представителя:

- в целях обследования гражданина, не способного выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему в возрасте до 15 лет для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий.

**Нотариальная тайна** вытекает из законодательной базы деятельности нотариата в РФ, которую определяет Конституция РФ и Основы законодательства РФ о нотариате.

**Адвокатская тайна** – сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

**Процессуальные тайны** – тайна совещания судей, тайна совещания присяжных заседателей, данные предварительного следствия (дознания) – содержат в себе признаки как служебной тайны, так и профессиональной.

Первые два вида направлены на обеспечение невмешательства в отправление правосудия и представляют из себя административно-правовой запрет на контакт с судьями в период их совещания по поводу вынесения приговора (вердикта, решения).

**Тайна страхования** – это разновидность служебной, а также коммерческой тайны. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о застрахованном лице, о состоянии его здоровья, а также о его имущественном положении.

**Тайна связи** – регулируется конституционными нормами (часть 2 статьи 23 Конституции РФ), а также соответствующими нормами федеральных законов «О связи» от 07 июля 2003 года № 126-ФЗ, «О почтовой связи» от 17 июля 1999 года № 176-ФЗ.

#### **Пользование информацией, составляющей служебную тайну**

В сфере ГМУ нередко фигурирует служебная тайна, которая наиболее сложна с точки зрения определения ее понятия и правового режима, поскольку в этот вид тайны в разное время включалось и теперь включается различное содержание. Служебная тайна является разновидностью конфиденциальной информации. Согласно Закону РФ «О государственной тайне» от 21 июля 1993 года № 5485-1, прежний режим служебной тайны упразднен, и секретные сведения относятся к государственной тайне. Однако в различных правовых актах термин «служебная тайна» продолжает упоминаться и в него вкладывается различное значение, причем в большинстве случаев оно даже не раскрывается.

**Объектами служебной тайны** являются преднамеренно скрываемые интересы и сведения о различных сторонах и сферах государственной, военной, управленческой, научно-технической, финансовой, экономической и др. деятельности хозяйствующего субъекта, охрана которых обусловлена возможной угрозой безопасности хозяйствующего субъекта.

**Субъектами служебной тайны** являются собственник служебной информации

ограниченного распространения (юридическое лицо, обладающее на законном основании служебной конфиденциальной информацией), конфиденгент служебной информации ограниченного распространения (физическое или юридическое лицо, использующее служебную информацию ограниченного распространения в пределах, установленных собственником или владельцем служебной информации ограниченного распространения на основании договора или распорядительных документов).

Содержащие служебную тайну документы:

- печатаются в специально выделенной комнате;
- учитываются, как правило, отдельно от несекретной документации;
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются только с письменного разрешения соответствующего руководителя;

### **Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

### **Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

### **Контрольные вопросы**

1. Какие сведения относятся к банковской тайне?
2. Перечислите известные вам виды профессиональной тайны.
3. Раскройте порядок обращения с документами, содержащими служебную тайну.
4. Какая информация относится к сведениям конфиденциального характера?
5. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?
6. Опишите структуру законодательства РФ о коммерческой тайне.

## Практическое занятие № 12. Модель Харрисона-Рузо-Ульмана

**Конфиденциальная информация** – достаточно широкое понятие, поскольку к этой категории (за исключением сведений, относящихся к государственной тайне) относятся все виды информации ограниченного доступа, защищаемой законами.

В соответствии с Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188 к этим сведениям относятся:

- 1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- 2) сведения, составляющие тайну следствия и судопроизводства;
- 3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
- 4) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);
- 5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);
- 6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Расширительному толкованию этот перечень не подлежит. Поэтому произвольное отнесение кем-либо к разряду конфиденциальной другой, не предусмотренной перечнем информации не влечет за собой правовых последствий. Более того, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ запрещено относить к конфиденциальной информации:

- 1) законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- 2) документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- 3) документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- 4) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений и организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК.

Под **технической защитой конфиденциальной информации** понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в

том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

В соответствии с Положением «О лицензировании деятельности по технической защите конфиденциальной информации» лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

1) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности «компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

2) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами РФ, руководящими и нормативно-методическими документами, утвержденными приказами ФСТЭК, которые зарегистрированы в Министерстве юстиции РФ;

3) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

4) использование третьими лицами программ для ЭВМ или баз данных на основании договора с их правообладателем.

#### **Законодательство Российской Федерации о коммерческой тайне**

В условиях рыночного хозяйствования коммерческая тайна защищает производителя от недобросовестной конкуренции, к которой относятся противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т. п.

Законодательство Российской Федерации о коммерческой тайне есть совокупность федеральных законодательных актов, которые содержат правовые нормы, регулирующие группу однородных общественных отношений, возникающих в связи и по поводу коммерческой тайны между ее обладателем и иными субъектами.

Закон «О предприятиях и предпринимательской деятельности» от 25 декабря 1990 года № 445-1 впервые закрепил понятие «коммерческая тайна»: информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

#### **Федеральный закон «О коммерческой тайне»**

Федеральный закон «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Положения закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована и не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

#### *Основные понятия и определения*

**Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Информация, составляющая коммерческую тайну (секрет производства)** –

сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

**Режим коммерческой тайны** – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

**Обладатель информации, составляющей коммерческую тайну** – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

**Доступ к информации, составляющей коммерческую тайну** – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

**Передача информации, составляющей коммерческую тайну** – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

**Контрагент** – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

**Предоставление информации, составляющей коммерческую тайну** – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

**Разглашение информации, составляющей коммерческую тайну** – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

### **Информация, относящаяся к коммерческой тайне**

Состав сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых предприятием по защите своей интеллектуальной собственности. Ошибочное или несвоевременное выделение предмета защиты существенно снижает эффективность системы информационной безопасности предприятия, что чревато существенным экономическим ущербом для него.

Перечень сведений, составляющих коммерческую тайну предприятия, следует формировать по следующим признакам:

- эта информация должна быть экономически выгодной для предприятия или выгодной для его конкурента в случае ее утечки. В качестве критерия важности конкретной информации принимается количественный показатель величины наносимого ущерба;
- эта информация не должна быть общеизвестной или общедоступной на законных основаниях;
- эти сведения не должны содержать государственной тайны или защищаться согласно нормам авторского или патентного права;
- информация, которая зафиксирована в письменной или иной материальной

форме или находится в исключительном ведении предприятия;

- такая информация должна быть понятным образом специально обозначена («грифована») и в отношении нее должны быть обеспечены необходимые меры по сохранению конфиденциальности;

- эти сведения не должны напрямую касаться деятельности предприятия, способной нанести ущерб обществу, жизни и здоровью людей.

При этом информация, подтверждающая сведения, компрометирующие компанию, не может быть только на этом основании отнесена к коммерческой тайне.

Обеспечение конфиденциальности требует определенных затрат, в число которых входят, с одной стороны, затраты на обеспечение режимных мероприятий, а с другой – потери от ограничений в использовании конфиденциальной информации. Экономический же эффект от утаивания информации может выразиться как в получении реальной прибыли, так и в предотвращении возможного ущерба предприятию. Сравнение положительных и отрицательных последствий ограничения доступа к рассматриваемым сведениям и их открытого использования, анализ возможностей предприятия по обеспечению необходимых защитных мер позволит определить экономическую или иную целесообразность отнесения тех или иных сведений к коммерческой тайне.

С течением времени ценность информации уменьшается, а суммарные затраты растут. Чем выше уровень защиты, тем дороже обходится ее обеспечение, поэтому необходимо оценивать оптимальный уровень защиты.

Самое сложное из приведенных понятий – отсутствие доступа на законном основании. За этой формулировкой стоят перечни сведений, которые запрещено относить к тому или иному виду тайны.

В законе «О коммерческой тайне» приведены сведения, которые не могут составлять коммерческую тайну.

Таким образом, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;

- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников,

об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

- обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

В статье 10 закона «О коммерческой тайне» приведены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, или лиц, которым такая информация была предоставлена или передана;

- 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, приведенных выше. Наряду с приведенными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Кроме того, меры по охране конфиденциальности информации признаются разумно достаточными, если:

- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

- 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

### **Порядок оформления отчета по практическому занятию и его защиты**

К защите требуется отчет с подробными ответами на вопросы.

Отчет по результатам выполнения практического занятия оформляется в соответствии с требованиями, предъявляемыми к оформлению такого рода работ и должен содержать ответы на вопросы для контроля владения компетенциями работы.

### **Содержание отчета о практическом задании**

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

### **Контрольные вопросы**

1. Что представляет собой информация, составляющая коммерческую тайну?
2. Что понимается под разглашением информации, составляющей коммерческую тайну?
3. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?
4. В отношении каких сведений не может быть установлен режим коммерческой тайны?
5. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

### Практическое занятие № 13. Модель Белла-ЛаПадула

Пусть абоненты сети  $A_1, A_2, \dots, A_N$  используют некоторый симметричный криптоалгоритм  $y = E(x, k)$  с секретным ключом. Как известно для того, чтобы для связи каждой пары абонентов использовать уникальную пару ключей, необходимо иметь 2 ключ. Притом для обеспечения высокой степени секретности для каждого очередного сеанса связи необходимо использование уникального сеансового ключа  $k_{session}$ . Таким образом, для эффективной работы такой сети нужен механизм распределения ключей, способный обеспечить конфиденциальность ключевой информации и оперативность распределения ключей. Протокол открытого распределения ключей Диффи-Хеллмана, предложенный на заре развития криптографии с открытым ключом, призван решить сформулированную задачу.

