ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФГКОУ ВО РЮИ МВД России)

А. Г. Карпика, П. В. Арбузов,

С. В. Гуде, Е. Н. Петрищева

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Практикум

Ростов-на-Дону
2016

УДК 004.056(075.8)
ББК 32.973
О-751

Рецензенты:
начальник кафедры информационно-компьютерных технологий
в деятельности органов внутренних дел Белгородского юридического
института МВД России им. И.Д. Путилина
кандидат технических наук, доцент ***А. Н. Прокопенко;***
начальник Отдела оперативно-разыскной информации
УТ МВД России по СКФО ***С. В. Лемайкина***

О-751 Карпика А. Г., Арбузов П. В., Гуде С. В., Петрищева Е. Н.
Основы информационной безопасности / под общ. ред. А. Г. Карпика: практикум. − Ростов н/Д: ФГКОУ ВО РЮИ МВД России, 2016.– 80 с.

Практикум содержит 6 заданий по изучаемым темам дисциплины «Основы информационной безопасности в органах внутренних дел». В каждом задании 25 вариантов и примеров, распределенных по темам: «Направления обеспечения информационной безопасности», «Защита компьютерной информации», «Криптоанализ». Излагается краткий теоретический материал по данным темам. Рассматриваются примеры решения задач и их оформление.

Адресовано курсантам и слушателям, обучающимся по специальностям: «Правовое обеспечение национальной безопасности», «Правоохранительная деятельность», а также преподавателям гуманитарных вузов и факультетов.

Печатается по решению редакционно-издательского совета
ФГКОУ ВО РЮИ МВД России.

УДК 004.056(075.8)
ББК 32.973
О-751

ПРЕДИСЛОВИЕ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

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 [1].

Одной из составляющих национальных интересов Российской Федерации в информационной сфере является «защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России» [1].

Изучение общих вопросов информационной безопасности необходимо специалистам для формирования целостной картины взаимодействия свойств информации и угроз этим свойствам, а умение применять на практике государственными служащими методов защиты информации позволит повысить безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации.

Именно комплексный подход к обеспечению информационной безопасности организации, основывающийся на умении анализировать потенциальные и реальные угрозы, использовать результаты анализа для разработки организационных мер и выбора технических средств защиты информации, способствует недопущению утечки конфиденциальных данных и нарушения действующего законодательства.

Решение прикладных задач – одна из необходимых составляющих в практике подготовки специалиста независимо от рода будущей деятельности. Решение задач предметной области «информационная безопасность» служит целям формирования умений применения на практике полученных знаний, привычки всесторонне изучать проблему с целью принятия оптимального (в рамках имеющихся ограничений) решения. Помимо этого, задачи развивают логическое мышление, позволяют правильно устанавливать причинно-следственные связи между явлениями, формируют умение группировать предметы, находить закономерности. Формирование перечисленных умений и

навыков будущих юристов, государственных служащих и является целью практикума.

В первом разделе приводятся основные определения и формулы, необходимые для самостоятельного решения задач. Кроме того, описываются методы и примеры решения типовых задач. Во втором разделе представлены варианты практических заданий для самостоятельного решения. Соответствие номеров задач темам практикума приводится в таблице.

Название темы	**Номера задач практикума**
1. Направления обеспечения информационной безопасности	1, 2
1.1. Защита информации от акустических угроз	
1.1. Экономическая модель защиты информации	
2. Защита компьютерной информации	3, 4
2.1. Традиционная (симметричная) криптография	
2.2. Асимметричная криптография	
3. Криптоанализ	5, 6

Оформление задач практикума

Результаты решения заданий практикума оформляются в виде электронных документов в текстовом процессоре, или процессоре электронных таблиц. Файлы сохраняются в личной папке курсанта (слушателя) на сервере кафедры и, при необходимости, отправляются в информационную образовательную среду института.

Для каждой задачи в файле решения должны содержаться:

исходные данные в соответствии с вариантом задания;

процесс решения (исследования);

полученный результат (выводы).

Примеры решения задач по всем темам практикума приводятся в каждом разделе.

I. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ С ПРИМЕРАМИ РЕШЕНИЯ

1. Направления обеспечения информационной безопасности

1.1. Защита информации от акустических угроз

Угроза (безопасности информации): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Физическая форма (звук, свет и др.) в значительной степени определяет характер информационных угроз, технологию и сценарии их развития, а соответственно и способы организационно – технического противодействия. По физической форме своего проявления информация делится на два основных вида: акустическую (чаще всего речевую) и сигнальную. Первая воспринимается органом слуха, вторая органом зрения, при этом не важно, какие промежуточные преобразования происходят с информацией.

Знание физической формы проявления информации в конкретном сценарии информационной угрозы теоретически достаточно для сопоставления однородных по виду информационных угроз в пределах одной и той же обстановки или зоны защиты.

Определение сценариев угроз включает:

моделирование угрозы физического проникновения злоумышленника к источникам информации;

определение каналов утечки информации.

В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежание грубых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход и может привести к увеличению затрат на защиту.

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве некоторых признаков (индикаторов) каналов утечки акустической информации могут служить признаки, указанные в таблице 1.

Таблица 1. Индикаторы утечки акустической информации

Вид канала	Индикаторы
Акустический	1. Малая толщина дверей и стен помещения. 2. Наличие в помещении открытых вентиляционных отверстий. 3. Отсутствие экранов на отопительных батареях. 4. Близость окон к улице и ее домам. 5. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. 6. Частая и продолжительная парковка возле организации чужих автомобилей.

Затухание акустической волны на границе контролируемой зоны зависит от множества факторов, таких как конструкция помещения, материал стен, тип и количество дверей и окон, наличие звукопоглощающих элементов и т.п. Для анализа и ориентировочной оценки можно использовать данные, приведенные в таблицах Т2-Т4 [3].

Для выполнения практического задания примем следующие соглашения:

1. Частота человеческого голоса ($F_{чг}$) лежит в диапазоне частот: 300 – 4000 Гц;

2. Уровень речевого сигнала ($R_{рс}$) составляет 50–60 дБ (обычная речь), 70–80 дБ (громкая речь).

3. Соотношение для определения уровня акустического сигнала за ограждением:

$$R_{ог} = R_{рс} + 6 + 10 \cdot \lg(S_{ог}) - K_{ог}, \quad Дб, \qquad (1)$$

где $R_{рс}$ – уровень речевого сигнала в помещении (перед ограждением), дБ;

$S_{ог}$ – площадь ограждения (м$^{2)}$;

$K_{ог}$ – звукоизолирующая способность ограждения (дБ).

Таблица Т2. Звукопоглощающие свойства строительных конструкций

№	Объект (Материал)	Толщина	$K_{об}$ Звукоизоляция (дБ) на частотах $F_{чг}$ (Гц)					
			125	**250**	**500**	**1000**	**2000**	**4000**
1	Стена (Кирпич)	0,5 кирпича	39	40	42	48	54	60
2		1,0 кирпич	36	41	44	51	58	64
3		1,5 кирпич	41	44	48	55	61	65
4		2 кирпича	45	45	52	59	65	70
5		2,5 кирпича	47	55	60	67	70	70
6	Стена (Железобетонный блок)	0,04 м.	32	36	35	38	47	53
7		0,1 м.	40	40	44	50	55	60
8		0,2 м.	42	44	51	59	65	65
9		0,3 м.	45	50	58	65	69	69
10		0,4 м.	48	55	61	68	70	70
11		0,8 м.	55	61	68	70	70	70
12	Стена (Шлакоблок)	0,22 м.	42	42	48	54	60	63

Таблица Т 3. Звукопоглощающие свойства некоторых оконных блоков

№	Схема остекления		$K_{об}$ Звукоизоляция (дБ) на частотах $F_{чг}$ (Гц)					
			125	**250**	**500**	**1000**	**2000**	**4000**
1	Одинарное остекление	стекло: 3 мм	17	17	22	28	31	32
2		стекло: 4 мм	18	23	26	31	32	32
3		стекло: 6 мм	22	22	26	30.	27	25
4	**Двойное остекление с воздушным промежутком**	57 мм стекло: 3 мм	15	20	32	41	49	46
5		90 мм стекло: 3 мм	21	29	38	44	50	48
6		57 мм стекло: 4 мм	21	31	38	46	49	35
7		90 мм стекло: 4 мм	25	33	41	47	48	36

Таблица Т4. Звукопоглощающие свойства некоторых дверных блоков

№	Конструкция двери	Условия применения	$K_{об}$ Звукоизоляция (дБ) на частотах $F_{чг}$ (Гц)					
			125	**250**	**500**	**1000**	**2000**	**4000**
1	Щитовая	без прокладки	21	23	24	24	24	23
2		с прокладкой из пористой резины	27	27	32	35	34	35
3	Типовая ГТ-327	без прокладки	13	23	31	33	34	36
4		с прокладкой из пористой резины	29	30	31	33	34	41
5	Звукоизолирующая	облегченная	18	30	39	42	45	43
6		облегченная двойная	25	42	55	58	60	60
7		тяжелая	24	36	45	51	50	49

Задание для самостоятельного выполнения

Оценить защищенность помещения от угроз акустической информации. Выработать рекомендации, направленные на повышение его защищенности.

Расчеты выполнить в табличном процессоре, используя соотношение 1.

Условия и соглашения:

1. Исходные данные для вашего варианта находятся в таблице для задания 1.

2. Уровень речевого сигнала в помещении $R_{рс}$=80 Дб.

3. Если в состав ограждения входит несколько элементов, например, кирпичная стена и дверь, то величина $R_{ог}$ этого ограждения принимается равной величине $R_{об}$ наихудшего объекта (наибольшее значение).

4. Величина R всего помещения принимается равной наибольшей величине $R_{ог}$ (наихудшего ограждения).

5. Рекомендации, направленные на повышение защищенности помещения должны быть направлены на выравнивание величин $R_{ог}$ всех ограждений в сторону уменьшения R.

Пример решения

Используя соотношение 1 и справочные данные (табл. Т2 – Т4), определить уровни акустического сигнала за каждым из ограждений помещения, конфигурация которого соответствует варианту (таблица Т5). Оценить помещение по наихудшему показателю. Выработать рекомендации по повышению акустической защищенности помещения.

Используем для расчета данные, соответствующие варианту «0» таблицы Т5.

Развертка помещения для наглядности изображена на рис. 1.

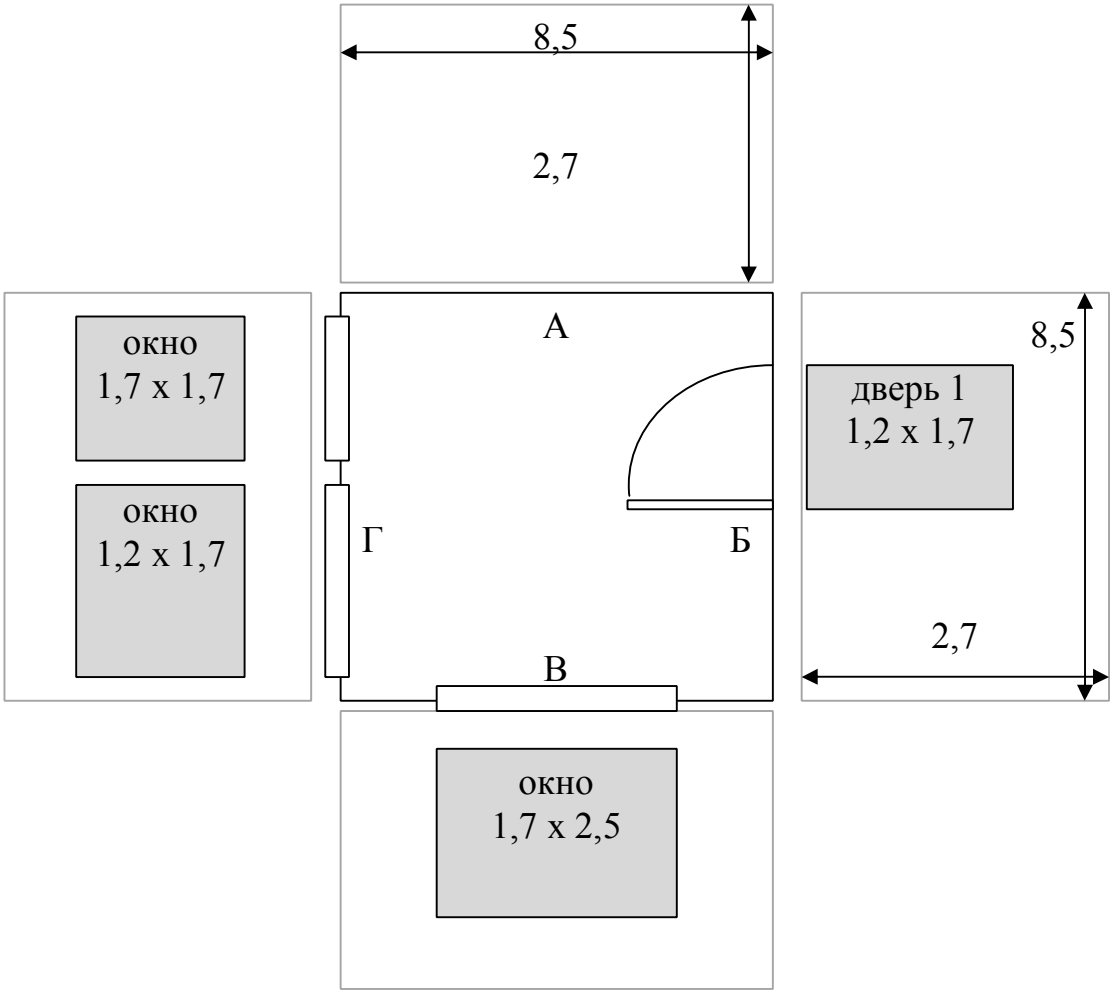


Рис. 1. Развертка помещения

Таблица Т5. Пример исходных данных

Вариант №	$F_{чг}$ (Гц)	Конфигурация (таблицы Т2 – Т4), состав и размеры объектов ограждений (м)			
		А	**Б**	**В**	**Г**
0	**125**	**стена 3** (2,7 х 8,5)	**стена 1** (2,7 х 8,5) **дверь 1** (1,2 х 1,7)	**окно 4** (1,7 х 2,5)	**окно 2** (1,7 х 1,7) **окно 2** (1,2 х 1,7)

Решение

1. Подготовка электронной таблицы для выполнения расчетов.

1.1. Заголовок и блок «исходные данные» (рис. 2).

