Министерство образования Российской Федерации
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет математики и информатики

И.Н. Кузьмин

Защита информации и информационная безопасность

Учебно-методическое пособие

Благовещенск
2002

ББК 32.973 – 018.2я73
К 89

Печатается по решению редакционно-издательского совета факультета математики и информатики Амурского государственного университета

Кузьмин И.Н.

Защита информации и информационная безопасность: Учебно-методическое пособие. Благовещенск: Амурский гос. ун-т, 2002.

Пособие является лабораторным практикумом по указанной дисциплине. Содержит методики оценочного расчета защищенности помещений от утечки информации по акустическому и электромагнитному каналам, знакомит с традиционными симметричными методами шифрования, а также набор заданий и последовательность их выполнения. Предназначено для студентов специальности "Информационные системы в технике и технологии".

Рецензент: **Штыкин М.Д., ведущий специалист группы режима и информационной безопасности управления федеральной службы налоговой полиции РФ по Амурской области, канд. техн. наук.**

ВВЕДЕНИЕ

В современном обществе информация стала одним из основных ресурсов, определяющим экономический, политический и военный потенциал государства. В связи с этим информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов общества, государства, а также отдельно взятой личности.

Информация, как объект права собственности, имеет следующие особенности:

1) не являясь материальным объектом, она неразрывно связана с материальным носителем (мозг человека, книга, дискета и т.д.);

2) легко перемещается от одного субъекта права собственности к другому, не изменяясь при копировании;

3) как правило, хранится и обрабатывается в сфере доступности большого числа субъектов, не являющихся субъектами права собственности на эту информацию.

Особое внимание уделяется автоматизированным системам обработки информации (АСОИ), комплексное обеспечение информационной безопасности которых охватывает совокупность криптографических, программно-аппаратных, технических, правовых и организационных методов и средств в автоматизированных системах при обработке, хранении и передаче информации с использованием современных информационных технологий.

Предлагаемый лабораторный практикум включает методики оценочного расчета защищенности помещений от утечки информации по акустическому и электромагнитному каналам, а также знакомит с традиционными симметричными методами шифрования.

ЛАБОРАТОРНАЯ РАБОТА 1

ОЦЕНОЧНЫЙ РАСЧЕТ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ ОТ УТЕЧКИ РЕЧЕВЫХ СООБЩЕНИЙ ПО АКУСТИЧЕСКОМУ КАНАЛУ

Циркуляция в помещении акустических колебаний, вызванных как значимыми для информационного обмена потоками речевых сообщений между их прямыми носителями (людьми), так и незначительными, но информативными потоками акустических колебаний (клавиатура ПЭВМ, пишущая машинка или телетайп, принтер и т.п.), при недостаточной звукоизоляции ограждающих конструкций, а также при наличии косвенных носителей информации (акустоэлектрических, акустовибрационных и акустооптических преобразователей) в этом помещении может привести к распространению сообщений по **обобщенному** акустическому каналу, средой передачи в котором могут являться:

в акустическом канале - окружающее воздушное пространство;

в акустоэлектрическом канале - провода, отходящие от различных электромеханических преобразователей, находящихся в помещении, за пределы этого помещения;

в акустовибрационном канале - стены и перегородки, перекрытия, оконные рамы, дверные коробки, трубопроводы, короба вентиляции;

- в акустооптическом канале - оптоволоконный кабель.

Акустический канал возникает из-за образования звуковых волн сжатия, создаваемых голосовым аппаратом человека, и распространения их в воздушной среде, а также проникновения через несущие стены зданий, окна, двери, вентиляционные воздуховоды сквозь поры, щели и т.п.

При произнесении звуков речи через речевой тракт, представляющий собой сложный акустический фильтр с рядом резонаторов, создаваемых полостями рта, носа и носоглотки, проходит либо тональный импульсный сигнал (звонкие звуки), либо шумовой (глухие звуки), либо тот и другой вместе. Вследствие этого равномерный тональный или шумовой спектр превращается в спектр с рядом максимумов, называемых формантами, и минимумов, называемых антиформантами. Так как наиболее информативными являются глухие согласные, то при действии шумов разборчивость речи снижается, в первую очередь из-за маскировки глухих звуков. Ухо человека обладает свойствами дискретного восприятия по частотному и динамическому диапазонам.

Слуховое ощущение пропорционально логарифму раздражающей силы:

$$\mathbf{E}_{\text{дБ}}=10\boldsymbol{lg}(\mathbf{I}/\mathbf{I}_{\text{п.с}}), \qquad (1)$$

где $\mathbf{I}_{\text{п.с}}$ - раздражающая сила на пороге слышимости.

Величину **E** называют уровнем ощущения, причем $\mathbf{E} = \mathbf{L}_1 - \mathbf{L}_{\text{п.с}}$, где $\mathbf{L}_1 = 10\boldsymbol{lg}\mathbf{I} + 120$ - уровень интенсивности звука **I**, Вт/м^2. Уровень ощущения, представляет собой уровень над порогом слышимости, т.е. относительный уровень.

Так как уровень ощущения неточно характеризует субъективное ощущение, в акустике применяется понятие "уровень громкости" звука (или шума),

под которым понимается уровень в децибелах равногромкого с ним чистого тона 1000 Гц.

В соответствии с кривыми равной громкости, при уровне 30-40 фон (уровень громкости в дБ на частоте 1000 Гц) в диапазоне частот 250...500 Гц происходит уменьшение громкости примерно на 6 дБ, поэтому при приеме элементов речи техническими средствами, это снижение можно компенсировать частотной коррекцией, что невозможно осуществить при приеме речи специально подготовленными людьми - артикулянтами.