Для вычисления этого ключа противнику Е надо уметь решать задачу логарифмирования в конечных полях, тогда как в настоящее время не разработано полиномиальных алгоритмов дискретного логарифмирования в произвольном конечном поле.

Схема Диффи и Хеллмана подвержена атаке “человек посередине”, суть которой состоит в том, что активный противник перехватывает компоненты ключа и формирует с каждым из участников протокола свой собственный ключ. Протокол Диффи-Хеллмана не содержит встроенных средств контроля присутствия активного противника. В качестве способа защиты может быть предложено использование электронной цифровой подписи с участием независимого арбитра, сертифицирующего ключи ЭЦП участников протокола 6.

#### Задания:

На основе параметров протокола, заданных в таблице вариантов (таблица 1 Приложения А) вычислить общий сеансовый ключ для пары участников.

Отчет по лабораторной работе представить в виде расчетного файла математического пакета по выбору студента (например, MathCAD)

Отчет по лабораторной работе представить в виде расчетного файла математического пакета по выбору студента (например, MathCAD)

#### Контрольные вопросы:

1. Протокол открытого распределения ключей Диффи-Хеллмана.
2. Уязвимости протокола Диффи-Хеллмана.
3. Способы усиления протокола Диффи-Хеллмана.
4. Сущность атаки «человек посередине».

## Практическое занятие № 14. Ролевая модель безопасности

### Основные термины *Зашифрование*

Процесс преобразования открытых данных в закрытые (зашифрованные). В данном программном продукте используется алгоритм шифрования ГОСТ 2814789. Это симметричный алгоритм, что означает, что для шифрования и расшифрования используется одинаковый ключ.

### Расшифрование

Процесс преобразования закрытых данных в открытые (расшифрованные).

### Ключ, ключевая система

Конкретное секретное значение криптографического преобразования, определяющее ход процесса преобразования данных. В данном пакете программ в качестве ключей шифрования могут использоваться: ÿ Ключ Пользователя; ÿ Сетевой ключ.

При работе с ключами всегда производится анализ имитоприставки. Узел Замены (УЗ)

Долговременный элемент ключевой системы ГОСТ 28147-89. Обычно хранится в файле uz.db3 на ключевом носителе и является первым ключевым элементом, вводимым в устройство шифрования при инициализации. Все компьютеры, между которыми предполагается обмен зашифрованной информацией (например, локальная сеть), должны использовать один и тот же УЗ, т. к. несоответствие Узлов Замены приведет к невозможности расшифрования файлов с другой машины.

### Главный Ключ (ГК)

Секретный ключ, используется для шифрования других ключей. Обычно хранится в файле gk.db3 на ключевом носителе. Может быть зашифрован на пароле. Создается администратором. При инициализации устройства шифрования загружается в него и находится там до выключения питания ЭВМ. Пароль

Последовательность символов, вводимых с клавиатуры. Пароль защищает ключи от несанкционированного использования в случае их хищения или потери. В пакете КРИПТОН® Шифрование максимальная длина пароля для ключей шифрования - 37 символов; минимальная длина - 4 символа. Длина пароля определяет стойкость системы. Поэтому рекомендуется использовать длинные пароли с неповторяющимися символами. Символы разных регистров (прописные и строчные буквы) различаются. Использовать символы с кодами меньше 32 и больше 127 (управляющие символы, псевдографику и русские буквы) не рекомендуется.

### Ключ пользователя (ПК)

Секретный ключ, используется для шифрования файлов и других ключей. Хранится в файле с расширением ".KEY", обычно в зашифрованном виде.

### Сетевой ключ

Секретный ключ, используется для шифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом Наборе.

### Имитовставка, имитоприставка

Применяется для обеспечения защиты системы шифрования от навязывания ложных данных. Имитовставка представляет собой отрезок информации фиксированной длины, полученный из открытых данных и ключа. Создается при зашифровании данных и добавляется к ним. При расшифровании данных также вычисляется имитовставка и сравнивается с хранимой. В случае несовпадения можно выделить следующие причины: изменен Узел Замены; изменен ключ, на котором были зашифрованы данные; изменены сами зашифрованные данные; если для зашифрования использовался пароль, то при

расшифрования он был неверно введен; неисправно устройство шифрования.

#### Сетевая Таблица

Для обмена зашифрованной информацией между  $N$  узлами необходимо  $N*(N-1)$  ключей (каждый с каждым). Фактически, это таблица, где в заголовках строк и столбцов проставлены номера узлов, а в ячейках хранятся ключи. Эта матрица симметрична, т.е. ключ для передачи от узла А узлу Б (сетевой ключ АБ) в точности равен сетевому ключу Б-А. Сетевая Таблица при создании зашифровывается на Ключе Сетевой Таблицы (КСТ).

#### Сетевой Набор

Из полной Сетевой Таблицы необходимо для каждого из узлов сформировать набор ключей для связи с другими узлами. Фактически, такой набор представляет собой одну из строк таблицы. Сетевой Набор хранится в файле NNNNN.SYS в каталоге сетевых ключей, где NNNNN - пятизначный десятичный номер данного узла. Он всегда зашифрован на Ключе Сетевого Набора (КСН), хранящемся в файле NNNNN.KEY в каталоге сетевых ключей. КСН получают вместе с Сетевым Набором от администратора криптографической сети. При получении КСН обычно незашифрован, поэтому рекомендуется перешифровать его.

#### Назначение КРИПТОН® Шифрование

Пакет КРИПТОН® Шифрование предназначен для защиты электронных документов (файлов) от несанкционированного доступа при хранении их на персональном компьютере или передаче по открытым каналам связи. Защита документов осуществляется путем их шифрования по ГОСТ 28147-89.

#### Иерархическая структура ключей

На рисунке 16.1 приведена иерархическая структура ключей, используемая в пакете КРИПТОН® Шифрование.

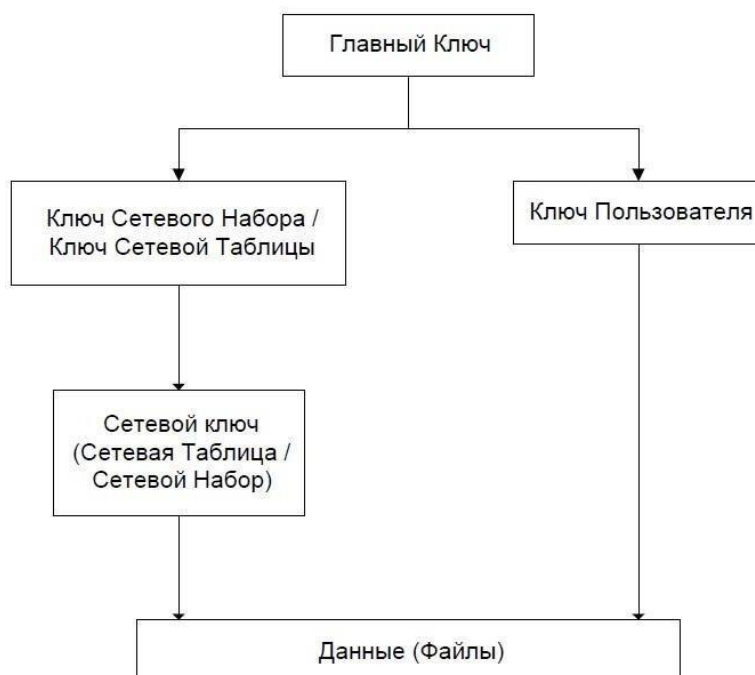


Рисунок 16.1 - Иерархическая структура ключей

#### Задания:

1. Изучить возможности шифрования пакета КРИПТОН® Шифрование
2. Создать отдельную папку Lab 16. В ней создать следующие папки:
3. Keys - для хранения пользовательских ключей
4. Source - для исходных тестовых файлов
5. Crypt - для зашифрованных файлов
6. Создать два ключа пользователя в каталоге Keys.

7. Скопировать тестовые файлы в папку Source. Занести размеры файлов в таблицу 1 (приложение А).
8. Сжать тестовые файлы при помощи WinRAR с максимальной степенью сжатия. Занести размеры полученных архивов в таблицу 1 приложения А.
9. Зашифровать тестовые файлы. Занести размеры зашифрованных файлов в таблицу 1 приложения А.
10. Сжать зашифрованные файлы при помощи WinRAR с максимальной степенью сжатия. Занести размеры полученных архивов в таблицу 1 приложения А.
11. Сделать выводы о закономерностях изменения размера файла.
12. Изучить возможности гарантированного удаления (уничтожения выбранных файлов без возможности их восстановления) пакета КРИПТОН® Шифрование.
13. Уничтожить все архивы и зашифрованные файлы. В режиме командной строки (в пакетном режиме) выполнить задание своего варианта согласно таблице 2 (приложение А). Команды включить в отчет.