Защита информации от акустических угроз

1. Исходные данные

Вариант №	$F_{чг}$(Гц)	Конфигурация ограждений			
		А	Б	В	Г
0	125	стена 3 (2,7 x 8,5)	стена 1 (2,7 x 8,5)	окно 4 (1,7 x 2,5)	окно 2 (1,7 x 1,7)
			дверь 1 (1,2 x 1,7)		окно 2 (1,2 x 1,7)

Рис. 2. Заголовок и «исходные данные»

Данные в блоке 1 соответствуют номеру варианта задания, представленного в таблице Т5.

1.2. Подготовить Блок 2 для расчета *Rоб* объектов, из которых состоят ограждения оцениваемого помещения и внести в них исходные данные, соответствующие варианту задания. $К_{об}$ необходимо взять из таблиц Т2 – Т4. При этом $К_{об}$ находится на пересечении столбца $F_{чг}$ и строки, соответствующей номеру объекта (например для $F_{чг}$ = 125 и объекта «*стена 3*» в таблице Т2 находим: $К_{об}$ =*41*) (рис. 3).

На этом и последующих рисунках ячейки электронной таблицы, содержащие данные, имеют белый цвет фона, а ячейки, в которых необходимо создать формулы для выполнения расчетов, окрашены в серый цвет.

2. Определение R объектов *(Rоб)*

Ограждение А					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 3	2,7	8,5	23,0	41,0	58,6

Ограждение Б					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 1	2,7	8,5	23,0	41,0	58,6
Дверь 1	1,2	1,7	2,0	21,0	68,1

Ограждение В					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 4	1,7	2,5	4,3	15,0	77,3

Ограждение Г					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 2	1,7	1,7	2,9	18,0	72,6
Окно 2	1,2	1,7	2,0	18,0	71,1

Рис. 3. Блок 2 для расчета $R_{об}$ объектов ограждений

1.3. Подготовка блока 3 для определения $R_{ог}$ ограждений (рис. 4).

3. Определение R ограждений *(Rог)*

Ограждение	**Rог**
А	58,6
Б	68,1
В	77,3
Г	72,6

Рис. 4. Блок 3 для расчета $R_{ог}$ ограждений А-Г

1.4. Подготовка блока 4 для определения R помещения в целом и выработки рекомендаций по повышению защищенности (рис. 5).

4. R помещения

Текущий (Rтек)	
Требуемый (Rтреб)	
Rтек-Rтреб	

Рис. 5. Блок 4 для расчета R помещения

2. Создание расчетных формул для выполнения вычислений.

2.1. В блок 2 (рис. 3) внести формулы для расчета

– площади объектов ограждения: $S_{об} = l \cdot h$, где l и h длина и высота объекта ограждения соответственно;

– уровня акустического сигнала за объектом ограждения:

$$R_{об} = R_{рс} + 6 + 10 \cdot \lg(S_{о,}) - K_{об},$$

где $R_{рс}$ – уровень речевого сигнала в помещении (принимаем =80 дБ);

$S_{об}$ – площадь объекта (м$^{2)}$;

$K_{об}$ – звукоизолирующая способность объекта (дБ).

2.2. В блок 3 (рис. 4) внести формулы для расчета $R_{ог}$ за ограждениями А-Г соответственно.

Учитывая, что уровень речевого сигнала за ограждением определяется наихудшим (наибольшим) показателем $R_{об}$, из которых состоит ограждение, следует использовать функцию *Max* электронной таблицы, аргументами которой будут $R_{об}$ объектов, из которых состоит ограждение.

2.3. В блок 4 (рис. 5) внести формулы для расчета текущего ($R_{тек}$) и требуемого ($R_{треб}$) уровней речевого сигнала за помещением.

$R_{тек}$ определяется наихудшим (наибольшим) значением из $R_{ог}$ ограждений А, Б, В, Г, т.е. наиболее слабое, в смысле звукоизоляции, ограждение определяет звукоизоляцию помещения в целом.

При наличии серьезного разброса показателей $R_{ог}$ ограждений целесообразно выровнять показатели, приблизив их к некоторому требуемому значению $R_{треб}$. Для простоты примем в качестве требуемого значения среднее значение $R_{ог}$ ограждений А–Г. Стремление к этому значению позволит выровнять показатели уровней речевого сигнала за ограждениями и повысить звукоизоляцию помещения, используя имеющиеся в нашем распоряжении средства (Таблицы Т2–Т4).

Таким образом, для расчета $R_{тек}$ и $R_{треб}$ следует использовать функции электронной таблицы *Макс* и *СрЗнач* соответственно. Аргументами этих функций являются значения $R_{ог}$ из таблицы для расчета

$R_{ог}$ ограждений А–Г (рис.4). Внешний вид электронной таблицы для «0» варианта представлен на рис. 6.

Защита информации от акустических угроз

1. Исходные данные

Вариант №	$F_в$(Гц)	Конфигурация ограждений			
		А	Б	В	Г
0	125	стена 3 (2,7 х 8,5)	стена 1 (2,7 х 8,5)	окно 4 (1,7 х 2,5)	окно 2 (1,7 х 1,7)
			дверь 1 (1,2 х 1,7)		окно 2 (1,2 х 1,7)

2. Определение R объектов *(Rоб)*

Ограждение А					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 3	2,7	8,5	23,0	41,0	58,6

Ограждение Б					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 1	2,7	8,5	23,0	41,0	58,6
Дверь 1	1,2	1,7	2,0	21,0	68,1

Ограждение В					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 4	1,7	2,5	4,3	15,0	77,3

Ограждение Г					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 2	1,7	1,7	2,9	18,0	72,6
Окно 2	1,2	1,7	2,0	18,0	71,1

3. Определение R ограждений *(Rог)*

Ограждение	**Rог**
А	58,6
Б	68,1
В	77,3
Г	72,6

4. R помещения

Текущий (Rтек)	77,3
Требуемый (Rтреб)	69,1
Rтек-Rтреб	**8,1**

Рис. 6. Внешний вид электронной таблицы с выполненными расчетами

В результате выполненных расчетов получены значения *текущего* и *требуемого* уровней речевого сигнала за границей исследуемого помещения. На рис.6 видно, что разница ($R_{тек} – R_{треб}$) = 8,1 Дб.

Для «выравнивания» этих показателей целесообразно заменить некоторые объекты ограждений на аналогичные, но обладающие большим $K_{ог}$.

3. Выработка предложений, направленных на повышение защищенности помещения.

3.1. Анализ $R_{ог}$ ограждений (блок 3 рис. 6).

Из таблицы видно, что за ограждением *В* наибольший уровень речевого сигнала (т.е. здесь звукоизоляция наихудшая). В блоке 2 (рис. 6) находим объекты, из которых состоит ограждение *В*. В данном случае объектом является «окно 4» с $K_{ог}$=15,0. Следовательно, необходимо заменить его на окно с большим $K_{ог}$. В таблице Т3 выбираем окно 7 ($K_{ог}$=25,0). При замене в электронной таблице (ограждение В) значения $K_{ог}$=25,0 наблюдаем следующие изменения: $R_{треб}$=*66, 6* и $R_{тек}$=*72,6.* Разница ($R_{тек} – R_{треб}$) = 6 Дб, что несколько лучше первоначального варианта.

Теперь «узким местом» является ограждение *Г*, состоящее из двух «окон 2» ($K_{ог}$=18,0). Заменяем оба «окна 2» на «окно 7» ($K_{ог}$=25,0). Наблюдаем очередные изменения: $R_{треб}$=*64,9* и $R_{тек}$=*68,1*. Разница ($R_{тек} – R_{треб}$) = 3,2 Дб.

Последняя замена – «дверь 1» на «дверь 6» ($K_{ог}$=22) в ограждении *Б*. Разница ($R_{тек} – R_{треб}$) = 3,1 Дб. Остальные замены дают результат, увеличивающий разницу.

Итоговая электронная таблица представлена на рис. 7.

2. Определение R объектов *(Rоб)*

Ограждение А					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 3	2,7	8,5	23,0	41,0	58,6

Ограждение Б					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Стена 1	2,7	8,5	23,0	41,0	58,6
Дверь6	1,2	1,7	2,0	24,0	65,1

Ограждение В					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 7	1,7	2,5	4,3	25,0	67,3

Ограждение Г					
Объект	**Высота (h), м**	**Длина (l), м**	**Sоб**	**Коб**	**Rоб**
Окно 7	1,7	1,7	2,9	25,0	65,6
Окно 7	1,2	1,7	2,0	25,0	64,1

3. Определение R ограждений *(Rог)*

Ограждение	**Rог**
А	58,6
Б	65,1
В	67,3
Г	65,6

4. R помещения

Текущий (Rтек)	67,3
Требуемый (Rтреб)	64,1
Rтек-Rтреб	**3,1**

Рис. 7. Внешний вид окончательного варианта электронной таблицы

Предложения, направленные на повышение защищенности помещения, следующие:

ограждение *В* – замена «окно 4» на «окно 7»;

ограждение *Г* – замена «окно 2» на «окно 7»;

ограждение *Б* – замена «дверь 1» на «дверь 6».

1.2. Экономическая модель защиты информации

Среди моделей, использующихся при проектировании системы информационной безопасности, наиболее популярной является «экономическая модель». Сущность этой модели основывается на тезисе: «все информационные угрозы в конечном итоге должны быть экономически оправданы».

Действительно, реализация любой информационной угрозы связана с определенными затратами: на изучение обстановки, на разработку плана и технологии реализации угрозы, на приобретение оборудования и необходимых специальных технических средств, кроме того, имеются расходы и на этапе реализации информационной угрозы.

Для реализации системы защиты информации на основе «экономической модели» необходимо получить такой уровень безопасности, при котором стоимость мер безопасности будет ниже стоимости защищаемой информации. Графически это можно представить следующим образом (рис. 8).

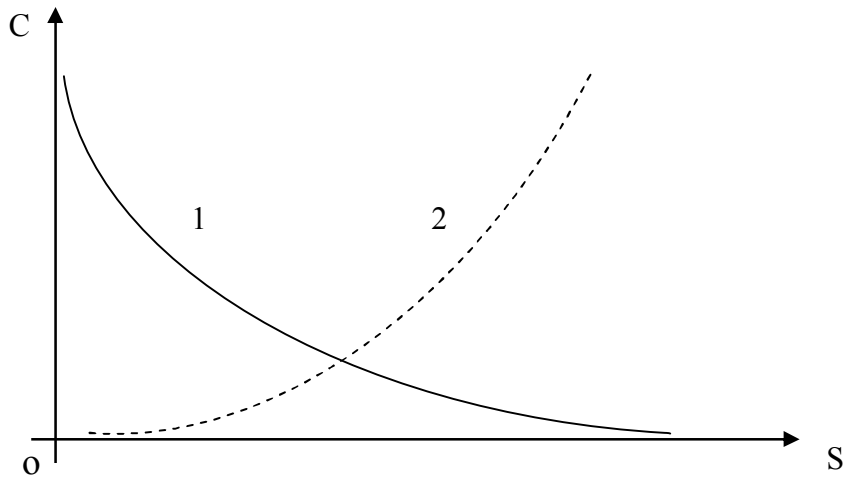


Рис. 8. Иллюстрация идеи «экономической модели»

На рисунке представлен вариант изменения стоимости незащищенной информации (непрерывная линия) при наращивании системы защиты, стоимость которой соответственно растет (штриховая линия) [4].

Источник угрозы рассчитывает, что затраты на преодоление системы защиты информации окупятся сведениями, которые он получит. Мерой такого сопоставления является коэффициент опасности конкретной *i*-й угрозы:

$$\alpha_i = \frac{z_i}{b_i}, \quad (2)$$

где: z_i – эквивалентная стоимость сведений, которые может получить злоумышленник в результате реализации *i* - й угрозы;

b_i – совокупные затраты злоумышленника по реализации *i* - й информационной угрозы;

$i = (\overline{1..n})$, n – число угроз информации.

Очевидно, что чем больше α_i, тем больше вероятность угрозы. Определив перечень информационных угроз можно подобрать и противопоставить им соответствующие средства защиты с мерой s_i – суммарной стоимостью внедрения и эксплуатации за заданный период времени. Используя α_i *и* s_i, можно определить для каждого технического средства **ранговый коэффициент** $\eta_i = F(\alpha_i, s_i)$,

$$\eta_i = \frac{\alpha_i \cdot \omega_i}{s_i}, \quad (3)$$

где ω_i – количество информации (Мб) в i – м канале утечки информации.

Ранговый коэффициент средства защиты позволяет определить качественный состав системы защиты информации. Чем больше величина η_i, тем больше оснований применить данное техническое средство для защиты от соответствующей информационной угрозы.

Применением ранжирования (упорядочивания по убыванию рангового коэффициента) технических средств с последующими расчетами, возможно достигнуть оптимального с точки зрения соотношения стоимостей защищаемой информации и системы ее защиты.

Для расчета эффективности технического средства защиты q_i используем соотношение, определяющее «вклад» *i*-го средства в систему защиты.

$$q_i = \frac{\eta_i s_i}{\sum_{i=1}^{n} \eta_i s_i} \qquad (4)$$

Для оценки эффективности системы защиты Q используем формулу:

$$Q = \sum_{i=1}^{n} q_i \qquad (5)$$

Для оценки стоимости системы защиты S используем формулу:

$$S = \sum_{i=1}^{n} s_i \qquad (6)$$

Для оценки стоимости незащищенной информации Ω используем формулу:

$$\Omega = (\sum_{i=1}^{n} \omega_i - \omega_i) \cdot 1 y.e., \qquad (7)$$

где ω_i – стоимость незащищенной информации при i- конфигурации системы защиты.

Условия и соглашения:

1. Исходные данные для вашего варианта находятся в таблице для задания 2.

2. Проектирование системы защиты акустической информации выполняется поэтапно.

3. При расчетах используется простой аддитивный подход без учета интегративного эффекта, свойственного всем системам.

4. Для выполнения расчетов используется табличный процессор.

Пример решения

Задание. Обоснуйте экономически оправданный состав системы защиты акустической информации.

Таблица Т6. Исходные данные

№	Вид защиты	Вид защиты	Вид угрозы	ω_i, Мб	S_i, у.е.	z_i	b_i
1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816
2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485
3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654
4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648
5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762
6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130

Этап 1. Подготовка электронной таблицы и ввод исходных данных в ячейки (рис. 9)

		№	Вид защиты	Вид защиты	Вид угрозы	ω_i	S_i	z_i	b_i
5									
6		1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816
7		2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485
8		3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654
9		4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648
10		5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762
11		6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130

Рис. 9. Таблица с исходными данными

Этап 2. Расчет коэффициента опасности угрозы α_i с использованием соотношения 2 и рангового коэффициента технического средства защиты η_i (соотношение 3) (рис. 10).

	№	Вид защиты	Вид защиты	Вид угрозы	ω_i	S_i	z_i	b_i	α_i	η_i
6	1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816	10	71,79
7	2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485	15	367,18
8	3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654	9	46,13
9	4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648	6	19,82
10	5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762	12	218,80
11	6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130	3	7,14

Рис. 10. Выполненный этап 2.

Этап 3. Ранжирование данных по убыванию величины рангового коэффициента технического средства защиты (используется инструмент «сортировка по убыванию» по столбцу η_i).

	№	Вид защиты	Вид защиты	Вид угрозы	ω_i	S_i	z_i	b_i	α_i	η_i
6	2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485	15	367,18
7	5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762	12	218,80
8	1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816	10	71,79
9	3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654	9	46,13
10	4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648	6	19,82
11	6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130	3	7,14

Рис. 11. Данные отсортированы по ранговому коэффициенту

Сортировка позволила определить порядок включения технических средств в состав системы защиты информации. Становится понятным, что начинать необходимо с «ЭЭ», а заканчивать «ПФ» (рис. 11).

Этап 4.

Расчет эффективности технического средства защиты q_i с использованием соотношения 4 и оценки эффективности системы в текущем составе Q с использованием соотношения 5 (рис. 12).

5	№	Вид защиты	Вид защиты	Вид угрозы	ω_i	S_i	z_i	b_i	α_i	η_i	q_i	Q
6	2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485	15	367,18	0,321055	0,321055
7	5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762	12	218,80	0,214229	0,535284
8	1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816	10	71,79	0,215973	0,751257
9	3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654	9	46,13	0,15424	0,905497
10	4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648	6	19,82	0,060582	0,966079
11	6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130	3	7,14	0,033921	1

Рис. 12. Выполнена оценка эффективности системы

Этап 5. Оценка стоимости системы и незащищенной информации с использованием соотношений 6 и 7.

Этап 6. Обоснование рационального состава системы с точки зрения экономического подхода

На этом этапе на одной диаграмме необходимо построить графические зависимости:

- изменения стоимости незащищенной информации Ω;
- изменения стоимости системы защиты.

Результат представлен на рис. 14.

5	№	Вид защиты	Вид защиты	Вид угрозы	ω_i	S_i	z_i	b_i	α_i	η_{ii}	q_{ii}	Q	S	стоимость незащищ информации
6	2	Электромагнитная экранировка помещений	ЭЭ	Долговременная радиозакладка с сетевым питанием	48639	1987	97278	6485	15	367,18	0,321055	0,321055	1987	354466
7	5	Повышение звукоизоляции окон и дверей	ПЗ	Направленные микрофоны	40569	2225	81138	6762	12	218,80	0,214229	0,535284	4212	273328
8	1	Радиомониторинг с использованием сканеров	РМ	Вносимая автономная радиозакладка	49079	6836	98158	9816	10	71,79	0,215973	0,751257	11048	175170
9	3	Зашумление естественных звуководов	ЗЕЗ	Использование естественных звуководов	38945	7598	77890	8654	9	46,13	0,15424	0,905497	18646	97280
10	4	Зашумление стен	ЗС	Контроль стен (стетоскопы)	22945	6947	45890	7648	6	19,82	0,060582	0,966079	25593	51390
11	6	Применение фильтров в телефонной сети	ПФ	Проводные телефонные закладки	25695	10793	51390	17130	3	7,14	0,033921	1	36386	0

Рис. 13. Выполнена оценка стоимости системы и информации

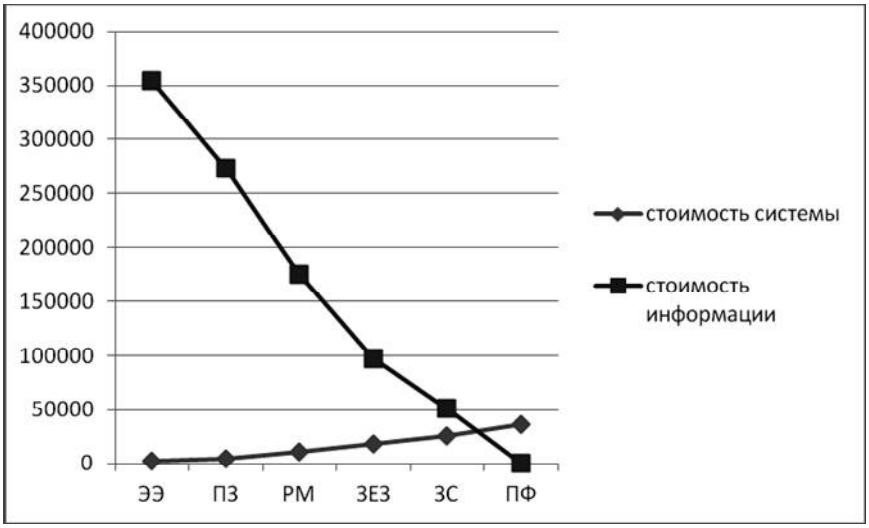


Рис. 14. Графики изменения стоимостей системы и информации

Вывод. Экономически обоснованный состав системы защиты информации включает в себя следующие мероприятия: «электромагнитная экранировка помещений», «повышение звукоизоляции окон и дверей», «радиомониторинг с использованием сканеров», «зашумление естественных звуководов», «зашумление стен, применение фильтров в телефонной сети».

2. Защита компьютерной информации

Одним из методов защиты компьютерной информации в процессе хранения и передачи является секретность – хранение и передача данных в таком виде, чтобы злоумышленник, получив доступ к носителю или среде передачи, не смог получить сами данные.

Рассмотрим более подробно реализацию этого метода защиты. В его основе лежит использование специального математического аппарата, преобразующего информацию в зашифрованную последовательность символов, непригодную для использования.

Для создания и совершенствования подобного математического аппарата развилось и сформировалось такое научно-прикладное направление, как криптология, которое состоит из сочетания двух понятий: крипто – «тайный» и логика – раздел научных познаний о способах доказательств и опровержений.

В свою очередь, научное направление криптология подразделяется на два функционально зависимых структурно логико-математических и технических направления: криптография и криптоанализ.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблему конфиденциальности (путем лишения противника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи).

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рисунке 15.

Отправитель генерирует открытый текст исходного сообще-

ния М. которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение.

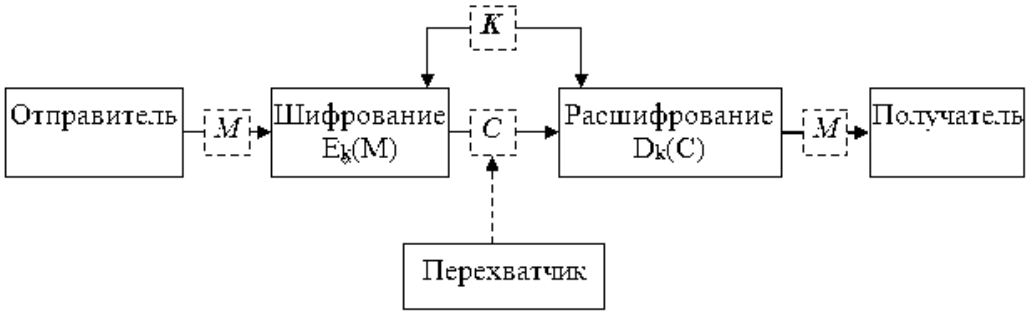


Рис. 15. Обобщенная схема криптосистемы

Для того чтобы перехватчик не смог узнать содержание сообщения *M* отправитель шифрует его с помощью обратимого преобразования E_k и получает шифртекст (или криптограмму) $C=E_k(M)$, который отправляет получателю.

Законный получатель, приняв шифртекст *C*, расшифровывает его с помощью обратного преобразования $D=E_k^{-1}$ и получает исходное сообщение в виде открытого текста *M: Dk(C)= Ek-1(Ek(M))=M.*

Преобразование E_k выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом *K*.

2.1. Традиционная (симметричная) криптография

К основным традиционным методам криптографии относятся следующие: моно и многоалфавитная подстановка (замена), перестановки символов по определенному правилу, гаммирование и блочные шифры.

Моно и многоалфавитная подстановка. Заключается в замене символов исходного текста на другие (того же алфавита) по определенному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Типичным примером моноалфавитной подстановки является шифр Цезаря.

Ключом преобразования в этом случае является формулы:

зашифровывания: $e_i = (t_i + k) \bmod N,$ (8)

расшифровывания: $t_i = (e_i - k + N) \bmod N,$ (9)

где e_i – числовой эквивалент (порядковый номер) символа шифртекста в алфавите, t_i – числовой эквивалент символа текста, k – смещение (сдвиг) относительно исходного положения символа в алфавите, N – мощность алфавита (количество символов алфавита), функция *mod* возвращает остаток от целочисленного деления (например, *67 mod 32=3*).

Символы алфавита, соответствующие рассчитанным по формулам 8 и 9 числовым эквивалентам символы представлены в таблице Т 7.

Таблица Т7. Символы алфавита

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Задание 1. Методом одноалфавитной подстановки, сдвиг k=15 зашифровать сообщение: *«сбор отменен»*.

Решение

Зашифруем символ «*с*».

1. Определяем по таблице Т7 t_1 («*с*») =17.

2. Используя соотношение 8, рассчитаем e_1.

$$e_1 = (17 + 15) \bmod 32 = 32 \bmod 32 = 0$$

3. Символ с числовым эквивалентом 1 – *«а»*.

Для наглядности представим процесс зашифровывания в виде таблицы.

Таблица Т8. Пример зашифровывания

Исходное сообщение	*с*	*б*	*о*	*р*	*о*	*т*	*м*	*е*	*н*	*е*	*н*
t_i	17	1	14	16	14	18	12	5	13	5	13
e_i	0	16	29	31	29	1	27	20	28	20	28
Зашифрованное сообщение	*а*	*р*	*э*	*я*	*э*	*б*	*ы*	*ф*	*ь*	*ф*	*ь*

Таким образом исходное сообщение *«сбор отменен»* в результате зашифровывания преобразовалось в *«арэя эбыфьф»*.

Задание 2. Методом одноалфавитной подстановки, сдвиг k=15 расшифровать сообщение: *«арэя эбыфьф».*

Решение

Расшифруем символ «*а*».

1. Определяем по таблице Т7 e_1 («*а*») =0.

2. Используя соотношение 9, рассчитаем t_1.

$$t_1 = (0 - 15 + 32) \bmod 32 = 17 \bmod 32 = 17$$

3. Символ с числовым эквивалентом 17 – *«с»*.

Для наглядности представим процесс расшифровывания в виде таблицы.

Таблица Т9. Пример расшифровывания

Зашифрованное сообщение	*а*	*р*	*э*	*я*	*э*	*б*	*ы*	*ф*	*ь*	*ф*	*ь*
e_i	0	16	29	31	29	1	27	20	28	20	28
t_i	17	1	14	16	14	18	12	5	13	5	13
Исходное сообщение	*с*	*б*	*о*	*р*	*о*	*т*	*м*	*е*	*н*	*е*	*н*

Таким образом исходное сообщение *«сбор отменен»* в результате зашифровывания преобразовалось в *«арэя эбыфьф»*.

Многоалфавитная подстановка (замена). Для шифрования используется несколько алфавитов, в результате один и тот же символ в исходном сообщении может быть заменен различными символами.

Частным случаем многоалфавитной подстановки можно рассматривать шифр Вижинера (в другом переводе – *Виженера*). Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо в книге «La cifra del. Sig.» в 1553 году, однако в XIX веке получил имя Блеза Вижинера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Существует два варианта использования шифра: с помощью «квадрата Вижинера» и с помощью расчетных формул. Последний способ применим тогда, когда символы алфавита пронумерованы (таблица Т 7). В качестве ключа шифрования выбирается слово, при этом, чем длиннее ключ, тем более стойким к криптоанализу будет зашифрованное сообщение.

Символы ключа записываются под символами сообщения. Если символов ключа не хватает, то ключ повторяется до последнего символа исходного сообщения.

Преобразование в этом случае осуществляется по формулам:

зашифровывание: $e_i = (t_i + k_j) \bmod N,$ (10)

расшифровывание: $t_i = (e_i - k_j + N) \bmod N,$ (11)

где $\boldsymbol{e_i}$ – числовой эквивалент (порядковый номер) символа шифртекста в алфавите, $\boldsymbol{t_i}$ – числовой эквивалент символа текста, $\boldsymbol{k_j}$ – числовой эквивалент символа ключа в алфавите, $\boldsymbol{N}$ – мощность алфавита (количество символов алфавита), функция *mod* возвращает остаток от целочисленного деления.

Символы алфавита, соответствующие рассчитанным по формулам 8 и 9 числовым эквивалентам символы представлены в таблице Т 7.

Задание 3. Шифром Вижинера, ключ «*тайнопись*» зашифровать сообщение: *«сбор отменен».*

Решение

Зашифруем первый символ сообщения «*с*».

1. Определяем по таблице Т7 $\boldsymbol{t_1}$ («*с*») =17.

2. Определяем по таблице Т7 $\boldsymbol{k_1}$ («*т*») = 18.

2. Используя соотношение 10, рассчитаем $\boldsymbol{e_1}$.

$$e_1 = (17 + 18) \bmod 32 = 35 \bmod 32 = 3$$

3. Символ с числовым эквивалентом 3 – *«г»*.

Для наглядности представим процесс зашифровывания в виде таблицы.

Таблица Т10. Пример зашифровывания

Исходное сообщение	*с*	*б*	*о*	*р*	*о*	*т*	*м*	*е*	*н*	*е*	*н*
t_i	17	1	14	16	14	18	12	5	13	5	13
Ключ	*т*	*а*	*й*	*н*	*о*	*п*	*и*	*с*	*ь*	*т*	*а*
k_j	18	0	9	13	14	15	8	17	28	18	0
e_i	3	1	23	29	28	1	20	22	9	23	13
Зашифрованное сообщение	*г*	*б*	*ч*	*э*	*ь*	*б*	*ф*	*ц*	*й*	*ч*	*н*

Таким образом исходное сообщение *«сбор отменен»* в результате зашифровывания преобразовалось в *«гбчэ ьбфцйчн»*.

Видно, что в отличии от одноалфавитной подстановки, в приведенном примере один и тот же символ (например «*о*») в зашифрованном сообщении представлен символами «*ч*» и «*ь*», что размывает статистическую «картинку» и затрудняет применение частотного криптоанализа.

Задание 4. Расшифровать зашифрованное шифром Вижинера сообщение *«гбчэ ьбфцйчн»*, ключ «*тайнопись*».

Решение

Расшифруем первый символ «*г*».

1. Определяем по таблице Т7 e_1 («*г*») =3.
2. Определяем по таблице Т7 k_1 («*т*») = 18.
2. Используя соотношение 11, рассчитаем t_1.

$$t_1 = (3 - 18 + 32) \bmod 32 = 17 \bmod 32 = 17$$

3. Символ с числовым эквивалентом 21 – *«с»*.