**Контрольные вопросы:**

1. Способы решения задачи защиты электронных документов от НСД методами криптографии.
2. Функции и состав пакета КРИПТОН® Шифрование.
3. Иерархия ключей в пакете КРИПТОН® Шифрование 4. Понятие сетевого набора и сетевой таблицы.
4. Особенности использования гарантированного удаления.

## Практическое занятие №15. Основы криптографии

### Основные термины

#### Криптографическая сеть

Множество компьютеров, называемых узлами, между которыми тем или иным способом осуществляется направленный обмен зашифрованной информацией, называется криптографической сетью. Направленный обмен подразумевает возможность зашифровать передаваемую информацию таким образом, чтобы расшифровать ее мог только тот узел, для которого она предназначалась. Обмен информацией между узлами криптографической сети может осуществляться как посредством локальных и глобальных сетей, так и с помощью сменных носителей. В пакете КРИПТОН® Шифрование для защиты данных в криптографической сети используется симметричный алгоритм шифрования - ГОСТ 28147-89.

#### Сетевой ключ

Секретный ключ, используется для зашифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом Наборе.

#### Сетевая Таблица

Для обмена зашифрованной информацией между  $N$  узлами необходимо  $N*(N-1)$  ключей (каждый с каждым). Фактически, это таблица, где в заголовках строк и столбцов проставлены номера узлов, а в ячейках хранятся ключи. Эта матрица симметрична, т. е. ключ для передачи от узла  $A$  узлу  $B$  (сетевой ключ  $AB$ ) в точности равен сетевому ключу  $B-A$ . Сетевая Таблица при создании зашифровывается на Ключе Сетевой Таблицы (КСТ).

#### Сетевой Набор

Из полной Сетевой Таблицы необходимо для каждого из узлов сформировать набор ключей для связи с другими узлами. Фактически, такой набор представляет собой одну из строк таблицы. Сетевой Набор хранится в файле `NNNNN.SYS` в каталоге сетевых ключей, где `NNNNN` - пятизначный десятичный номер данного узла. Он всегда зашифрован на Ключе Сетевого Набора (КСН), хранящемся в файле `NNNNN.KEY` в каталоге сетевых ключей.

КСН получают вместе с Сетевым Набором от администратора криптографической сети. При получении КСН обычно зашифрован на главном ключе, поэтому рекомендуется перешифровать его на пароле.

#### Организация криптографической сети

Для организации криптографической сети администратор должен выполнить следующие действия

Создать Сетевую Таблицу. Для этого необходимо указать количество узлов криптографической сети и имя Сетевой Таблицы. В результате автоматически создается новый Ключ Сетевой Таблицы `NET_SYS.KEY`, на котором автоматически зашифровывается Сетевая Таблица `KEY_NET.SYS`

Создать Сетевые Наборы (СН) для узлов криптографической сети.

По умолчанию создаются СН для всех узлов и в каждом сетевом наборе все узлы являются доступными. При необходимости можно создать такие СН, чтобы узел мог шифровать данные только для ограниченного множества узлов криптографической сети. В результате получается множество Ключей Сетевого Набора (`NNNNN.KEY`) и Сетевых Наборов (`NNNNN.SYS`) для узлов криптографической сети.

Каждому узлу присвоить свой номер `NNNNN`. Распределить Ключи Сетевого Набора и Сетевые Наборы по соответствующим узлам криптографической сети. Узлу с номером `NNNNN` необходимо передать два файла: `NNNNN.KEY` и `NNNNN.SYS`.

Шифрование файлов для передачи в криптографической сети

Файл данных, передаваемый узлом А узлу Б, зашифровывается на Файловом (сеансовом) Ключе. Файловый Ключ создается автоматически при зашифровании файла данных и передается вместе с ним. Так как файловый ключ не может передаваться в открытом виде, то он зашифровывается на Сетевом Ключе А-Б. Этот ключ узел А берет из своего Сетевого Набора.

Сетевой Набор узла А зашифрован на Ключе Сетевого Набора (КСН) узла А, который, в свою очередь, тоже может быть зашифрован на каких либо ключах узла А (как правило, ГК).

Узел Б, по информации, присовокупленной к зашифрованному файлу, понимает, что файл пришел от узла А. Используя свои ключи, узел Б расшифровывает свой КСН.

Затем, используя КСН, узел Б расшифровывает свой набор и извлекает из него Сетевой Ключ А-Б. Так как этот Сетевой Ключ совпадает с тем Сетевым Ключом, который использовал узел А для зашифрования, то узел Б может расшифровать Файловый Ключ, пришедший вместе с файлом.

Наконец, с помощью Файлового Ключа расшифровывается сам файл.

Настройка параметров

После запуска Мастера ключей шифрования и выбора настройки параметров (рисунок 17.1) правая сторона панели содержит следующие настраиваемые параметры: *"Каталог Ключей Пользователя"*.

Следует ввести каталог Ключей Пользователя. В этом каталоге будет производиться поиск Ключей Пользователя в следующих ситуациях: - Зашифровании файла на Ключе Пользователя.

Расшифровании файла, зашифрованного на Ключе Пользователя. Перешифровании файла, зашифрованного на Ключе Пользователя.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов. По данной кнопке на экран выводится меню "Диски"/"Карточки", позволяющее указать каталог с помощью стандартного диалога Windows или диалога выбора устройств SCSI.

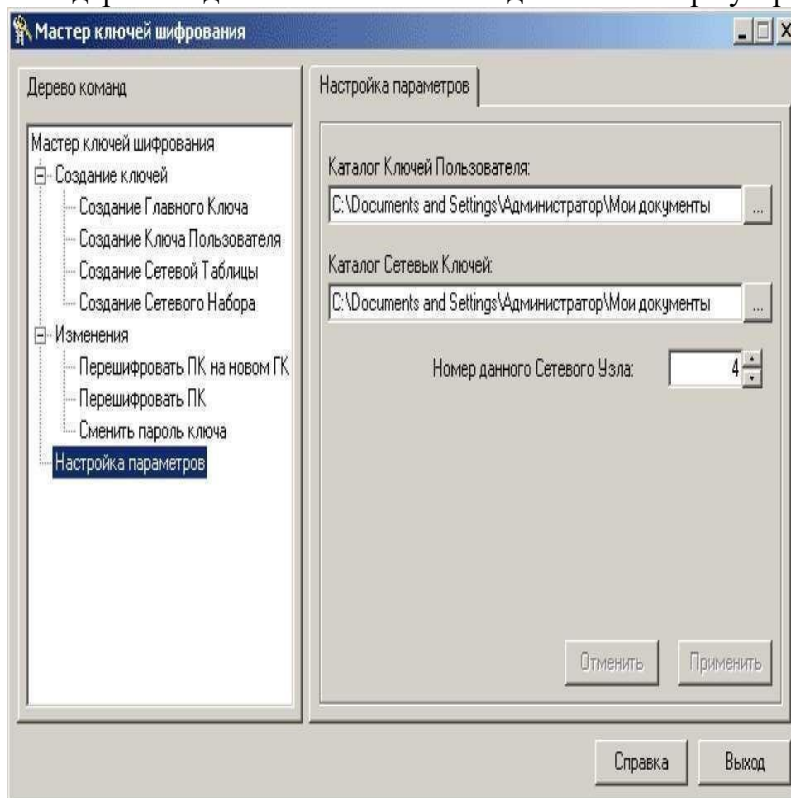


Рисунок 17.1 - Мастер ключей шифрования пакета КРИПТОН® Шифрование  
*"Каталог Сетевых Ключей"*

Следует ввести каталог Сетевых Ключей. В этом каталоге будет производиться

поиск Сетевых Ключей в следующих ситуациях: - Зашифровании файла на Сетевом Ключе.

Расшифровании файла, зашифрованного на Сетевом Ключе. Перешифровании файла, зашифрованного на Сетевом Ключе.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов, по которой вызывается стандартный диалог обзора папок Windows. Сетевые Ключи хранятся в Сетевых Наборах в фалах NNNNN.sys, где

NNNNN - номер данного сетевого узла - см. главу "Создать Сетевой Набор".

"Номер данного сетевого узла".

Следует ввести номер сетевого узла - целое число в диапазоне от 1 до 30000, идентифицирующее данный сетевой узел (пользователя или компьютер - в зависимости от организационных решений).

Для ввода в действие сделанных изменений в конфигурации следует нажать кнопку "Применить". Конфигурация будет изменена.

Для отмены внесенных изменений следует нажать кнопку "Отменить".

Следует учесть, что в Windows NT/2000/XP данные параметры являются персональными для каждого локального пользователя Windows. Параметры сохраняются в системном реестре Windows.

#### **Задания:**

Создать отдельную папку Lab17. В ней создать следующие папки:

**Key\_net** - для Ключа СТ и самой СТ;

**00001, 00002, 00003, 00004** - для Ключей СН исамихСН; - **Source** - для тестовых файлов и их зашифрованных вариантов.