Для наглядности представим процесс расшифровывания в виде таблицы.

Таблица Т11. Пример зашифровывания

Зашифрованное сообщение	*г*	*б*	*ч*	*э*	*ь*	*б*	*ф*	*ц*	*й*	*ч*	*н*
e_i	3	1	23	29	28	1	20	22	9	23	13
Ключ	*т*	*а*	*й*	*н*	*о*	*п*	*и*	*с*	*ь*	*т*	*а*
k_j	18	0	9	13	14	15	8	17	28	18	0
t_i	17	1	14	16	14	18	12	5	13	5	13
Исходное сообщение	*с*	*б*	*о*	*р*	*о*	*т*	*м*	*е*	*н*	*е*	*н*

Таким образом полученное сообщение *«гбчэ ьбфцйчн «* после расшифровывания преобразовалось в *«сбор отменен»*.

Перестановки. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам.

Алгоритм метода множественной перестановки.

1. Построить таблицу, размер которой определяется размерами двух ключевых слов («ключей»), при этом буквы в одном ключе не должны повторяться. Ключи выписываются сверху и сбоку таблицы.

2. В таблицу по определенному маршруту (рис. 16) заносится исходный текст, а неиспользованные места полностью заполняются любыми, но лучше всего часто встречающимися буквами.

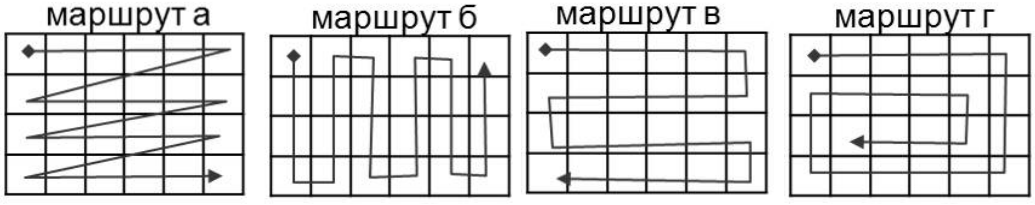


Рис. 16. Варианты маршрутов

3. Переместить столбцы в порядке, соответствующем взаимному расположению букв ключа № 1 в алфавите.

4. Переместить строки в соответствий с последовательностью букв ключа № 2 в алфавите.

5. Выписать последовательно буквы из получившейся таблицы, стандартно разбивая их на пятизнаковые группы, причем если последняя из них окажется неполной, она дописывается любыми часто встречающимися буквами.

Расшифровка производится в обратном порядке.

Пример зашифровывания и **расшифровывания** методом множественной перестановки.

Задание. Зашифровать сообщение *«встреча на прежнем месте»* методом множественной перестановки. Маршрут записи – «*а*», ключи: «*кефаль*», «*грот*».

Решение

1.		***к***	***е***	***ф***	***а***	***л***	***ь***
		3	***2***	***5***	***1***	***4***	***6***
г	***1***	в	с	т	р	е	ч
р	***3***	а	н	а	п	р	е
о	***2***	ж	н	е	м	м	е
т	***4***	с	т	е	**с**	**в**	**и**

Примечание: буквы «с, в, и» дописываем в конце для заполнения всех ячеек таблицы.

1. Строим таблицу, в которую записываем ключ 1, ключ 2 и исходное сообщение, используя маршрут «*а*» (рис. 16). Расставляем номера взаимного расположения букв ключа в алфавите (например, «а» стоит раньше остальных букв, поэтому ей присваиваем «1»), «ь» – последняя из букв ключа в алфавите, поэтому ей присваиваем – «6».

2.		***а***	***е***	***к***	***л***	***ф***	***ь***
		1	***2***	***3***	***4***	***5***	***6***
г	***1***	р	с	в	е	т	ч
р	***3***	п	н	а	р	а	е
о	***2***	м	н	ж	м	е	е
т	***4***	с	т	с	в	е	и

2. Перемещаем столбцы в порядке, соответствующем взаимному расположению букв ключа 1 («*кефаль*») в обычном алфавите.

3.		***а***	***е***	***к***	***л***	***ф***	***ь***
		1	***2***	***3***	***4***	***5***	***6***
г	***1***	р	с	в	е	т	ч
о	***2***	м	н	ж	м	е	е
р	***3***	п	н	а	р	а	е
т	***4***	с	т	с	в	е	и

3. Перемещаем строки в порядке, соответствующем взаимному расположению букв ключа 2 («*грот*») в обычном алфавите.

4. Выписываем последовательно буквы из получившейся таблицы, стандартно разбивая их на пятизнаковые группы, причем если последняя из них окажется неполной, она дописывается любыми часто встречающимися буквами.

Зашифрованное сообщение: *«рсвет чмнжм еепна раест свеи**с**»*.

Задание. Расшифровать сообщение *«рсвет чмнжм еепна раест свеи**с**»* методом множественной перестановки. Маршрут записи – «*а*», ключи: «*кефаль*», «*грот*».

Решение

1.		*а*	*е*	*к*	*л*	*ф*	*ь*
		1	*2*	*3*	*4*	*5*	*6*
г	*1*	р	с	в	е	т	ч
о	*2*	м	н	ж	м	е	е
р	*3*	п	н	а	р	а	е
т	*4*	с	т	с	в	е	и

1. Сообщение вписывается в таблицу определяемую длинами ключей (размера 6x4) столбцы и строки в ней последовательно нумеруются, а избыток букв отбрасывается.

2.		*а*	*е*	*к*	*л*	*ф*	*ь*
		1	*2*	*3*	*4*	*5*	*6*
г	*1*	р	с	в	е	т	ч
р	*3*	п	н	а	р	а	е
о	*2*	м	н	ж	м	е	е
т	*4*	с	т	с	в	е	и

2. Перемещаем строки в порядке, соответствующем взаимному расположению букв ключа 2 («*грот*») в обычном алфавите.

3.		*к*	*е*	*ф*	*а*	*л*	*ь*
		3	*2*	*5*	*1*	*4*	*6*
г	*1*	в	с	т	р	е	ч
р	*3*	а	н	а	п	р	е
о	*2*	ж	н	е	м	м	е
т	*4*	с	т	е	с	в	и

3. Перемещаем столбцы в порядке, соответствующем взаимному расположению букв ключа 1 («*кефаль*») в обычном алфавите.

4. буквы выписываются в строку, следуя обговоренному маршруту заполнения-чтения.

Расшифрованное сообщение: *«встреча на прежнем месте»*.

Гаммирование. Эта группа методов заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры. Представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста.

2.2. Асимметричная криптография

Слабым местом криптографических систем, при их практической реализации, является проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами информационной системы, ключ должен быть сгенерирован одним из них, а затем, в конфиденциальном порядке, передан другому.

В общем случае для передачи ключа опять же требуется использование криптосистемы. Для решения этой проблемы на основе результатов, полученных классической и современной математикой, были предложены системы с открытым ключом. Суть их состоит в том, что каждым адресатом информационной системы генерируются два ключа, связанные между собой по определенному правилу.

Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом и передается адресату. Зашифрованный текст не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только адресату (рис. 17). Здесь ИС –

исходное сообщение, ОК – открытый ключ, ШС – зашифрованное сообщение, ЗК – закрытый ключ.

Асимметричные криптографические системы используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении *x* относительно просто вычислить значение *y=f(x)*.

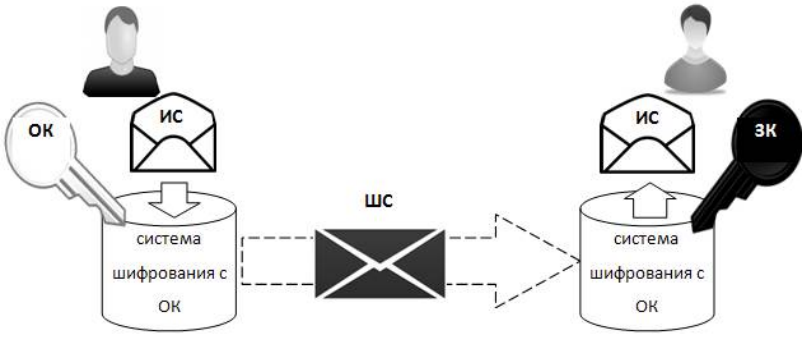


Рис. 17. Обобщенная схема асимметричного шифрования

При этом, если известен у, то нет простого пути для вычисления значения х. Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах.

Алгоритмы криптосистем с открытым ключом можно использовать как:

– самостоятельные средства защиты передаваемых и хранимых данных;

– средства для распределения ключей;

– средства аутентификации пользователей.

Алгоритмы криптосистем с открытым ключом более трудоемки, чем традиционные криптосистемы, поэтому использование их в качестве самостоятельных средств защиты нерационально. Поэтому на практике рационально с помощью криптосистем с открытым ключом распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

Несмотря на довольно большое число различных криптосистем с открытым ключом, наиболее популярна – криптосистема RSA, разработанная в 1977 г. и получившая название в честь ее создателей: Ривеста, Шамира и Эйдельмана.

Ривест, Шамир и Эйдельман воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению.

Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Метод распространения ключей Диффи-Хеллмана

Передача ключа по открытым каналам была большой проблемой криптографии 20 века, но эту проблему удалось решить после появления метода Диффи-Хеллмана. Этот метод позволил дать ответ на главный вопрос:

«Как при обмене зашифрованными посланиями уйти от необходимости передачи секретного кода расшифровки, который, как правило, не меньше самого послания»?

Открытое распространение ключей Диффи-Хеллмана позволяет паре пользователей системы выработать общий секретный ключ, не обмениваясь секретными данными.

Предположим, существует два абонента: ***A1*** и ***B1***. Обоим абонентам известны некоторые два числа ***g*** и ***p***, которые не являются секретными и могут быть известны также другим заинтересованным лицам.

Для того, чтобы создать не известный более никому секретный ключ:

Шаг 1. Оба абонента генерируют большие случайные числа: ***A1*** – число ***a***, ***B1***– число ***b***.

Шаг 2**.** ***A1*** вычисляет значение *A* и пересылает его ***B1***:

$$A = g^a \bmod p \qquad (12)$$

Шаг 3. ***B1*** вычисляет *B* и пересылает его ***A1***

$$B = g^b \bmod p \qquad (13)$$

Предполагается, что злоумышленник может перехватить оба эти значения (*A* и *B*), но не изменить (подменить) их.

На втором этапе ***A1*** на основе имеющегося у него ***a*** и полученного по сети ***B*** вычисляет значение ***K***

$$K = B^a \bmod p \qquad (14)$$

Подставив в формулу 14 значение *B* (соотношение 13), получим

$$K = g^{ab} \bmod p \qquad (15)$$

B1 на основе имеющегося у него ***b*** и полученного по сети ***A*** вычисляет свое значение ***K***:

$$K = A^b \bmod p \qquad (16)$$

Подставив в формулу 16 значение *A* (соотношение 12), получим

$$K = g^{ab} \bmod p \qquad (17)$$

Как нетрудно видеть, у ***A1 и B1*** получилось одно и то же число ***K*** (соотношения 15, 17).

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления (15) или (17) по перехваченным ***A*** и ***B***, если числа ***p***, ***a***, ***b*** выбраны достаточно большими. Наглядная работа алгоритма показана на рисунке 18.

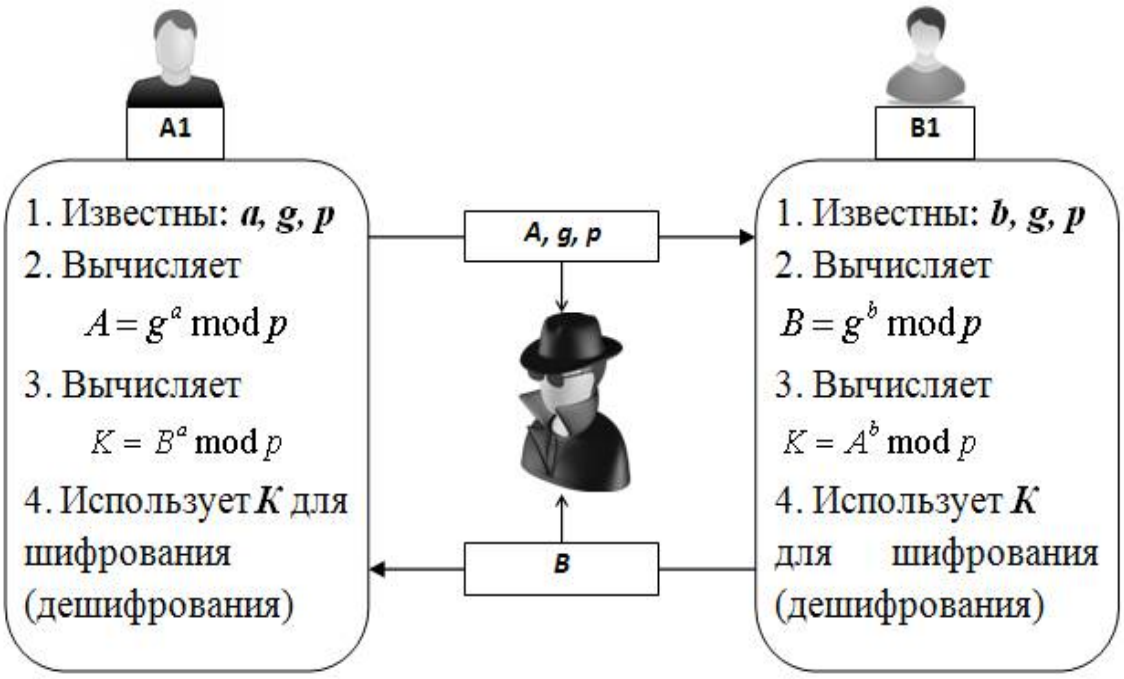


Рис. 18. Метод распространения ключей Диффи-Хеллмана

В практических реализациях для ***a*** и ***b*** используются числа порядка *10100* и ***p*** порядка *10300*. Число ***g*** не обязано быть большим и обычно имеет значение в пределах первого десятка.

Задание. Используя метод Диффи-Хелмана, создать открытый ключ, передать его абоненту по переписке и использовать его для шифрования и дешифрования сообщений.

Исходные данные: *g=3851*, *p=7319, a=1221, b=2112.*

Алгоритм действий.

Этап 1. Абоненту ***A1***:

– используя метод Диффи-Хеллмана, создать открытый ключ ***A***;

– передать созданный открытый ключ абоненту ***B1***.

Этап 2. Абоненту ***B1*** после получения открытого ключа ***A***:

– сгенерировать сеансовый ключ ***K***;

– зашифровать с его помощью сообщение «*перехват*» методом Вижинера (см. п.2.1), используя цифры числа ***K*** в качестве цифр ключа;

– используя метод Диффи-Хеллмана создать открытый ключ ***B***;

– передать открытый ключ ***B*** и зашифрованное сообщение абоненту ***A1***.

Этап 3. Абоненту ***A1*** после получения открытого ключа ***B*** и зашифрованного сообщения:

– сгенерировать сеансовый ключ ***K***;

– расшифровать с его помощью сообщение «*перехват*» методом Вижинера (см. п.2.1), используя цифры числа ***K*** в качестве цифр ключа;

– зашифровать с помощью ***K*** сообщение «*операция*» методом Вижинера (см. п.2.1), используя цифры числа ***K*** в качестве цифр ключа;

– передать открытый ключ ***A*** и зашифрованное сообщение абоненту ***B1***.

Решение (расчеты выполняются с помощью стандартного калькулятора в режиме инженерных расчетов).

Этап 1. Абонент ***A1***:

1. Использует для получения открытого ключа ***A*** свой секретный ключ ***a*** и соотношение 12:

$A=g^a \bmod p=3851^{1221} \bmod 7319=\mathbf{79}$

2. Передает открытый ключ ***A=79*** абоненту ***A2***.

Этап 2. Абонент ***A2***:

1. Получает открытый ключ ***A=79***.

2. Генерирует сеансовый ключ ***K*** (соотношение 16) используя открытый ключ ***A*** и свой секретный ключ ***b***:

$K=A^b \bmod p= 79^{2112} \bmod 7319=\mathbf{4486}$.

3. Шифрует сообщение «***перехват***» методом Вижинера, используя в качестве ключа цифры сеансового ключа ***K=4486***, при этом записывать вместо цифр соответствующие им буквы алфавита не имеет смысла, т.к. ключ дальнейшей передаче не подлежит:

Исходное сообщение	*п*	*е*	*р*	*е*	*х*	*в*	*а*	*т*
t_i	15	5	16	5	21	2	0	18
Ключ k_j	4	4	8	6	4	4	8	6
e_i	19	9	24	11	25	6	8	24
Зашифрованное сообщение	*у*	*й*	*ш*	*л*	*щ*	*ж*	*и*	*т*

3. Использует для получения открытого ключа ***B*** свой секретный ключ ***b*** и соотношение 13: $\boldsymbol{B}=g^b \bmod p=3851^{2112} \bmod 7319=\boldsymbol{963}$

4. Отправляет зашифрованное сообщение «***уйшлщжит***» и открытый ключ ***B*** абоненту ***A1***.

Этап 3. Абонент ***A1*** после получения открытого ключа ***B*** и зашифрованного сообщения:

1. Генерирует сеансовый ключ ***K*** (соотношение 16) используя открытый ключ ***B*** и свой секретный ключ ***a***: $\boldsymbol{K}=B^a \bmod p= 963^{1221} \bmod 7319=\boldsymbol{4486}$

Видно, что сеансовые ключи обоих абонентов совпадают.

2. Расшифровывает с его помощью сообщение ***«уйшлщжит»*** методом Вижинера (см. п. 2.1), используя в качестве ключа цифры сеансового ключа ***K***:

Зашифрованное сообщение	*у*	*й*	*ш*	*л*	*щ*	*ж*	*и*	*т*
t_i	19	9	24	11	25	6	8	24
Ключ k_j	4	4	8	6	4	4	8	6
e_i	15	5	16	5	21	2	0	18
Исходное сообщение	*п*	*е*	*р*	*е*	*х*	*в*	*а*	*т*

3. Криптоанализ

Криптоанализом (от греческого krypts – «скрытый» и analein – «ослаблять» или избавлять») называют науку восстановления (дешифрования) открытого текста без доступа к ключу. Два последних десятилетия ознаменовались резким ростом числа открытых работ по криптологии, а криптоанализ становится одной из наиболее активно развивающихся областей исследований. Появился целый арсенал математических методов, представляющих интерес для криптоаналитика. Кроме того, повышение производительности вычислительной техники сделало возможными такие типы атак, которые раньше были неосуществимы.

Появление новых криптографических алгоритмов приводит к разработке методов их взлома. Если целью криптоаналитика является раскрытие возможно большего числа шифров (независимо от того, хочет ли он этим нанести ущерб обществу, предупредить его о возможной опасности или просто получить известность), то для него наилучшей стратегией является разработка универсальных методов анализа. Вместе с тем, эта задача является также и наиболее сложной. Результатом возникновения каждого нового метода криптоанализа является пересмотр оценок безопасности шифров, что, в свою очередь, влечет необходимость создания более стойких шифров. Таким образом, исторические этапы развития криптографии и криптоанализа неразрывно связаны.

Опишем некоторые методы криптоанализа:

Метод полного перебора. Заключается в подборе ключа шифрования путем перебора всех возможных комбинаций сисмволов ключа. До появления компьютеров применялся редко ввиду высокой трудоемкости метода. С появлением высокопроизводительной вычислительной техники у криптоаналитиков появилась возможность вскрывать шифры методом перебора ключей.

При осуществлении попытки атаки на основе только шифртекста криптоаналитику требуется анализировать выходные данные алгоритма и проверять их «осмысленность». В случае, когда в качестве объекта шифрования выступает графический файл или программа, задача определения «осмысленности» выходных данных становится очень трудной.

Если известно, что открытый текст представляет собой предложение на естественном языке, проанализировать результат и опознать успешный исход дешифрования сравнительно несложно, тем более что криптоаналитик зачастую располагает некоторой априорной информацией о содержании сообщения. Задачу выделения осмысленного текста, т.е. определения факта правильной дешифрации, решают при помощи ЭВМ с использованием теоретических положений, разработанных в конце XIX века петербургским математиком Марковым А. А. цепей Маркова.

Атака по ключам. Одной из причин ненадежности криптосистем является использование слабых ключей. Фундаментальное допущение криптоанализа, впервые сформулированное О. Кирхгоффом, состоит в том, что секретность сообщения всецело зависит от ключа, т.е. весь механизм шифрования, кроме значения ключа, известен противнику (секретность алгоритма не является большим препятствием: для определения типа программно реализованного криптографического алгоритма требуется лишь несколько дней инженерного анализа исполняемого кода). Слабый ключ – это ключ, не обеспечивающий достаточного уровня защиты или использующий в шифровании закономерности, которые могут быть взломаны. Алгоритм шифрования не должен иметь слабых ключей. Если это невозможно, то количество слабых ключей должно быть минимальным, чтобы уменьшить вероятность случайного выбора одного из них; все слабые ключи должны быть известны заранее, чтобы их можно было отбраковать в процессе создания ключа.

Линейный криптоанализ. Является комбинированным методом, сочетающим в себе поиск линейных статаналогов для уравнений шифрования, статистический анализ имеющихся открытых и шифрованных текстов, использующий также методы согласования и перебора. Этот метод исследует статистические линейные соотношения между отдельными координатами векторов открытого текста, соответствующего шифртекста и ключа, и использует эти соотношения для определения статистическими методами отдельных координат ключевого вектора.

Криптоанализ по побочным каналам. Атаки по сторонним, или побочным, каналам используют информацию, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом. Такие атаки основаны на корреляции между значениями физических параметров, измеряемых в разные моменты во время вычислений, и внутренним состоянием вычислительного устройства, имеющим отношение к секретному ключу. Этот подход менее обобщенный, но зачастую более мощный, чем классический криптоанализ.

Частотный криптоанализ. Основывается на предположении существования характерной закономерности сочетания букв, использования отдельных слов и их сочетаний в национальных языках.

Упрощенно, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам и т.д. в случае полиалфавитных шифров.

Метод частотного криптоанализа известен с IX-го века, хотя наиболее известным случаем его применения в реальной жизни, возможно, является дешифровка египетских иероглифов Ж.-Ф. Шам-

польоном в 1822 году. В художественной литературе наиболее известными упоминаниями являются рассказы «Золотой жук» Эдгара По, «Пляшущие человечки» Конан Дойля, а также роман «Дети капитана Гранта» Жюль Верна.

Начиная с середины XX века большинство используемых алгоритмов шифрования разрабатываются изначально устойчивыми к частотному криптоанализу, поэтому он применяется, в основном, для обучения.

3.1. Метод полного перебора («грубой силы»)

Основывается на конечности числа символов алфавита, из которого состоит ключ шифрования.

Полный перебор (метод «грубой силы» , «brute force») относится к классу методов поиска решения исчерпыванием всевозможных вариантов. Сложность полного перебора зависит от количества всех возможных решений задачи. Если пространство решений очень велико, то полный перебор может не дать результатов в течение нескольких лет или даже столетий.

В криптографии на вычислительной сложности полного перебора основывается оценка криптостойкости шифров. В частности, шифр считается криптостойким, если не существует метода «взлома» существенно более быстрого, чем полный перебор всех ключей. Криптографические атаки, основанные на методе полного перебора, являются самыми универсальными, но и самыми долгими.

В криптографии на полном переборе основывается криптографическая атака методом «грубой силы». Ее особенностью является возможность применения против любого практически используемого шифра [5]. Однако такая возможность существует лишь теоретически, зачастую требуя нереалистичные временные и ресурсные затраты. Наиболее оправдано использование атаки методом «грубой силы» в тех случаях, когда не удается найти слабых мест в системе шифро-

вания, подвергаемой атаке (либо в рассматриваемой системе шифрования слабых мест не существует). При обнаружении таких недостатков разрабатываются методики криптоанализа, основанные на их особенностях, что способствует упрощению взлома.

Устойчивость к подобным атакам определяет используемый в криптосистеме ключ шифрования. Так, с увеличением длины ключа сложность взлома этим методом возрастает экспоненциально. В простейшем случае шифр длиной в N битов взламывается, в наихудшем случае, за время, пропорциональное 2^N [6]. Среднее время взлома в этом случае в два раза меньше и составляет 2^{N-1}.

Современные персональные компьютеры позволяют взламывать пароли полным перебором вариантов с некоторой эффективностью. Однако, при оптимизации атаки, основанной на параллельных вычислениях, эффективность атаки можно существенно повысить. В процессе улучшения системы информационной безопасности по отношению к атаке полным перебором можно выделить два основных направления:

– повышение требований к ключам доступа от защищаемой информации;

– повышение надежности всех узлов системы безопасности.

Может показаться, что с ростом мощности компьютеров разрядность ключа, достаточная для обеспечения безопасности информации против атаки методом полного перебора, будет неограниченно расти. Однако это не так. Существуют фундаментальные ограничения вычислительной мощности, наложенные структурой вселенной: например, скорость передачи любого сигнала не может превышать скорость распространения света в вакууме, а количество атомов во Вселенной (из которых, в конечном счете, состоят компьютеры) огромно, но конечно.

Минимальный размер ключа, необходимый для защиты информации от атак злоумышленника, будет расти по мере повышения быстродействия компьютеров, тем не менее приведенные вычисления

показывают, что существует возможность выбрать такую длину ключа, что атаку методом полного перебора будет провести в принципе невозможно, вне зависимости от повышения вычислительной мощности компьютеров или успехов в области классической теории алгоритмов.

Для проведения эксперимента по определению стойкости ключа к взлому методом полного перебора понадобится любой программный продукт, позволяющий формировать ключи заданной длины и при этом, состоящие из определенного набора символов. Вторым условием успешности эксперимента является автоматизация процесса подстановки ключа в исследуемый файл.

Кроме этого, программа должна показывать время, затраченное на подбор ключа и количество ключей, формируемых в единицу времени.

Для выполнения вычислений используем следующие соотношения:

1. Число возможных ключей n:

$$n = N^k, \tag{18}$$

где N – мощность алфавита, k – длина ключа.

2. Максимальное время нахождения ключа (в секундах) $t_{макс.с}$:

$$t_{макс.с.} = \frac{n}{v}, \tag{19}$$

где v – количество ключей, подбираемых в секунду.

Допустим, что подбор ключа идет классическим образом, начиная от первого символа алфавита и заканчивая последней возможной комбинацией без оптимизации, например методом распараллеливания вычислений. В этом случае $t_{макс.с}$ характеризует время перебора всех возможных комбинаций.

Другим вопросом, который является достаточно интересным, является вопрос определения длины ключа заданной стойкости.

«Заданная» стойкость означает максимально возможное время раскрытия ключа с учетом принятых ранее допущений.

Для определения этого параметра используем следующие соотношения:

1. Число ключей *s*, которые способна перебрать программа за определенный период $t_{cm.c}$ *(секунд)*:

$$s = v \cdot t_{cm.c} \tag{20}$$

2. Длина ключа *k* «заданной» стойкости:

$$k = \log_N(s), \tag{21}$$

где *N* –мощность алфавита.

3.2. Частотный криптоанализ

Утверждается, что вероятность появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются статистическим закономерностям: например, пара стоящих рядом букв «ся» в русском языке более вероятна, чем «цы», а «оь» в русском языке не встречается вовсе. Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст.

Как упоминалось выше, важными характеристиками текста являются повторяемость букв (количество различных букв в каждом языке ограничено), пар букв, то есть m (m-грамм), сочетаемость букв друг с другом, чередование гласных и согласных и некоторые другие особенности. Примечательно, что эти характеристики являются достаточно устойчивыми.

В общем смысле частоту букв в процентном выражении можно определить следующим образом: подсчитывается сколько раз она встречается в шифротексте, затем полученное число делится на об-

щее число символов шифротекста; для выражения в процентном выражении, еще умножается на 100.

Существует некоторая разница значений частот, которая объясняется тем, что частоты существенно зависят не только от длины текста, но и от характера текста. Например, текст может быть технического содержания, где редкая буква «ф» может стать довольно частой. Поэтому для надежного определения средней частоты букв желательно иметь набор различных текстов.

Частотность – термин лексикостатистики, предназначенный для определения наиболее употребительных слов (символов).

Расчет осуществляется по формуле:

$$F_x = \frac{Q_x}{Q_{all}}, \qquad (22)$$

где F_x – частотность слова (символа) «x», Q_x – количество употреблений слова (символа) «x», Q_{all} – общее количество слов (символов). В большинстве случаев частотность выражается в процентах:

$$F_x = \frac{Q_x}{Q_{all}} \cdot 100\% .$$

В словарях частотность слов может отражаться пометами – «употребительное», «малоупотребительное» и т. д. Частотный анализ используется в криптографии для выявления наиболее частотных букв того или иного языка. В таблице Т12 приведена частотность букв русского языка на основе данных о «частотах словоформ и словосочетаний», приведенных организацией «Национальный корпус русского языка», занимающейся вопросами анализа текущего состояния и тенденций развития устной и письменной русской речи.

Таблица Т12.