Создать Сетевую Таблицу для четырех узлов в каталоге **Key\_net**.

Создать Сетевые Наборы для всех узлов. Разложить полученные Ключи СН и сами СН по соответствующим папкам **00001, ... 00004**.

Установить номер своего узла равный 2 и указать в параметрах соответствующий каталог сетевых ключей.

Зашифровать тестовые файлы для узла 3.

Установить номер своего узла равный 3 и указать в параметрах соответствующий каталог сетевых ключей..

Расшифровать тестовые файлы с автоматическим переименованием и затем полученные файлы уничтожить.

Установить номер своего узла равный 1 и указать в параметрах соответствующий каталог сетевых ключей.

Расшифровать тестовые файлы (зашифрованные для узла 3) с автоматическим переименованием.

Оформить отчет о проделанных шагах 2 - 9, в который включить краткое описание результатов каждого шага (например, создана сетевая таблица для четырех узлов и т. д.).

Из папки **Материалы** для данной лабораторной работы в папку **Lab17** скопировать Ключ СН и сам СН, соответствующий номеру варианта.

Установить номер своего узла, соответствующий номеру варианта и указать в параметрах каталог сетевых ключей **Lab17**.

Зашифровать тестовые файлы для узла 11.

Полученные зашифрованные файлы предоставить для проверки.

#### **Контрольные вопросы:**

1. Понятие сетевого набора и сетевой таблицы.
2. Особенности защиты данных в криптографической сети с помощью симметричных и асимметричных алгоритмов шифрования
3. Назначение Сетевых Ключей и Ключей Сетевых Наборов.

4. Параметры, настраиваемые в пакете КРИПТОН®
5. Шифрование, для работы в криптографической сети.
6. Процесс обмена зашифрованными файлами в криптографической сети.
7. Создание сетевых наборов для ограниченного числа узлов криптографической сети.

## Практическое занятие №16. Симметричные шифры

Организация взаимосвязи пользователей. Прямой обмен открытыми ключами. Все пользователи, обменивающиеся документами, предварительно должны обменяться своими открытыми ключами. При этом необходимо исключить подмену на этапе пересылки.

Создается персональная дискета с собственными ключами. Секретный ключ закрывается паролем.

Для собственного открытого ключа формируется подпись на собственном секретном ключе, и открытый ключ записывается на дискету для передачи.

Подготавливается юридический документ на бумаге (например, письмо), в котором указываются: данные о владельце (Ф.И.О., должность, место работы), сам открытый ключ (распечатка в шестнадцатеричном виде), полномочия владельца (перечень документов, которые уполномочен удостоверить владелец открытого ключа). Данный документ должен быть оформлен таким образом, чтобы иметь юридическую силу в случае возникновения спорных вопросов о принадлежности подписи и полномочиях владельца. Если в письме не установлено полномочий, то они определяются по должности и месту работы. Например, бухгалтер одного предприятия не может удостоверить платежные поручения другого, а программист не может удостоверить платежные поручения и своего предприятия.

Дискеты и соответствующие сопроводительные документы направляются по адресам предприятий и пользователей, с которыми будет производиться обмен документами.

Получив такой комплект, необходимо убедиться в юридической силе полученного документа, а также в идентичности копий открытого ключа на дискете и в документе. Если открытый ключ верен, необходимо поместить его в каталог открытых ключей для последующего использования.

Такую операцию по пересылке ключей необходимо выполнить столько раз, сколько существует пользователей, с которыми Вы работаете. Это возможно, но для большого числа пользователей неэффективно.

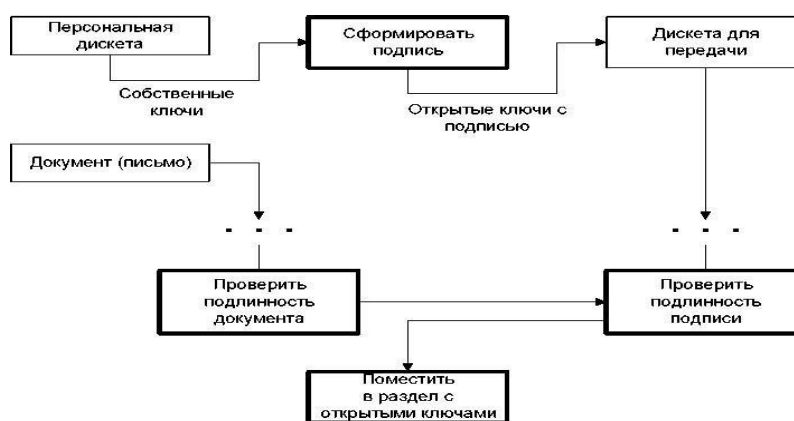


Рисунок 18.1 - Прямой обмен открытыми ключами

### Задания:

Создать отдельную папку Lab18. В ней создать папку PUBLIC и персональные папки для каждого человека, выполняющего лабораторную работу на данном компьютере. В персональных папках создать следующие папки:

PKDIR - для хранения открытых ключей;

FLOPPY - каталог, имитирующий персональную дискету.

Изучить параметры, настраиваемые в программе КРИПТОН® Подпись - Конфигурация по Руководству пользователя (раздел 4.2).

Поочередно в программе КРИПТОН Подпись - Конфигурация установить в соответствующих параметрах созданные папки персональной дискеты и открытых ключей хранения ключей, для каждого - соответственно - свои.

Каждому в своей папке Floppy создать пару ключей, секретный ключ закрыть собственным паролем, открытый ключ сертифицировать на своем же ключе, скопировав его в папку своих открытых ключей. При создании ключа обязательно указать свое полное ФИО и место работы (студент СГУ, факультет ..., группа ...)

Каждому в своей папке создать документ (MS Word) - сопроводительное письмо по форме, приведенной в приложении 1, для пересылки вместе со своим открытым ключом другим пользователям.

Скопировать свой открытый ключ вместе с сопроводительным письмом в папку PUBLIC. Эта папка будет играть роль курьера, доставляющего ключи и сопроводительные письма другим пользователям. Теперь необходимо, чтобы остальные пользователи получили ключи и сохранили у себя.

Каждый заходит в папку PUBLIC, изучает сопроводительные письма остальных пользователей, проверяет сертификацию открытых ключей и соответствие их распечатке в соответствующем сопроводительном письме. В случае отсутствия несоответствий, открытые ключи копируются в свои персональные папки в каталоги открытых ключей (PKDIR).

У всех полученных открытых ключей каждый удаляет подпись, и сертифицирует на своем ключе.

Теперь каждому пользователю необходимо получить открытые ключи, которые расположены в папке материалов к лабораторной работе в соответствии со своим вариантом. Для этого необходимо проделать те же операции, что указаны в п. 7, 8 по отношению к ключам и открытым ключам в папке материалов.

Для отчета необходимо будет показать все созданные файлы.

#### **Контрольные вопросы:**

1. Возможные угрозы для секретных и открытых ключей.
2. Мероприятия по защите секретных и открытых ключей.
3. Состав персональной дискеты.
4. Схема прямого обмена открытыми ключами.
5. Схема обмена открытыми ключами через сертификационный центр.
6. Задачи, возлагаемые на сертификационный центр.
7. Генерация секретных ключей.
8. Сертификация открытых ключей.

## Практическое занятие №17. Асимметричные шифры

Для составления таблицы всех простых чисел, которые не превосходят заданного числа  $N$ , надо из таблицы чисел  $2, 3, \dots, N$  вычеркнуть все числа, которые делятся на два, кроме 2. Затем вычеркнуть все числа, которые делятся на три, кроме 3. Далее этот процесс (оставить наименьшее из оставшихся простых и вычеркивать все кратные этому простому) продолжаем до тех пор, пока очередное выбранное число не превысит  $N$ .

Данный метод позволяет строить множество простых чисел, но он неудобен для проверки простоты заданного числа.

### Задания:

В программной реализации решета Эратосфена должен быть разработан интерфейс, удобный для эксплуатации в интерфейсе предусмотреть:

- ввода начальной информации из сформированного заранее файла и файла, который создается в оболочке программы;
- ввод начальной информации с клавиатуры.

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

### Контрольные вопросы:

1. Возможные угрозы для секретных и открытых ключей.
2. Мероприятия по защите секретных и открытых ключей.
3. Состав персональной дискеты.
4. Схема прямого обмена открытыми ключами.
5. Схема обмена открытыми ключами через сертификационный центр.
6. Задачи, возлагаемые на сертификационный центр.
7. Генерация секретных ключей.
8. Сертификация открытых ключей.

## Практическое занятие №18. Хэш-функции

Основные этапы алгоритма DES при шифровании текста: Генерируется (задается) случайная последовательность  $Q$  из 56 бит.

В последовательность  $Q$ , для контроля четности, добавляются восемь контрольных битов в позиции 8, 16, 24, ..., 64.

Получается блок  $U$  размером в 64 бита.

Для удаления контрольных битов из блока  $U$  и формирования ключа  $K$  для шифрования, блок  $U$  преобразуют, используя функцию  $G(U)$ . Функция  $G$  определяется в виде стандартной таблицы, которую надо использовать в неизменном виде. В результате преобразования получают блок  $K=G(U)$  размером в 56 бит. Блок  $K$  разбивают на две половины  $C_0$  и  $D_0$  по 28 бит.

Используя  $C_0$  и  $D_0$ , последовательно определяются  $C_i$  и  $D_i$ ,  $i = 1, 2, \dots, 16$ . Для формирования  $C_i$  и  $D_i$  применяют операции циклического сдвига влево на один или два бита. Величина сдвига определяется стандартной таблицей. Операции сдвига для  $C_i$  и  $D_i$  выполняются независимо. Последовательность  $C_5$  получается из  $C_4$  посредством циклического сдвига влево на 2 бита, а  $D_5$  – посредством циклического сдвига влево на 2 бита  $D_4$  (см. таблицу сдвигов для вычисления ключа). В результате четвертого этапа формируется 16 ключей для 16 раундов алгоритма DES.

Завершающий этап формирования ключей. Используя перестановку  $H$ , которая задается стандартной таблицей, каждый ключ размером в 56 бит преобразуется в блок из 48 бит. Данным преобразованием завершается этап формирования ключей.

Текущий блок открытого текста размером в 64 бит, представленный в виде двух 32 битовых блоков ( $L_0R_0$ ) преобразуется начальной перестановкой  $IP$ , которая задается фиксированной стандартной таблицей.

Выполняется 16 раундов преобразований по следующим формулам  $L_i = R_{i-1}$ ,

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ ,  $i = 1, 2, \dots, 16$ .

Функция  $f(R_{i-1}, K_i)$  представляет собой некоторую суперпозицию простых преобразований, детальное описание которых будет дано ниже. Отметим, что функция  $f(R_{i-1}, K_i)$  является нелинейной. Нелинейность функции  $f(R_{i-1}, K_i)$  обеспечивается  $S$ -блоками.

Алгоритм вычисления функции шифрования  $f(R_{i-1}, K_i)$

К блоку  $R_{i-1}$  применяют функцию расширения  $E(R_{i-1})$ , которая 32битовый блок  $R_{i-1}$  преобразовывает в блок  $R' = E(R_{i-1})$  размером в 48 бит. Функция  $E(R_{i-1})$  определяется стандартной таблицей. Алгоритм вычисления функции шифрования формулируется следующим образом.

Вычисляется новый блок размером в 48 бит по формуле  $B = E(R_{i-1}) \oplus K_i$ .

Блок  $B$  размером в 48 бит разбивается на восемь блоков  $B_j$ ,  $j=1,2,\dots, 8$ , по шесть битов каждый

$B = B_1B_2B_3B_4B_5B_6B_7B_8$ .

Каждый блок  $B_j$  размером в шесть бит, используя свою функцию  $S_j$ , преобразуется в блок  $S_j(B_j)$  размером в четыре бита. В результате получается следующий блок данных

$B' = S_1(B_1) S_2(B_2) S_3(B_3) S_4(B_4) S_5(B_5) S_6(B_6) S_7(B_7) S_8(B_8)$

размером в 32 бита.

Алгоритм преобразования блока  $B_j$  размером в шесть бит в блок  $S_j(B_j)$  размером в четыре бита следующий. Каждая функция  $S_j$  представляет собой стандартную таблицу, которая состоит из четырех строк с номерами 0, 1, 2, 3, и шестнадцати столбцов с номерами 0,1,2,...,15. Пусть, например, некоторый блок

$B_j = b_1 b_2 b_3 b_4 b_5 b_6 = 110010$ ,  $j = 1, 2, \dots, 8$ .

Тогда имеет место: биты  $b_1b_6 = 10$  формируют номер столбца (двоичное число 10 равно десятичному числу 2) таблицы  $S_j$ , биты  $b_2 b_3 b_4 b_5 = 1001$  формируют номер

строки (двоичное число 1001 равно десятичному числу 9) таблицы  $S_j$ . Блок  $B_j = b_1 b_2 b_3 b_4 b_5 b_6 = 110010$  заменяют двоичным значением числа таблицы  $S_j$ , которое находится на пересечение строки с номером  $b_1 b_6 = 10$  (2) со столбцом с номером  $b_2 b_3 b_4 b_5 = 1001$  (9). Преобразуя каждое  $B_j$ ,  $j = 1, 2, \dots, 8$ , из блока  $B$ , получим новый блок  $B'$  размером в 32 бита.

#### **Задания:**

Программная реализация криптографической системы, основанной на алгоритме шифрования *DES*, должна быть оформлена как некоторая программная оболочка. В программной реализации должен быть разработан интерфейс, удобный для эксплуатации программы, в интерфейсе следует предусмотреть:

- два режима формирования ключа – ключ задан, ключ формируется по умолчанию;
- ввод начальной информации из сформированного заранее файла и из файла, который создается в оболочке программы;
- режимы шифрования, которые предусмотрены в *DES*;
- режимы шифрования и дешифрования информации.

Подготовить отчет по работе. В отчете описать алгоритм *DES*, описать структуру представления данных в программе, основные функции программы, назначение функций, входные и выходные параметры функций. В отчет включить описание алгоритма генерации ключа, детали программной реализации, которые представляют интерес с точки зрения разработчика.

#### **Контрольные вопросы:**

1. По какому принципу построен блочный шифр *DES*?
2. Какой шифр предшествовал шифру *DES*?
3. Указать длину начального ключа в алгоритме *DES*.
4. Перечислить основные этапы формирования ключей в алгоритме *DES*.
5. Сколько раундов в алгоритме *DES*?
6. Сколько ключей формируется в алгоритме *DES* для шифрования текста?
7. Указать длину ключа при шифровании текста в алгоритме *DES*.
8. Сколько *S*-функций определено в алгоритме *DES*?
9. Какая арифметическая операция используется при преобразованиях в алгоритме *DES*.
10. Укажите длину шифруемого блока в алгоритме *DES*.

#### **Литература**

1. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2013. – 88 с.
2. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2013. – 288 с.
3. Крушный В.В. Основы теории информации и кодирования. – Снежинск: СГФТА, 2013. – 69 с.
4. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2013. – 320 с.
5. Филоненков А. И., Самсонов Б. Б., Кречет Т. В., Плохов Е. М. Теория информации и кодирования – М.: ФЕНИКС, 2013. – 288 с.
6. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений / Г.И.Хохлов. – М.: Издательский центр “Академия”, 2015. – 176 с.
7. Шеннон К. Математическая теория связи // К.Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л.Добрушина и О.Б.Лупанова. – М.: ИЛ, 2015. – 512 с.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Методические указания**  
по выполнению самостоятельных работ  
по дисциплине «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»  
для студентов специальности 10.05.01 Компьютерная безопасность  
специализация «Информационно-аналитическая и техническая экспертиза  
компьютерных систем»

Ставрополь  
2025

## Содержание

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Введение.....                                                                | 144 |
| Общая характеристика самостоятельной работы студента .....                   | 145 |
| Технологическая карта самостоятельной работы студента.....                   | 146 |
| Самостоятельное изучение тем лекций .....                                    | 147 |
| Паспорт фонда оценочных средств для проверки самостоятельной<br>Работы ..... | 147 |
| Вопросы для собеседования по лабораторным работам.....                       | 148 |
| Комплект разноуровневых задач и заданий .....                                | 153 |
| Список рекомендуемой литературы .....                                        | 158 |

## Введение

Целью дисциплины «Основы информационной безопасности» является овладение теоретическими и прикладными профессиональными знаниями и умениями в области развития основы современных форм и методов информационной безопасности личности, общества, государства и предприятия в условиях рыночной экономики, а также приобретение навыков самостоятельного инициативного и творческого использования теоретических знаний в практической деятельности в работе специалиста по специальности 10.05.01 Компьютерная безопасность.

Задачами дисциплины являются:

1. Сформировать представление об основных компонентах комплексной дисциплины «Основы информационной безопасности».
2. Знать определения основных направлений информационной безопасности.
3. Сформировать навыки работы со справочной литературой и нормативно-техническими материалами.
4. Сформировать навыки составления обзора по вопросам обеспечения информационной безопасности.
5. Ознакомиться со средствами и методами защиты информации.
6. Сформировать представления о концепции информационной безопасности.
7. Приобрести умения самостоятельно и творчески использовать знания и полученные практические навыки в процессе последующего обучения в соответствии с учебным планом подготовки бакалавров по направлению.

«Информационная безопасность» по профилю «Организация и технология защиты информации».