ранг	буква	употреблений	ранг	буква	употреблений	ранг	буква	употреблений
1	о	52295949	12	м	15252377	23	й	5753983
2	е	40392978	13	д	14173134	24	х	4597146
3	а	38081816	14	п	13349597	25	ж	4476464
4	и	35075552	15	у	12452612	26	ш	3420179
5	н	31900994	16	я	9528713	27	ю	3044673
6	т	30084462	17	ы	9036813	28	ц	2314208
7	с	26058590	18	ь	8263123	29	щ	1719607
8	р	22595850	19	г	8031521	30	э	1573696
9	в	21582499	20	з	7811723	31	ф	1268926
10	л	20678280	21	б	7579289	32	ъ	175908
11	к	16599539	22	ч	6904749	33	е	63623

Таблица содержит буквы, ранжированные по числу употреблений в значительном числе текстов на русском языке, содержащихся в сети Интернет.

II. ЗАДАНИЯ ДЛЯ ИНДИВИДУАЛЬНОГО ВЫПОЛНЕНИЯ

Задание 1. Защита информации от акустических угроз

Используя соотношение 1 и справочные данные (табл. Т2 – Т4), определить уровни акустического сигнала за каждым из ограждений помещения, конфигурация которого соответствует Вашему варианту (таблица к заданию 1). Оценить помещение по наихудшему показателю. Выработать рекомендации по повышению акустической защищенности помещения. Расчеты выполнить в среде табличного процессора.

Таблица к заданию 1

Вариант №	$F_{чг}$ (Гц)	Конфигурация (таблицы Т2 – Т4), состав и размеры объектов ограждений А – Г			
		Ограждение			
		А	**Б**	**В**	**Г**
0	125	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
1	250	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
2	500	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 1	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
3	1000	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7	стена 4 (2,7 х 8,5)

Вариант №	$F_{чг}$ (Гц)	Конфигурация (таблицы Т2 – Т4), состав и размеры объектов ограждений А – Г			
		Ограждение			
		А	**Б**	**В**	**Г**
4	2000	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
5	4000	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
6	250	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 1	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
7	500	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7 (1,2 х 1,7)	стена 4 (2,7 х 8,5)
8	1000	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
9	2000	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
10	4000	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 1	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
11	250	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7	стена 4 (2,7 х 8,5)

Вариант №	$F_{чг}$ (Гц)	Конфигурация (таблицы Т2 – Т4), состав и размеры объектов ограждений А – Г			
		Ограждение			
		А	**Б**	**В**	**Г**
12	500	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
13	1000	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
14	2000	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 3	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
15	4000	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7	стена 4 (2,7 х 8,5)
16	250	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
17	500	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
18	1000	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 1	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
19	2000	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7	стена 4 (2,7 х 8,5)

Вариант №	$F_{чг}$ (Гц)	Конфигурация (таблицы Т2 – Т4), состав и размеры объектов ограждений А – Г			
		Ограждение			
		А	**Б**	**В**	**Г**
20	4000	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
21	250	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)
22	500	окно 7 (1,7 х 2,5)	окно 1 (1,7 х 1,7) окно 1	стена 3 (2,7 х 8,5)	дверь 5 (1,2 х 1,7)
23	1000	дверь 6 (1,2 х 1,7)	окно 2 (1,7 х 2,5)	окно 3 (1,7 х 1,7) дверь 7	стена 4 (2,7 х 8,5)
24	2000	стена 1 (2,7 х 8,5)	стена 2 (2,7 х 8,5) дверь 2	окно 3 (1,7 х 2,5)	окно 4 (1,7 х 1,7) окно 4
25	4000	окно 5 (1,7 х 1,7) дверь 3	стена 2 (2,7 х 10)	дверь 4 (1,2 х 1,7)	окно 6 (1,7 х 2,5)

Задание 2. Обоснование состава системы защиты информации

Используя соотношения 2–7, и пример выполнения задания определить экономически обоснованный состав мероприятий защиты для включения в состав системы защиты акустической информации. Исходные данные, соответствующие Вашему варианту в таблице к заданию 2). Расчеты выполнить в среде табличного процессора.

Таблица к заданию 2

Вариант	1				2				3			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	1123	7868	2246	173	41303	1285	82606	13768	8093	8845	16186	2312
ЭЭ	22976	3110	45952	4595	43849	4998	87698	5481	44704	9937	89408	8128
ЗЕЗ	24527	1573	49054	4459	43921	10738	87842	5167	43927	4316	87854	4393
ЗС	40416	2991	80832	26944	17447	7257	34894	1939	40971	7589	81942	5121
ПЗ	15501	10188	31002	2214	35025	3362	70050	17513	50079	10420	100158	7704
ПФ	18868	8622	37736	2220	39695	7432	79390	8821	18905	8348	37810	6302
Вариант	4				5				6			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	45083	10776	16186	1012	11039	7679	16186	2698	29410	7358	16186	4047
ЭЭ	19739	7839	89408	5961	45951	10724	89408	14901	18088	9121	89408	7451
ЗЕЗ	29556	3275	87854	21964	34936	5086	87854	6758	43019	8847	87854	4881
ЗС	45622	1465	81942	4097	8690	10887	81942	4820	42211	9000	81942	27314
ПЗ	20249	10274	100158	25040	49680	8695	100158	33386	32057	7416	100158	100158
ПФ	49773	3089	37810	3781	36826	4016	37810	2701	22123	4915	37810	1990
Вариант	7				8				9			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	28066	1454	16186	5395	27678	8627	16186	2698	42596	8706	16186	8093
ЭЭ	45126	8338	89408	14901	15435	8880	89408	5961	48080	2589	89408	14901
ЗЕЗ	49144	7929	87854	12551	37024	1367	87854	8785	13145	9652	87854	4393
ЗС	43373	7799	81942	4820	14552	8543	81942	4820	45277	1705	81942	10243
ПЗ	26210	4132	100158	5892	14462	9981	100158	5008	1270	7691	100158	16693
ПФ	28002	1683	37810	4726	39129	6138	37810	18905	22998	7679	37810	4201
Вариант	10				11				12			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	5974	4032	16186	1471	10283	4733	16186	1245	38325	5723	16186	1245
ЭЭ	11956	9709	89408	8128	1916	8680	89408	29803	1976	6406	89408	11176
ЗЕЗ	15735	10252	87854	8785	43445	1361	87854	87854	46958	7349	87854	9762
ЗС	36098	10279	81942	9105	41449	9130	81942	6829	1083	9917	81942	10243
ПЗ	39288	2101	100158	14308	14036	10261	100158	5892	30868	2896	100158	11129
ПФ	8755	10300	37810	2363	43355	7929	37810	4201	36908	1284	37810	37810

Вариант	13				14				15			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	12879	1720	16186	5395	6738	5843	16186	1156	37889	8960	16186	1619
ЭЭ	13720	2245	89408	5961	14473	10198	89408	8128	50665	6180	89408	14901
ЗЕЗ	11757	9593	87854	29285	18755	6015	87854	10982	27496	3318	87854	4624
ЗС	37845	10149	81942	6303	20323	6296	81942	5121	23403	4885	81942	13657
ПЗ	33358	2559	100158	5564	31755	9134	100158	6260	40856	3119	100158	6260
ПФ	22365	7475	37810	2908	20929	8951	37810	2908	19855	3989	37810	2701
Вариант	16				17				18			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	13349	6941	16186	1079	27669	4169	16186	16186	45093	3629	16186	8093
ЭЭ	17261	2192	89408	12773	20839	6717	89408	44704	34687	3544	89408	29803
ЗЕЗ	5033	6677	87854	6758	10931	5714	87854	21964	27280	10864	87854	6758
ЗС	40065	6880	81942	81942	3728	8178	81942	6303	12253	2084	81942	13657
ПЗ	49297	2170	100158	33386	20499	4295	100158	5271	28451	5758	100158	5008
ПФ	50493	7981	37810	3151	31571	9790	37810	9453	38386	2111	37810	5401
Вариант	19				20				21			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	15087	9366	16186	1079	21799	7959	16186	1349	27671	10843	16186	1156
ЭЭ	31891	2643	89408	5961	10394	4824	89408	44704	41854	10862	89408	5259
ЗЕЗ	20367	5888	87854	7321	45192	6714	87854	29285	9824	5783	87854	5168
ЗС	10148	6301	81942	4313	35923	7965	81942	27314	46232	5455	81942	4820
ПЗ	9551	6492	100158	6677	37725	10326	100158	6677	50433	5008	100158	11129
ПФ	1977	6004	37810	3151	32207	4280	37810	2908	44431	5018	37810	2363
Вариант	22				23				24			
	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i	ω_i	s_i	z_i	b_i
РМ	17182	4289	16186	8093	15948	5722	16186	16186	47012	2494	16186	1079
ЭЭ	47448	8737	89408	89408	36656	6412	89408	4470	18861	9566	89408	9934
ЗЕЗ	26913	8767	87854	6758	9027	1069	87854	7321	42470	2456	87854	17571
ЗС	24611	2931	81942	6829	10307	6290	81942	40971	1047	5842	81942	4820
ПЗ	32611	4550	100158	5271	35663	4929	100158	10016	46480	6385	100158	5271
ПФ	27198	6735	37810	2363	18881	10484	37810	4726	18564	2025	37810	3151

Задание 3. Симметричная криптография

1. Используя соотношения 8–11, и алгоритмы симметричного шифрования зашифровать свои ***ФамилиюИмя*** (без пробела) для передачи по открытому каналу методами:

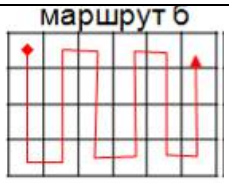
– *одноалфавитной подстановки* (***k***= Вашему номеру по журналу);

– *множественной перестановки* (ключи шифрования и маршрут – в таблице к заданию 3);

– *Вижинера* (ключ шифрования – в таблице к заданию 3).

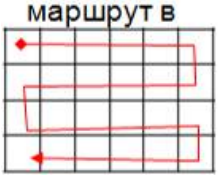
Отчет представить в виде текстового документа, созданного в табличном процессоре. Пример оформления отчета – рис. 3-1.

Таблица к заданию 3

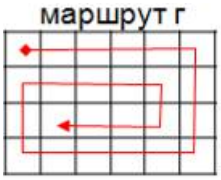
№ по журналу	**Метод множественной перестановки**			**Метод Вижинера**
	k1	*k2*	*Маршруты*	*ключ шифрования*
1	гром	склад	маршрут а 	клод
2	гриб	место		шера
3	клад	сотка		олес
4	банк	мерка		край
5	кран	песто		бора
6	вега	схрон		дрон
7	крым	прога	маршрут б 	кипа
8	блиц	резон		лента
9	кома	стейк		пемза

10	крот	козел		гладь
11	трон	страх		клоун
12	тина	горец		борец
13	мера	школа		перга
14	клод	скраб		бекас
15	шера	долма		секач
16	олес	грунт		затон
17	край	стопа		склад
18	бора	полка		место
19	дрон	ложка		сотка
20	кипа	сталь		мерка
21	кума	гюрза		песто
22	быль	лента		схрон
23	понт	пемза		прога
24	кант	гладь		резон
25	зеро	клоун		стейк
26	лань	борец		козел
27	борт	перга		страх
28	корт	бекас		кума
29	топь	секач		быль
30	рука	затон		понт

маршрут в



маршрут г



Выполнил: **курсант 201 учебной группы рядовой полиции Тихонов П.С.**
Номер по журналу: **30.**

1. Метод одноалфавитной подстановки

Исходное сообщение: "**Тихонов Петр**"
Ключ: *к=30*.

Исходное сообщение	*т*	*и*	*х*	*о*	*н*	*о*	*в*	*п*	*е*	*т*	*р*
t_i	18	8	21	14	13	14	2	15	5	18	16
e_i	12	6	19	12	11	12	0	13	3	12	14
Зашифрованное сообщение	*м*	*ж*	*у*	*м*	*л*	*м*	*а*	*н*	*г*	*м*	*о*

Зашифрованное сообщение: ***мжумлмангмо***

2. Метод множественной перестановки

Исходное сообщение: "**Тихонов Петр**"
Ключи: *k1*: "*рука*", *k2*: "*затон*", Маршрут "*г*".

Таблица А.

		р	*у*	*к*	*а*
		3	**4**	**2**	**1**
з	**2**	т	и	х	о
а	**1**	и	с	в	н
т	**5**	в	и	и	о
о	**4**	с	в	с	в
н	**3**	р	т	е	п

Таблица Б.

		а	*к*	*р*	*у*
		1	**2**	**3**	**4**
з	**2**	о	х	т	и
а	**1**	н	в	и	с
т	**5**	о	и	в	и
о	**4**	в	с	с	в
н	**3**	п	е	р	т

Таблица В.

		а	*к*	*р*	*у*
		1	**2**	**3**	**4**
а	**1**	н	в	и	с
з	**2**	о	х	т	и
н	**3**	п	е	р	т
о	**4**	в	с	с	в
т	**5**	о	и	в	и

Зашифрованное сообщение: ***нвиси твиви овпох трссе***

3. Метод Вижинера

Исходное сообщение: "**Тихонов Петр**"
Ключ: "**понт**".

Исходное сообщение	*т*	*и*	*х*	*о*	*н*	*о*	*в*	*п*	*е*	*т*	*р*
t_i	18	8	21	14	13	14	2	15	5	18	16
Ключ	*п*	*о*	*н*	*т*	*п*	*о*	*н*	*т*	*п*	*о*	*н*
k_j	15	14	13	18	15	14	13	18	15	14	13
e_i	1	22	2	0	28	28	15	1	20	0	29
Зашифрованное сообщение	*б*	*ц*	*в*	*а*	*ь*	*ь*	*п*	*б*	*ф*	*а*	*э*

Зашифрованное сообщение: "***бцваььпбфаэ***"

Рис. 3-1. Пример оформления задания в текстовом процессоре

Задание 4. Асимметричная криптография

Используя *метод распространения ключей Диффи-Хеллмана* (соотношения 12–17), *личный секретный ключ* и известные значения *g=2237 и p=3049*:

4.1. Создать и передать абоненту по переписке (АП) свой открытый ключ.

4.2. Получить от абонента по переписке его открытый ключ, зашифровать наименование своего населенного пункта, игнорируя пробелы и тире, передать зашифрованное сообщение АП.

4.3. Получить от АП зашифрованное сообщение и расшифровать его.

4.4. В текстовом процессоре оформить отчет.

Методические рекомендации

4.1. Создание открытого ключа

1. Выбрать из таблицы простых чисел (таблица к заданию 4) секретный ключ. *Этот ключ сообщать АП нельзя!*

2. Используя соотношения 12–17, метод распределения открытых ключей Диффи-Хеллмана, создать *открытый ключ*.

3. В текстовом редакторе «блокнот» создать текстовый файл, содержащий созданный *открытый ключ*. Имя файла – «*Фамилия_ключ.txt»*.