Компетенции обучающегося, формируемые в результате освоения дисциплины:

| Индекс | Формулировка:                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-1  | Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства |
| ОПК-5  | Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации                                                                    |

В результате освоения дисциплины обучающийся должен:

| Перечень компонентов                                                                                                                                                                                                                                                                                                                                      | Технологии формирования компетенции | Средства и технологии оценки    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---------------------------------|
| <b>Знать:</b><br>- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;<br>- основные направления информационной безопасности;<br>- организационно-правовые основы защиты информации;<br>- основные элементы технической защиты информации;<br>- основные элементы программно-аппаратной защиты информации; | лекции, самостоятельная работа      | собеседование, письменный отчет |



эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным работам, оформление отчета по выполненному лабораторному заданию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

- 1) для овладения знаниями:
  - чтение текста (конспекта лекций, учебника дополнительной литературы) и конспектирование текста;
  - работа с нормативными документами;
  - поиск информации в Интернет;
- 2) для закрепления и систематизации знаний:
  - работа с конспектом лекции (обработка текста);
  - повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
  - составление плана и тезисов ответа или графическое изображение структуры ответа;
  - составление таблиц для систематизации учебного материала;
  - изучение нормативных документов;
  - ответы на контрольные вопросы;
- 3) для формирования умений:
  - подготовка к лабораторным работам;
  - решение задач и лабораторных заданий;
  - подготовка отчетов по лабораторным работам;
  - рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные работы, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным работам, а также варианты тестовых заданий.

#### **Технологическая карта самостоятельной работы студента**

| Код реализуемой компетенции | Вид деятельности студентов  | Итоговый продукт самостоятельной работы | Средства и технологии оценки | Объём часов |
|-----------------------------|-----------------------------|-----------------------------------------|------------------------------|-------------|
| <b>1 семестр</b>            |                             |                                         |                              |             |
| ОПК-1 ОПК-5                 | Изучение тем № 4, 8 лекций. | Устный отчет                            | Собеседование                | 6           |

|                           |                                                                                             |                                                  |               |           |
|---------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------|---------------|-----------|
| ОПК-1 ОПК-5               | Подготовка к лабораторным работам по темам № 11, 13.                                        | Письменный отчет                                 | Собеседование | 6         |
| ОПК-1 ОПК-5               | Самостоятельное решение разноуровневых задач и заданий по темам № 1- 14 лабораторных работ. | Письменный отчет с решением разноуровневых задач | Коллоквиум    | 6         |
| <b>Итого за 2 семестр</b> |                                                                                             |                                                  |               | <b>18</b> |

### Самостоятельное изучение тем лекций

| п/п       | Темы для самостоятельного изучения                                               | Рекомендуемые источники информации<br>(№ источника) |                |              |                  |
|-----------|----------------------------------------------------------------------------------|-----------------------------------------------------|----------------|--------------|------------------|
|           |                                                                                  | Основная                                            | Дополнительная | Методическая | Интернет-ресурсы |
| 1 семестр |                                                                                  |                                                     |                |              |                  |
| 1         | Способы реализации угроз Информационной безопасности и результаты их воздействия | 1, 2, 4, 5                                          | 2, 4, 5        | 1, 2         | 1                |
| 2         | Методы оценки уязвимости и защищенности информации                               | 2, 4, 5                                             | 1, 2, 5        | 1, 2         | 1                |

### Паспорт фонда оценочных средств для проверки самостоятельной Работы

| Код оцениваемой компетенции (или её части) | Модуль, раздел, тема (в соответствии с Программой) | Тип контроля | Вид контроля | Компонент фонда оценочных средств                                 | Количество заданий для каждого уровня, шт. |            |
|--------------------------------------------|----------------------------------------------------|--------------|--------------|-------------------------------------------------------------------|--------------------------------------------|------------|
|                                            |                                                    |              |              |                                                                   | Базовый                                    | Повышенный |
| 1 семестр                                  |                                                    |              |              |                                                                   |                                            |            |
| ОПК-1<br>ОПК-5                             | 1,2,4,6,8                                          | текущий      | устный       | Вопросы для собеседования по подготовке к лабораторным работам    | 28                                         | 28         |
| ОПК-1<br>ОПК-5                             | 3,4,7,8,9                                          | текущий      | устный       | Вопросы для собеседования по самостоятельному изучению тем лекций | 28                                         | 22         |

|                |                      |         |        |                                                                            |    |    |
|----------------|----------------------|---------|--------|----------------------------------------------------------------------------|----|----|
| ОПК-1<br>ОПК-5 | 2,4,5,7,10,11,1<br>2 | текущий | устный | Комплект<br>разноуровне<br>вых задач<br>по темам<br>лабораторн<br>ых работ | 23 | 26 |
|----------------|----------------------|---------|--------|----------------------------------------------------------------------------|----|----|

### **Вопросы для собеседования по лабораторным работам**

Базовый уровень:

**Тема 1. Анализ терминов и определений информационной безопасности.**

**Госты и руководящие документы**

**Цель лабораторной работы** – изучение места и роли информационной безопасности в системе национальной безопасности Российской Федерации для формирования способности осознавать социальную значимость своей будущей профессии и обладать высокой мотивацией к выполнению профессиональной деятельности.

**Организационная форма занятия** – круглый стол.

**Вопросы, выносимые на обсуждение:**

1. Когда создана государственная система защиты информации в России?
2. В каком документе отражается система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз в различных сферах деятельности?
3. Какой документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?
4. В каком Федеральном законе идет речь о регулировании отношений, возникающих в связи с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием в интересах обеспечения безопасности Российской Федерации?
5. Какие источники внешних угроз национальной безопасности вам известны?
6. Какие источники внутренних угроз национальной безопасности вам известны?
7. Какие методы обеспечения информационной безопасности РФ вам известны?

**Тема 2. Концепция информационной безопасности предприятия** **Цель лабораторной работы** – формирование способности определять виды и формы информации, подверженной угрозам, на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.

**Организационная форма занятия** – деловая игра.

**Вопросы, выносимые на обсуждение:**

1. Поясните, почему руководитель предприятия должен принять обязательства по управлению информационным ресурсом предприятия?
2. Почему цели и обязательства в области управления информацией должны определяться в отдельном документе, таком как политика предприятия?
3. Каким образом руководство предприятия может определить основную информационную базу и установить ценность элементов информации?
4. Что собой представляет классификационная политика на предприятии?
5. Как распространяются на предприятии основы безопасной работы с информацией?
6. Что собой представляет общий порядок работы с конфиденциальной информацией на предприятии?

7. Почему необходимо назначить руководителей, ответственных за выполнение мер безопасности?

8. В чем преимущество концепции владельца информации для каждого важного информационного объекта?

9. Кто должен принимать решения по классификации информации?

10. Как должна классифицироваться новая информация или новое сочетание существующих данных предприятия?

11. Что собой представляет контроль важных элементов информации по всему циклу их обработки?

12. Как должны выполняться операции в случае форс-мажорных обстоятельств, повредивших инфраструктуру обработки данных или устройства их хранения?

13. Должен ли руководитель по безопасности нести ответственность за безопасность информации в любых формах или только за безопасность компьютерной информации?

14. Доверенное ПО системы поддерживает мандатный контроль и управление доступом. Необходимо разработать программу – драйвер принтера. Объясните причины, по которым данная программа должна быть доверенным процессом.

### **Тема 3. Угрозы информации: проведение анализа информации на предмет целостности**

**Цель лабораторной работы** – формирование способности определять возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности современного предприятия.

**Организационная форма занятия** – решение ситуационных задач.

#### **Вопросы, выносимые на обсуждение:**

1. Дать определение понятию «угроза».
2. Дать определение понятию «источник угроз».
3. Дать определение понятию «уязвимость».
4. Дать определение понятию «последствия».
5. Классификация угроз информационной безопасности.
6. Классификация источников угроз информационной безопасности.
7. Классификация уязвимостей информационных систем.
8. Угрозы нарушения конфиденциальности, целостности и доступности информации.

### **Тема 4. Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации**

**Цель лабораторной работы** – овладение теоретическими и прикладными знаниями и умениями в оценивании защищаемой информации для формирования способности провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

**Организационная форма занятия** – решение ситуационных задач.

#### **Вопросы, выносимые на обсуждение:**

1. Какие показатели и характеристики информации Вы знаете?
2. Как Вы понимаете свойство важности информации? 3. Как Вы понимаете свойство полноты информации? 4. Как Вы понимаете свойство адекватности информации? 5. Как Вы понимаете свойство релевантности информации? 6. Как Вы понимаете свойство толерантности информации?

### **Тема 5. Технические средства защиты информации**

#### **Технические средства защиты переговоров по телефонным линиям**

**Цель лабораторной работы** – овладение теоретическими знаниями и практическими навыками использования современных средств технической защиты информации для формирования способности активной созидательной деятельности в условиях информационного противоборства.

**Организационная форма занятия** – репрезентация изученного материала.

**Вопросы, выносимые на обсуждение:**

1. Перечислите технические каналы утечки информации.
2. Опишите структуру и основные характеристики каждого класса технических каналов утечки информации.
3. Какие современные средства защиты телефонных линий Вы знаете?
4. Чем отличаются методы пассивной и активной защиты речевой информации?

**Тема 6. Оценка безопасности информации на объектах ее обработки** **Цель лабораторной работы** – овладение теоретическими знаниями и практическими навыками в области оценивания безопасности информации на объектах ее обработки для формирования способностей проводить комплексный анализ функционального процесса объекта защиты и его информационных составляющих для возможности определения источников информационных угроз, разработки предложений и тактики по повышению их устойчивости к деструктивным воздействиям.