4. Распространить свой открытый ключ, *скопировав созданный файл с открытым ключом в сетевую папку общего доступа*.

4.2. Шифрование с использованием открытого ключа

5. Открыть файл с *открытым ключом* АП.

6. Используя полученный *открытый ключ***,** свой *секретный ключ* и параметры ***g=2237*** и ***p=3049***, создать *сеансовый ключ* ***K*** и зашифровать наименование своего населенного пункта (игнорируя пробелы и тире) методом Вижинера, используя в качестве ключа цифры *сеансового ключа* ***K***.

7. В текстовом редакторе «блокнот» создать текстовый файл, содержащий зашифрованное сообщение. Имя файла – *«Фамилия_шифртекст.txt»*.

8. Зашифрованное сообщение отправить АП, *скопировав созданный файл в сетевую папку общего доступа*.

4.3. Расшифровка с использованием открытого ключа

9. Получить от своего АП зашифрованное методом Виженера сообщение и расшифровать его.

10. Убедиться, что расшифровка выполнена правильно.

4.4. Оформить результаты работы, используя текстовый процессор (рис. 4-1).

Таблица к заданию 4

3067	3079	3083	3089	3109	3119
3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221
3229	3251	3253	3257	3259	3271
3299	3301	3307	3313	3319	3323
3329	3331	3343	3347	3359	3361
3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467
3469	3491	3499	3511	3517	3527
3529	3533	3539	3541	3547	3557
3559	3571	3581	3583	3593	3607
3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697
3701	3709	3719	3727	3733	3739
3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851
3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931
3943	3947	3967	3989	4001	4003

Задание 4. Асимметричная криптография

Выполнил курсант 201 учебной группы рядовой полиции Тихонов П.С.

Исходные данные:

Сообщение для шифрования	*Новокузнецк*
g	*3851*
p	*7319*
секретный ключ ***a***	*1221*
АП	*Сергеев А.В.*

4.1. Создание своего открытого ключа ***A***:

$$A = g^a \bmod p = 3851^{1221} \bmod 7319 = 79$$

4.2. Шифрование с использованием открытого ключа ***B*** АП

- Получен открытый ключ АП: ***B=963***;
- создание сеансового ключа $K = B^a \bmod p = 963^{1221} \bmod 7319 = 4486$;
- используем ключ для | 4 | 4 | 8 | 6 | шифрования:
- шифрование методом Вижинера:

Исходное сообщение	*н*	*о*	*в*	*о*	*к*	*у*	*з*	*н*	*е*	*ц*	*к*
t_i	13	14	2	14	10	19	7	13	5	22	10
Ключ k_j	4	4	8	6	4	4	8	6	4	4	8
e_i	17	18	10	20	14	23	15	19	9	26	18
Зашифрованное сообщение	***с***	***т***	***к***	***ф***	***о***	***ч***	***п***	***у***	***й***	***ъ***	***т***

4.3. Расшифровка с использованием открытого ключа

Получено сообщение АП: *епийтжняйсщр*

- Расшифровывание методом Вижинера с помощью ***K***:

Зашифрованное сообщение	*е*	*п*	*и*	*й*	*т*	*ж*	*н*	*я*	*й*	*с*	*щ*	*р*
t_i	5	15	8	9	18	6	13	31	9	17	25	16
Ключ k_j	4	4	8	6	4	4	8	6	4	4	8	6
e_i	1	11	0	3	14	2	5	25	5	13	17	10
Исходное сообщение	***б***	***л***	***а***	***г***	***о***	***в***	***е***	***щ***	***е***	***н***	***с***	***к***

Рис. 4-1. Пример оформления отчета

Задание 5. Практическая оценка стойкости ключей

Используя исходные данные (таблица к заданию 5) и соотношения 18 – 21, рассчитайте:

5.1. Криптографическую стойкость ключей;

5.2. Длину ключа «заданной» стойкости.

Все расчеты выполните в процессоре электронных таблиц.

5.3. Сделать выводы о том:

– как зависит стойкость ключа от его длины и состава символов;

– как зависит длина ключа «заданной» стойкости от состава символов ключа.

Таблица к заданию 5

Вариант	**N 1**	**N 2**	**N 3**	**k 1**	**k 2**	**k 3**	**v**
1	9	20	23	3	7	14	5511
2	8	12	24	4	8	12	15613
3	8	17	25	2	6	11	9601
4	8	16	25	4	7	14	9303
5	8	12	25	2	8	10	16779
6	10	12	23	4	8	10	9283
7	8	15	23	5	7	12	9724
8	9	18	21	2	8	11	18695
9	8	14	24	5	8	13	15857
10	9	20	22	2	8	10	19382
11	10	16	25	2	7	13	14170
12	8	12	24	3	8	11	19329
13	10	14	22	2	6	15	18127
14	8	16	25	2	8	14	11865
15	9	12	24	3	7	14	19669
16	9	19	21	4	7	11	12454
17	10	20	25	3	8	15	9310
18	10	16	24	3	6	12	19718
19	10	19	22	4	8	15	10199
20	10	18	23	2	7	12	5236
21	8	13	25	3	6	10	5779
22	8	18	25	5	6	10	18734
23	10	14	25	2	8	10	11772
24	8	19	25	5	6	13	16622
25	8	15	22	4	7	13	14303

Методические указания по выполнению задания.

5.1. Подготовьте электронную таблицу (рис. 5-1).

	A	B	C	D	E	F	G	H	I	J
1			Оценка стойкости ключа методу "полного перебора"							
2										
3			**1. Оценка стойкости ключа**							
4			№	Мощность алфавита, N	Длина ключа, k	Число возможных ключей, n	Количество ключей в сек, v	Максимальное время нахождения ключа (секунды), $t_{макс.с}$	Максимальное время нахождения ключа (годы), $t_{макс.г}$	
5			1	***N1***	***k1***		***v***			
6			2	***N1***	***k2***					
7			3	***N1***	***k3***					
8			4	***N2***	***k3***					
9			5	***N3***	***k3***					
10										
11			**2. Определение длины ключа "заданной" стойкости**							
12			Стойкость (Месяцы)	Стойкость (Секунды), $t_{ст.с}$	Число перебранных ключей, s	Требуемая длина ключа k при различных N				
13						n=				
14						***N1***	***N2***	***N3***		
15			**1**							
16			**12**							
17			**60**							
18			**120**							
19										
20			***Вариант***	***N 1***	***N 2***	***N 3***	***k1***	***k2***	***k3***	***v***
21				10	16	22	2	6	13	2860
22										
23			Выполнил курсант 201 уч. группы рядовой полиции							

Рис. 5-1. Вариант электронной таблицы

В ячейки, содержащие переменные (*N1, N2, N3,…, k1, k2, k3, v*), внесите исходные данные, соответствующие вашему варианту.

Используя соотношения 18–19, создайте в соответствующих ячейках электронной таблицы «*Оценка стойкости ключа*» (*ячейки выделены серым фоном*) формулы и рассчитайте параметры:

n – число возможных ключей;

$t_{макс.с}$ максимальное время нахождения ключа (в секундах);

$t_{макс.г}$ максимальное время нахождения ключа (в годах).

5.2. Используя соотношения 20-21, создайте в соответствующих ячейках электронной таблицы «*Определение длины ключа заданной стойкости*» (*ячейки выделены серым фоном*) формулы и рассчитайте параметры:

$t_{ст.с}$ – заданное время стойкости ключа в секундах при известной стойкости в месяцах;

s – число перебираемых программой ключей за период $t_{ст.с}$;

k –требуемую длину ключа «заданной» стойкости, состоящего из алфавитов мощностью *N1, N2, N3*.

5.3. Постройте графические зависимости:

максимального времени нахождения ключа длины *k3* от мощности алфавита *N*;

сравнения длин ключей *k* от требуемого временного периода стойкости для *N1, N2, N3*.

Сделайте выводы о том:

1. Как зависит стойкость ключа от его длины и мощности алфавита;

2. Как мощность алфавита влияет на длину ключа и по какой причине.

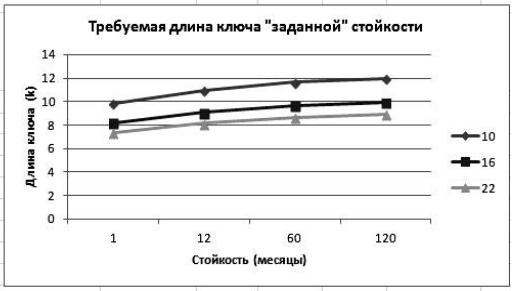
Оценка стойкости ключа методу "полного перебора"

1. Оценка стойкости ключа

№	Мощность алфавита, N	Длина ключа, k	Число возможных ключей, n	Количество ключей в сек, v	Максимальное время нахождения ключа (секунды), $t_{макс.с}$	Максимальное время нахождения ключа (годы), $t_{макс.г}$
1	*10*	*2*	100,0	*2860*	0,0	0
2	*10*	*6*	1000000,0		349,7	0
3	*10*	*13*	10000000000000,0		3496503496,5	111
4	*16*	*13*	4503599627370500,0		1574685184395,3	49933
5	*22*	*13*	282810057883083000,0		98884635623455,5	3135611

2. Определение длины ключа "заданной" стойкости

Стойкость (Месяцы)	Стойкость (Секунды), $t_{ст.с}$	Число перебранных ключей, s	Требуемая длина ключа k при различных N		
			n=		
			10	*16*	*22*
1	2592000	7413120000	10	8	7
12	31104000	88957440000	11	9	8
60	155520000	4,44787E+11	12	10	9
120	311040000	8,89574E+11	12	10	9



Выполнил курсант 201 уч. группы рядовой полиции

Вариант 1

Вариант	*N 1*	*N 2*	*N 3*	*k1*	*k2*	*k 3*	*v*
1	10	16	22	2	6	13	2860

Рис. 5-2. Пример выполненного задания

Примерный внешний вид электронной таблицы с выполненным заданием представлен на рис. 5-2.

Задание 6. Частотный криптоанализ

6.1. Используя текстовый процессор MS Word, создайте интерфейс документа (рис. 6-1) и среду разработки VBA, наберите и отладьте программу (рис. 6-2), осуществляющую подсчет частот символов в тексте.

6.2. Расшифруйте предложенный зашифрованный методом простой замены текст.

6.3. Определите частотность символов предложенных текстов и в процессоре электронных таблиц MS Excel проведите сравнительный анализ эталонной частотности символов русского языка и полученных результатов.

6.4. Сделайте выводы.

6.1. Создание программы

6.1.1. Создайте в личной папке новый документ MS Word и сохраните его с поддержкой макросов. Внешний вид документа представлен на рисунке 6-1.

Для размещения кнопок управления «Расчет статистики», «Сортировка», «Замена по таблице» перейдите во вкладку «Разработчик» (включается в «Параметры Word») и в группе «Элементы управления» выберите элемент «Кнопка. (Элемент ActiveX)» (рис. 6-2.).

6.1.2. Установив кнопки, настройте их следующие свойства (Кнопка «Свойства» на панели «Элементы управления»:

«Caption» – надписи на кнопках «расчет статистики», «сортировка», «замена по таблице» в соответствии с рис. 6-1;

«Name» – соответственно «shifr», «sort», «rashifr».

6.1.3. Дважды щелкните по кнопке «*Расчет статистики*». В открывшемся окне введите текст процедуры расчета статистики (рис. 6-3.).

6.1.4. Дважды щелкните по кнопке «*Сортировка*» и введите текст процедуры сортировки (рис. 6-4).

6.1.5. Дважды щелкните по кнопке «*Замена по таблице*» и введите текст процедуры замены символов зашифрованного текста на табличные (рис. 6-5).

Исходный (зашифрованный) текст

Буквы русского алфавита	Частоты букв русского алфавита	Буквы русского алфавита в порядке убывания частот	Символы подстановки	Расчетный порядок букв русского алфавита по убыванию частот
				о
				е
				а
				и
				т
				н
				с
				р
				в
				л
				к
				м
				д
				п
				у
				ч
				г
				ь
				я
				б
				ж
				з
				ы
				ш
				й
				х
				ю
				э
				ф
				ц
				щ
				ъ

Расшифрованный текст

Расчет статистики | Сортировка | Замена по таблице

Рис. 6-1. Интерфейс документа

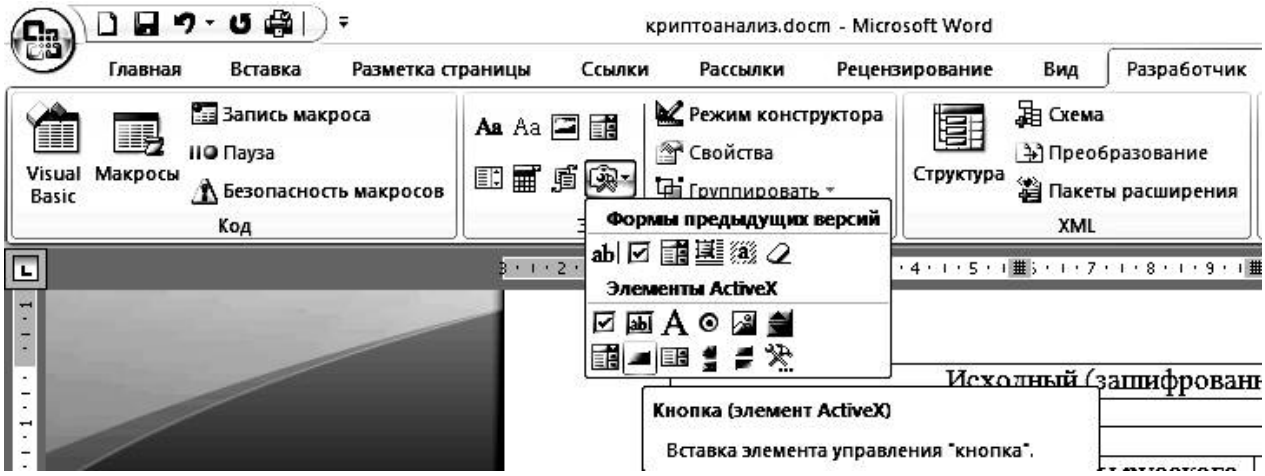


Рис. 6-2. Кнопка (Элемент ActiveX)

6.2. Криптоанализ текста

6.2.1. Откройте предложенный преподавателем файл, содержащий текст, зашифрованный методом простой замены и скопируйте его через буфер обмена во вторую строку таблицы «Исходный (зашифрованный) текст».

6.2.2. Нажмите кнопку «*Расчет статистики*». При этом программа подсчитывает количество повторений различных букв в тексте и вписывает в ячейки таблицы буквы и соответствующие им частотности.

6.2.3. Для ранжирования букв в соответствии с их частотностями нажмите кнопку «*сортировка*». При этом программа отсортирует значения частотности по убыванию и в следующий столбец впишет соответствующие им буквы текста.