**Организационная форма занятия** – деловая игра.

**Вопросы, выносимые на обсуждение:**

1. Перечень нормативной документации в сфере ИБ, необходимой для ознакомления руководителям организаций.
2. Виды и способы организации работ по выполнению норм в области информационной безопасности на предприятиях.
3. Аутсорсинг в сфере информационной безопасности.
4. Обзор основных современных средств массовой информации в области защиты информации на территории РФ и за её пределами.
5. Лучшие мировые и российские практики в организации информационной безопасности на предприятиях.

**Вопросы для собеседования по самостоятельному изучению тем дисциплины**

Базовый уровень

**2 семестр:**

1. Назначение и характеристика аппаратных средств защиты информации.
2. Защита персонального ЭВМ от несанкционированного доступа.
3. Системы защиты информации.
4. Защита информации в ЭВМ.
5. Криптографические средства защиты информации.
6. Анализ и оценка угроз информационной безопасности в банке.
7. Задачи защиты информации.
8. Классификация угроз информации.
9. Система нормативно-правовых актов по обеспечению информационной безопасности в РФ.
10. Общие принципы защиты программных продуктов от вирусов.
11. Закон о государственной тайне и механизм его обеспечения.
12. Характеристика программных средств защиты информации.
13. Информационная безопасность и средства массовой информации.
14. Защита баз данных.
15. Защита информации в электронных платежных системах.
16. Классификация средств защиты информации.

17. Политика безопасности информации предприятия.
18. Каналы утечки информации: акустический канал.
19. Технические средства защиты акустических каналов.
20. Компьютерные преступления и законодательная основа борьбы с ними.
21. Средства защиты информации.
22. Защита информации и Интернет.
23. Общие подходы к формированию перечня конфиденциальной информации.
24. Концепция совершенствования правового обеспечения информационной безопасности РФ.
25. Защита информации от компьютерных вирусов.
26. Информационная война и информационное оружие.
27. Организация политики безопасности в отделе кадров предприятия.
28. Структура безопасности предприятия.
29. Клод Шеннон – основоположник секретной связи.
30. Понятие сертификации средств защиты информации.
31. Понятие сетевого экрана и порядок его применения на предприятии.
32. Средства защиты информации на предприятии.
33. Основные понятия информационной безопасности распределенных локально-вычислительных сетей на предприятии.
34. Политика безопасности. Ее основные свойства и задачи.
35. Механизмы защиты баз данных.
36. Основы региональной политики безопасности.
37. Основы проектирования систем защиты.
38. Понятие защиты информации. Сетевой экран.
39. Методология построения систем защиты в автоматизированных системах.
40. Организационно-правовые методы защиты информации.
41. Управление системой защиты информации на предприятии.
42. Мероприятия защиты информации фирмы.
43. Выработка политики защиты информационных ресурсов.
44. Стандартизация и сертификация в процессе защиты информационных ресурсов.
45. Атаки на информационные ресурсы.
46. Угрозы информационным ресурсам.
47. Единое информационное пространство как средство обеспечения общегосударственной информационной безопасности.
48. Элементы и средства управления защитой информации.
49. Меры информационной безопасности.
50. Механизмы защиты ПК.
51. Организация информационной безопасности и защиты информации.
52. Администрирование систем и контроллинг информационных ресурсов как элементы систем защиты.
53. Технологии защиты информационных ресурсов.
54. Аудит и мониторинг безопасности.
55. Обзор современных систем управления безопасностью.
56. Анализ и управления информационными рисками.
57. Методология построения системы информационной безопасности предприятий.
58. Технологии анализа защищенности систем.
59. Технологии обнаружения атак.
60. Современные методы и средства обеспечения информационной безопасности.

61. Современные методы и средства обеспечения безопасности объектов.
62. Технологии защиты при хранении и обработке информации.
63. Биометрическая защита информации.
64. Новые технологии электронной памяти для хранения и защиты информации.
65. Технологии личной безопасности.
66. Архитектура системы защиты.
67. Принципы антивирусной защиты.
68. Требования к защите компьютерной информации.
69. Каналы утечки аудио-, видеоинформации.
70. Принципы организации и работы электронной почты.
71. Система безопасности фирмы.
72. Структура службы безопасности государственного предприятия.
73. угрозы руководителю предприятия.
74. Безопасность в Интернет.
75. Безопасность электронной почты.
76. Мошенничество в Интернет.
77. Система безопасности фирмы.
78. Организация службы безопасности фирмы.
79. Безопасность электронного бизнеса.
80. Обеспечение конфиденциальности и контроль целостности информации.
81. Аутентификация и идентификация информации.
82. Устройства скрытого съема аудиовидеоинформации.
83. Мероприятия по защите коммерческой тайны.
84. Задачи защиты информации.
85. Классификация угроз информации.
86. Система нормативно-правовых актов по обеспечению информационной безопасности в РФ.
87. Общие принципы защиты программных продуктов от вирусов
88. Характеристика программных средств защиты информации.
89. Информационная безопасность и средства массовой информации.
90. Защита баз данных.
91. Защита информации в электронных платежных системах.
92. Классификация средств защиты информации.
93. Политика безопасности информации предприятия.
94. Каналы утечки информации: акустический канал.
95. Технические средства защиты акустических каналов.
96. Защита информации от компьютерных вирусов.
97. Меры информационной безопасности.
98. Механизмы защиты ПК.

## **Комплект разноуровневых задач и заданий**

### **Тема 1. Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы.**

#### **Типовые задачи:**

Задания базового уровня:

- 1) Когда создана государственная система защиты информации в России?
- 2) В каком документе отражается система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз в различных сферах деятельности?
- 3) Какой документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?
- 4) В каком Федеральном законе идет речь о регулировании отношений, возникающих в связи с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием в интересах обеспечения безопасности Российской Федерации?
- 5) Какие источники внешних угроз национальной безопасности вам известны?
- 6) Какие источники внутренних угроз национальной безопасности вам известны?
- 7) Какие методы обеспечения информационной безопасности РФ вам известны?

*Задания повышенного уровня:*

- 1) Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?
- 2) Чем отличается степень секретности от грифа секретности?
- 3) Какие степени и грифы секретности определены для сведений и их носителей в ФЗ «О государственной тайне»?
- 4) Какие данные содержатся в реквизитах носителей сведений, содержащих гос. тайну?
- 5) В каких случаях возможно рассекречивание гос. тайны?
- 6) Какие органы защищают государственную тайну?
- 7) Как осуществляется допуск должностных лиц и граждан к государственной тайне?
- 8) Условия допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну?

### **Тема 2. Анализ источников угроз информационной безопасности Российской Федерации.**

#### **Типовые задачи:**

Задания базового уровня:

- 1) Перечислить виды угроз информационной безопасности Российской Федерации.
- 2) Какие бывают источники угроз информационной безопасности?
- 3) Разработать перечень методов обеспечения информационной безопасности Российской Федерации.
- 4) Привести основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации.
- 5) Перечислить первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.

*Задания повышенного уровня:*

- 1) Идентифицировать источники угроз объектов обеспечения и мер обеспечения информационной безопасности Российской Федерации.
- 2) Определить отношения элементов модели информационной безопасности РФ.
- 3) Дать оценку риску реализации угроз информационной безопасности Российской Федерации.
- 4) Модели защиты российского сегмента глобальной сети Интернет в современных условиях.
- 5) Привести основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

### **Тема 3. Анализ способов реализации угроз информационной безопасности.**

#### **Типовые задачи:**

Задания базового уровня:

- 1) Перечислить источники возникновения и последствия реализации угроз информационной безопасности.
- 2) Классифицируйте источники угроз.
- 3) Обозначьте антропогенные источники угроз.
- 4) Приведите примеры техногенных источников угроз.
- 5) Разработать перечень внутренних источников угроз.

Задания повышенного уровня:

- 1) Привести способы и средства нарушения конфиденциальности информации.
- 2) Описать основные методы реализации угроз информационной безопасности.
- 3) Перечислить основные виды непреднамеренных искусственных угроз.
- 4) Перечислить основные виды преднамеренных искусственных угроз.
- 5) Классифицировать каналы проникновения в систему и утечки информации.
- 6) Дать определение неформальной модели нарушителя.

### **Тема 4. Исследование методов оценки рисков и ущербов информационной безопасности.**

#### **Типовые задачи:**

Задания базового уровня:

- 1) Проанализировать риски при реализации информационной безопасности.
- 2) Обосновать средства и меры контроля рисков.
- 3) Привести существующие виды систем анализа информационных рисков.
- 4) Произвести алгоритмический анализ технологических особенностей защищенности ИС.
- 5) Дать оценку ущербу от угроз безопасности.
- 6) Дать оценку вероятности реализации обнаруженных угроз.