Если обратить внимание на последний столбец, содержащий буквы алфавита в порядке, определяющем их эталонную частотность, то видно, что порядок букв отличается от порядка букв в тексте.

Можно предположить, что заменив буквы зашифрованного текста « Буквы русского алфавита в порядке убывания частот « на буквы эталонного столбца « Расчетный порядок букв русского алфавита по убыванию частот «, мы получим расшифрованный текст.

6.2.4. Для выполнения операции замены букв текста на буквы эталонного столбца скопируйте буквы из эталонного столбца в столбец «Символы подстановки» и нажмите кнопку «*замена по таблице*». При этом во вторую строку программа выведет расшифрованный текст.

Обратите внимание на то, что идеальный результат с первого раза достигнуть маловероятно и расшифрованный текст требует дополнительной неформализованной обработки криптоаналитиком. Иными словами, только некоторые слова будет расшифрованы верно, а остальные будут как максимум узнаваемы.

6.2.5. Найдите в тексте узнаваемые слова, что в большинстве случаев возможно в силу значительной избыточности языка и выполните корректировку порядка букв в столбце «символы подстановки».

Например, если слово «*собынай*» вы определили как «событий», то следует в столбце «символы подстановки» последовательно: поменять местами буквы «*н*» и «*т*», «*а*» и «*и*».

Shifr | Click

```
Option Explicit
Dim Nalf(32) As Single, Salf(32) As String, Zalf(32) As String
' Nalf - массив частот букв русского алфавита
' Salf - массив строчных букв русского алфавита

Private Sub Shifr_Click()
' процедура вычисления частот букв русского алфавита
Dim myRange As Range
Dim myTable1 As Table, myTable2 As Table
Dim ShifrText As String
Dim i As Integer, j As Integer, M As Integer
Dim k As Integer, s As Integer
Dim n As Long
Const K1 As Integer = 192
Const K2 As Integer = 224
Const K3 As Integer = 255
' K1-K2 диапазон кодов заглавных букв русского алфавита
' K2-K3 диапазон кодов строчных букв русского алфавита
Set myRange = ActiveDocument.Range
Set myTable1 = myRange.Tables(1)
Set myTable2 = myRange.Tables(2)
' myTable2 - кодировочная таблица
For j = 0 To 32
    Nalf(j) = 0
Next j
ShifrText = myTable1.Rows(2).Cells(1).Range.Text
M = myTable1.Rows(2).Cells(1).Range.End - myTable1.Rows(2).Cells(1).Range.Start - 1
' M - количество символов в зашифрованном тексте
For i = 1 To M
    k = Asc(Mid(ShifrText, i, 1))
    If (k >= K1) And (k <= K3) Then
        If (k >= K1) And (k < K2) Then
        k = k + 32
        End If
        Nalf(k - K2) = Nalf(k - K2) + 1
    End If
Next i
s = 0
For j = 0 To 31
          s = s + Nalf(j)
Next j
For j = 0 To 31
           Salf(j) = Chr(K2 + j)
           myTable2.Columns(1).Cells(j + 2).Range = Salf(j)
           Nalf(j) = Nalf(j) / s
           myTable2.Columns(2).Cells(j + 2).Range = Nalf(j)
Next j
End Sub
```

Рис. 6-3. Процедура расчета статистики символов в тексте

```
Private Sub Sort_Click()
' процедура сортировки массива букв русского алфавита по убыванию частоты
Dim myRange As Range
Dim myTable As Table
Dim i As Integer, j As Integer, tempB As Single, tempA As String
Set myRange = ActiveDocument.Range
Set myTable = myRange.Tables(2)
For i = 0 To 30
        For j = i + 1 To 31
            If Nalf(i) < Nalf(j) Then
                tempB = Nalf(j)
                Nalf(j) = Nalf(i)
                Nalf(i) = tempB
                tempA = Salf(j)
                Salf(j) = Salf(i)
                Salf(i) = tempA
            End If
        Next j
Next i
For j = 0 To 31
           myTable.Columns(2).Cells(j + 2).Range = Nalf(j)
           myTable.Columns(3).Cells(j + 2).Range = Salf(j)
Next j
End Sub
```

Рис. 6-4. Процедура сортировки символов по убыванию частоты

После каждой замены необходимо нажимать кнопку «*замена по таблице*» для того, чтобы программа повторила операцию замены символов с учетом новой последовательности символов. Процедура повторяется до тех пор, пока весь текст не будет выглядеть верно.

6.2.6. Представьте результат работы преподавателю!

6.3. Сравнительный анализ частотностей символов.

6.3.1. Используя несколько предложенных текстов для анализа, оцените их качественный состав (художественный, официальный, технический) и объем (большой (несколько страниц), фрагмент (1–2 абзаца)).

6.3.2. Подготовьте интерфейс программы частотного криптоанализа для выполнения задания, для чего:

из первой (верхней) таблицы удалите зашифрованный текст;

из второй (средней) таблицы удалите все данные, кроме тех, что находятся в столбце «*Расчетный порядок букв русского алфавита по убыванию частот*».

из третьей (нижней) таблицы удалите расшифрованный текст.

```
Private Sub Rashifr_Click()
' процедура замены букв русского алфавита на табличные
Dim myRange As Range
Dim myTable1 As Table, myTable2 As Table, myTable3 As Table
Dim ShifrText1 As String, ShifrText2 As String
Dim S1 As String, S2 As String
Dim Zam(32, 32) As String
Dim i As Integer, j As Integer, M As Integer
Dim k As Integer
Dim n As Long
Const K1 As Integer = 192
Const K2 As Integer = 224
Const K3 As Integer = 255
' K1-K2 диапазон кодов заглавных букв русского алфавита
' K2-K3 диапазон кодов строчных букв русского алфавита
Set myRange = ActiveDocument.Range
Set myTable1 = myRange.Tables(1)
Set myTable2 = myRange.Tables(2)
Set myTable3 = myRange.Tables(3)
' myTable - кодировочная таблица

ShifrText1 = myTable1.Rows(2).Cells(1).Range.Text
M = myTable1.Rows(2).Cells(1).Range.End - myTable1.Rows(2).Cells(1).Range.Start - 1
    For j = 0 To 31
              Zam(j, 1) = myTable2.Columns(3).Cells(j + 2).Range.Characters(1)
              Zam(j, 2) = myTable2.Columns(4).Cells(j + 2).Range.Characters(1)
    Next j
 For i = 1 To M
    S1 = Mid(ShifrText1, i, 1)
    k = Asc(S1)
    If (k >= K1) And (k <= K3) Then
        If (k >= K1) And (k < K2) Then
        k = k + 32
        End If
        For j = 0 To 31
            If Chr(k) = Zam(j, 1) Then
              S2 = Zam(j, 2)
        End If
        Next j
           Mid(ShifrText1, i, 1) = S2
      End If
Next i
    myTable3.Rows(2).Cells(1).Range.Text = Left(ShifrText1, M)

End Sub
```

Рис. 6-5. Процедура замены символов текста
на соответствующие табличные

6.3.2. Последовательно:

внесите во вторую строку первой таблицы каждый из предложенных текстов;

после внесения текста последовательно нажмите кнопки «расчет статистики», «сортировка»;

выделите и скопируйте данные из столбцов « Частоты букв русского алфавита» и «Буквы русского алфавита в порядке убывания частот» в ячейки шаблона электронной таблицы (лист «Лист расчетов»);

отсортируйте данные в «Листе расчетов» электронной таблицы по возрастанию столбца, содержащего буквы столбца « Буквы русского алфавита в порядке убывания частот», при этом символы алфавита должны выстроиться в порядке от «А» до «Я» (рис. 6-6).

	A	B
1	7,17E-02	а
2	1,37E-02	б
3	4,75E-02	в
4	1,92E-02	г
5	2,68E-02	д
6	8,46E-02	е
7	8,86E-03	ж
8	1,67E-02	з
9	8,10E-02	и
10	1,55E-02	й
11	3,20E-02	к
12	4,25E-02	л
13	2,72E-02	м
14	6,86E-02	н
15	1,18E-01	о
16	2,73E-02	п
17	4,78E-02	р
18	5,87E-02	с

	A	B	C	D	E
1					
2				НКРЯ	БТ
3		X	Q_x	F_x	F_x
4		а	38081816	0,0800	7,17E-02
5		б	7811723	0,0164	1,37E-02
6		в	21582499	0,0453	4,75E-02
7		г	9036813	0,0190	1,92E-02
8		д	14173134	0,0298	2,68E-02
9		е	40392978	0,0848	8,46E-02
10		ё	63623	0,0001	8,86E-03
11		ж	7579289	0,0159	1,67E-02
12		з	6904749	0,0145	8,10E-02
13		и	35075552	0,0737	1,55E-02
14		й	4476464	0,0094	3,20E-02
15		к	16599539	0,0349	4,25E-02
16		л	20678280	0,0434	2,72E-02
17		м	15252377	0,0320	6,86E-02
18		н	30084462	0.0632	1.18E-01

Рис. 6-6. Отсортированные символы.
Фрагмент эталонных данных и данных эксперимента

6.3.3. Вставьте отсортированные ячейки, содержащие данные частотности (на рисунке это столбец «А») в соответствующие ячейки листа «Частотность» так, чтобы они оказались под соответствующим заголовком столбца (рис. 6-6). В нашем случае это столбец «БТ» «Большой Текст».

6.3.4. Повторите п.п. 6.3.2. – 6.3.3 для каждого из предложенных текстов. Фрагмент варианта результата предложен на рис. 6-7.

6.4. Построение графиков и формулировка выводов.

6.4.1. Постройте графики зависимости частотности символов (ось x – ячейки, содержащие символы («А» – «Я»), ось Y – частотность символов).

6.4.2. Проанализируйте результаты исследования и сформулируйте выводы:

– о причине расхождения эталонной статистики и результатов эксперимента;

– о том, числовые данные частотности букв какого текста наиболее приближены к эталонным частотностям символов. Поясните причину этого.

	A	B	C	D	E	F	G
1							
2				НКРЯ	БТ	ФТ	СТ
3		X	Q_x	F_x	F_x	F_x	F_x
4		а	38081816	0,0800	0,0717	0,0549	0,0342
5		б	7811723	0,0164	0,0137	0,1016	0,1002
6		в	21582499	0,0453	0,0475	0,1126	0,0910
7		г	9036813	0,0190	0,0192	0,0522	0,0673
8		д	14173134	0,0298	0,0268	0,0440	0,0351
9		е	40392978	0,0848	0,0846	0,0742	0,0749
10		ё	63623	0,0001	0,0089	0,0055	0,0138
11		ж	7579289	0,0159	0,0167	0,0522	0,0450
12		з	6904749	0,0145	0,0810	0,0385	0,0250
13		и	35075552	0,0737	0,0155	0,0110	0,0187

Рис. 6-7. Фрагмент полученного результата

Вариант результатов для анализа представлен на рис. 6-8.

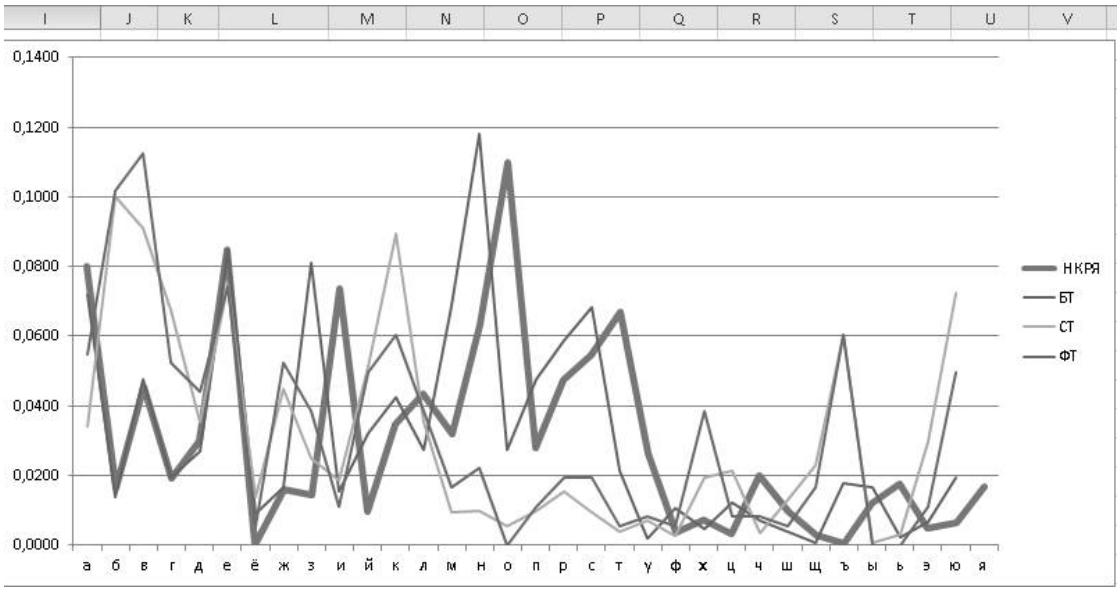


Рис. 6-8. Вариант полученных результатов

Литература

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895).

2. Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст).

3. Инженерно-техническая защита информации: Методические указания по выполнению курсовой работы для студентов. ГОУ ВПО «Удмуртский государственный университет», 2007.

4. Медянцев Д. В., Гуде С. В., Ревин С. Б., Арбузов П. В. Информационная безопасность и защита информации: учебное пособие. Ростов н/Д., 2005.

5. Шаньгин В. Ф. Информационная безопасность и защита информации: учебное пособие. М., 2014.

6. Ярочкин В. И. Информационная безопасность: учебник для вузов. М., 2013.

СОДЕРЖАНИЕ

КАРПИКА Анатолий Григорьевич,
кандидат технических наук, доцент;
АРБУЗОВ Петр Владимирович,
кандидат физико-математических наук, доцент;
ГУДЕ Сергей Васильевич,
кандидат технических наук, доцент;
ПЕТРИЩЕВА Елена Николаевна

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Практикум

Редактор *Л. А. Михайлова*
Корректоры *Л. А. Михайлова, М. М. Борзенко*
Технический редактор *Л. А. Михайлова*
Компьютерная верстка – *Е. Е. Пелехатая*

Сдано в набор 08.08.2016. Подписано к печати 26.09.2016.
Формат 60×84/16. Объем 16 п.л. Набор компьютерный.
Гарнитура Times New Roman. Печать ризография. Бумага офсетная.
Тираж 72 экз. Заказ № .
Редакционно-издательское отделение НИиРИО
ФГКОУ ВО РЮИ МВД России.
Отпечатано в ГПиОП НИиРИО
ФГКОУ ВО РЮИ МВД России.
344015, г. Ростов-на-Дону, ул. Еременко, 83.