Задания повышенного уровня:

- 1) Создать модели информационных активов компании с точки зрения безопасности. Классифицировать и оценить ценности активов.
- 2) Составлять списки наиболее значимых угроз и уязвимостей безопасности.
- 3) Ранжировать угрозы и уязвимости безопасности.
- 4) Разработать корректирующие меры.
- 5) Формализовать и автоматизировать процедуры оценивания и управления рисками.

## **Тема 5. Анализ методов нарушения конфиденциальности и доступности информации.**

### **Типовые задачи:**

Задания базового уровня:

- 1) Дать определение безопасной информационной системе.
- 2) Дать определение доступности информации.
- 3) Дать определение целостности информации.
- 4) Выделить типы умышленных угроз.
- 5) Перечислить необходимые меры по поддержанию работоспособности компьютерных систем.

Задания повышенного уровня:

- 1) Привести способы и средства нарушения конфиденциальности информации.
- 2) Отразить основные методы реализации угроз информационной безопасности.
- 3) Указать типичные приёмы атак на локальные и удалённые компьютерные системы.
- 4) Перечислить основные положения и назначение Федерального закона РФ «О коммерческой тайне»
- 5) Привести основные положения и назначение Гражданского кодекса, Уголовного кодекса РФ в области защиты информации.
- 6) Назвать государственные органы по контролю и надзору за обеспечением защиты государственной тайны и служебной тайны их задачи и функции.

## **Тема 6. Анализ информации на предмет целостности. Типовые задачи:**

Задания базового уровня:

- 1) Дать определение понятию «угроза».
- 2) Дать определение понятию «источник угроз».
- 3) Дать определение понятию «уязвимость».
- 4) Дать определение понятию «последствия».
- 5) Классификация угроз информационной безопасности.
- 6) Классификация источников угроз информационной безопасности.
- 7) Классификация уязвимостей информационных систем.
- 8) Угрозы нарушения конфиденциальности, целостности и доступности информации.

Задания повышенного уровня:

- 1) Какие показатели и характеристики информации Вы знаете?
- 2) Как Вы понимаете свойство важности информации?
- 3) Как Вы понимаете свойство полноты информации?
- 4) Как Вы понимаете свойство адекватности информации?
- 5) Как Вы понимаете свойство релевантности информации?

## **Тема 7. Анализ потенциально возможных злоумышленных действий в автоматизированных системах обработки информации.**

### **Типовые задачи:**

Задания базового уровня:

- 1) Узнать цели создания и эксплуатации АС ОРГАНИЗАЦИИ как объекта информатизации.
- 2) Рассмотреть структуру, состав и размещение основных элементов АС ОРГАНИЗАЦИИ, информационные связи с другими объектами.
- 3) Определить категории информационных ресурсов, подлежащих защите.
- 4) Выявить уязвимость основных компонентов АС ОРГАНИЗАЦИИ.

5) Интересы затрагиваемых при эксплуатации АС ОРГАНИЗАЦИИ субъектов информационных отношений.

6) Основные задачи системы обеспечения безопасности информации АС ОРГАНИЗАЦИИ.

7) Основные пути достижения целей защиты.

*Задания повышенного уровня:*

1) Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации в АС ОРГАНИЗАЦИИ.

2) Обезопасить от умышленных действий сторонних лиц, зарегистрированных пользователей и обслуживающего персонала.

3) Устранить утечку информации по техническим каналам.

4) Построить неформальную модель возможных нарушителей.

5) Формировать режим безопасности информации.

6) Оснастить техническими средствами хранения и обработки информации.

**Тема 8. Исследование архитектуры систем защиты информации. Типовые задачи:**

*Задания базового уровня:*

1) Привести виды угроз.

2) Узнать характер происхождения угроз.

3) Классифицировать каналы несанкционированного получения информации.

4) Найти источники появления угроз.

5) Определить причины нарушения целостности информации.

*Задания повышенного уровня:*

1) Определить требования к защите информации.

2) Классифицировать автоматизированную систему.

3) Определить факторы, влияющие на требуемый уровень защиты информации.

4) Выбрать или разработать способы и средства защиты информации.

5) Построить архитектуру систем защиты информации.

6) Сформулировать рекомендации по увеличению уровня защищенности.

**Тема 9. Анализ моделей «нарушителя». Типовые задачи:**

*Задания базового уровня:*

1) Определить тип «нарушителя».

2) Составить предположения о имеющейся у нарушителя информации.

3) Составить предположения о имеющихся средствах атак у нарушителя.

4) Определить возможности «нарушителя».

5) Проанализировать каналы атак.

*Задания повышенного уровня:*

1) Негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации.

2) Негласное проникновение нарушителя-сотрудника предприятия с целью доступа к закрытой информации.

3) Проникновение группы нарушителей в охраняемые помещения в нерабочее время путем разрушения инженерной защиты объекта и обхода средств охранной сигнализации.

4) Проникновение одного или группы вооруженных нарушителей под видом посетителей с целью силового захвата ценностей.

5) Вооруженное нападение на объект с целью захвата заложников, ценностей, получения важной информации или организации собственного управления.

## **Тема 10. Анализ методов оценки уязвимости информации. Типовые задачи:**

Задания базового уровня:

- 1) Выполнить разработку модели нарушителей.
- 2) Выделить и категорирование особо важных зон объекта.
- 3) Дать оценку показателям уязвимости.
- 4) Определить слабые места и недостатки в системе охраны.

Задания повышенного уровня:

- 1) Все возможные риски идентифицировать.
- 2) Уязвимости ресурсов идентифицировать и их уровни оценить.
- 3) Угрозы идентифицировать и их уровни оценить.
- 4) Применить контрмеры.
- 5) расходы, связанные с ИБ, оправдать.

## **Тема 11. Анализ методов оценки защищенности информации. Типовые задачи:**

Задания базового уровня:

- 1) Независимо обосновать и проверить задокументированные в профиле и проекте защиты показатели безопасности.
- 2) Убедить потребителя в том, что объект оценки обладает заявленными показателями безопасности.
- 3) Более эффективно использовать при построении систем безопасности результатов, полученных при оценке других продуктов и систем.
- 4) Уменьшить затраты временных и материальных ресурсов на осуществление процесса оценки безопасности.

Задания повышенного уровня:

- 1) Документ о политике информационной безопасности.
- 2) Распределение обязанностей по обеспечению информационной безопасности.
- 3) Обучение и подготовка персонала к поддержанию режима информационной безопасности.
- 4) Уведомление о случаях нарушения защиты.
- 5) Средства защиты от вирусов.
- 6) Планирование бесперебойной работы организации.

## **Тема 12. Анализ криптографических алгоритмов шифрования. Типовые задачи:**

Задания базового уровня:

- 1) Рассмотреть симметричные алгоритмы шифрования.
- 2) Рассмотреть асимметричные алгоритмы шифрования.
- 3) Рассмотреть стандарт шифрования RSA.
- 4) Изучить генерацию ключей.
- 5) Изучить электронную подпись.

Задания повышенного уровня:

- 1) Рассмотреть круг задач, на решение которых ориентированы криптографические методы.
- 2) Изучить основные понятия и определения криптографии.
- 3) Ознакомиться с рекомендациями Microsoft по применению криптографических алгоритмов.
- 4) Рассмотреть отечественный стандарт шифрования данных ГОСТ 28147-89 и американский стандарт шифрования данных AES.
- 5) Изучить концепцию криптосистемы с открытым ключом.

**Тема 13. Анализ моделей обеспечения безопасности: дискреционного доступа (DAC), безопасности Белла-ЛаПадулы, ролевая модель контроля доступа (RBAC), системы разграничения доступа.**

**Типовые задачи:**

Задания базового уровня:

- 1) Изучить модели контроля доступа.
- 2) Изучить дискреционную модель.
- 3) Изучить модель Белла-Ла Падулы.
- 4) Изучить модель Биба.
- 5) Изучить ролевую модель.

Задания повышенного уровня:

- 1) Выполнить обзор функциональности.
- 2) Изучить используемые технологии.
- 3) Рассмотреть архитектуру.
- 4) Реализовать базу функциональности RBAC.
- 5) Выполнить работу с базой данных.

**Тема 14. Анализ существующих антивирусных программных продуктов.  
Порядок проведения антивирусной защиты компьютерной системы.**

**Типовые задачи:**

Задания базового уровня:

- 1) Что такое компьютерный вирус?
- 2) Признаки появления вирусов.
- 3) Классификация вирусов.
- 4) Основные меры по защите от вирусов.
- 5) Способы противодействия компьютерным вирусам.

Задания повышенного уровня:

- 1) Антивирусные программы.
- 2) Требования к антивирусным программам.
- 3) Характеристика антивирусных программ.
- 4) Методики антивирусных программ.
- 5) Краткий обзор антивирусных программ.

**Список рекомендуемой литературы**

**Основная литература**

1. Расторгуев С.П. Основы информационной безопасности. – М.: Академия, 2014. – 192 с.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Академия, 2015. – 336 с.
3. Краковский Ю.М. Информационная безопасность и защита информации: Учебное пособие. – М.: ИКЦ «МарТ», Ростов н/Д: Издательский центр «МарТ», 2015. – 288 с.