Восприятие речи в значительной степени зависит от уровня акустических шумов, которые могут распространяться и как акустические сигналы и как помехи. Последние подразделяются на три вида: белый шум (имеет одинаковую спектральную плотность во всем частотном диапазоне), розовый (имеет тенденцию спада на 3 дБ/окт. в сторону высоких частот) и речевой шум - шум, создаваемый одновременным разговором нескольких человек.

Обычно при расчетах рассматриваются стационарные шумы, однако в течение длительного периода времени (день - ночь, рабочие дни - выходные) шумы могут носить нестационарный характер, т.е. изменяться во времени. Маскирующие свойства шумов проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона. Наибольший маскирующий эффект имеют широкополосные помехи с "гладким" спектром, но удовлетворительная разборчивость речи может быть достигнута даже в том случае, если уровень речи будет на несколько децибел ниже уровня шума.

Узкополосные помехи даже высокого уровня не могут обеспечить требуемой степени зашумления речи, так как они, как правило, имеют периодический характер, что позволяет частично их компенсировать с помощью различных фильтров.

Для определения максимально допустимого уровня шума в помещениях, в соответствии с санитарными нормами, применяются предельные спектры (ПС). Число при ПС означает уровень шума в октавной полосе со среднегеометрической частотой 1000 Гц. Так как санитарные нормы ограничивают максимальное значение уровня шума для различных типов помещений, то предельные спектры можно использовать для расчета разборчивости речи в конкретных условиях.

Уровни интенсивности речи в октавных полосах и некоторые значения предельных спектров шумов приводятся в табл. 1. Значения уровней шумов, измеренные на частоте 1000 Гц в различных местах, приводятся в табл. 2.

Разборчивостью называют относительное или процентное количество принятых специально тренированными слушателями (артикулянтами) элементов речи из общего количества переданных по тракту. Так как в качестве элементов речи применяют звуки, слоги, слова и фразы, то имеет место **звуковая, слоговая, словесная и фразовая** разборчивость. Все они при испытании одной и той же системы будут выражаться разными численными величинами, так как процент правильных оценок для предвиденного сообщения всегда выше, чем для непредвиденного, степень же предвидения при прослушивании фразы выше, чем при прослушивании отдельных слов или слогов.

Однако все виды разборчивости связаны друг с другом однозначными функциональными зависимостями, представляемыми обычно в виде кривых или таблиц.

Разборчивость представляет собой статистическую характеристику речи, принимаемой на фоне шумов, и описывается вероятностными характеристиками. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону.

Объективные измерительные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. По формантной разборчивости **А**ф определяют слоговую **S**, словесную **W**, фразовую разборчивость и понятность речи. Зависимость между формантной **А**ф (суммарной вероятностью приема формант), слоговой S и словесной **W** разборчивостью речи приведена в табл.3.

Форманты звуков речи заполняют весь частотный диапазон 150...7000 Гц. Этот частотный диапазон делят на 20 полос равной разборчивости. Вероятность появления формант в каждой полосе равной разборчивости равна 0,05. При прослушивании речи в условиях шумов разборчивость получается меньшей, чем в их отсутствие. Коэффициент ***w***, определяющий это уменьшение, называют ***коэффициентом восприятия, или коэффициентом разборчивости***, т.е. в каждой полосе равной разборчивости вероятность приема формант $\Delta\mathbf{A} = 0{,}05\,\boldsymbol{w}$. Коэффициент разборчивости ***w*** определяется уровнем ощущения формант $\mathbf{E}_ф = \mathbf{B}_р. - \mathbf{B}_ш.$, где $\mathbf{B}_р.$ - средний спектральный уровень речи; $\mathbf{B}_ш.$ - спектральный уровень шумов.

Для практики применение полос равной разборчивости неудобно, так как получающиеся частотные полосы нестандартны. Для каждой полосы равной разборчивости коэффициент разборчивости ***w*** в общем случае будет разный, поэтому в акустических измерениях используются октавные или третьоктавные частотные полосы. Значения коэффициентов разборчивости речи ***w***, соответствующие определенным уровням ощущения формант **Е**ф, приведены в табл. 4.

Градации понятности речи и соответствующие им значения слоговой (**S**) и словесной (**W**) разборчивости, измеренные артикулянтами и дополненные значениями формантной **А**ф разборчивости (суммарной вероятностью приема формант), взятой из табл. 3, приведены в табл. 5. Учитывая, что восприятие человеком формант обладает свойством аддитивности, т.е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи, можно рассчитать вклады октавных полос для формантной разборчивости. На основании данных о вкладах октавного анализа для русской речи можно определить выражение для формантной разборчивости **А**ф.русск. для русской речи:

$$\mathbf{A}\text{ ф.русск.} = 0{,}05*(1{,}34\boldsymbol{w}\mathbf{1} + 2{,}5\,\boldsymbol{w}\mathbf{2} + 4{,}24\boldsymbol{w}\mathbf{3} + 5{,}88\,\boldsymbol{w}\mathbf{4} + 5\boldsymbol{w}\mathbf{5} + 1{,}04\boldsymbol{w}\mathbf{6}), \qquad (2)$$

где ***w***i - коэффициенты разборчивости речи на средних октавных частотах (250, 500, 1000, 2000, 4000, 6000).

От качественного приема каждой частотной полосы зависит суммарная разборчивость. Минимальная формантная разборчивость Аф, при которой еще возможно понимание смысла речевого сообщения (суммарная вероятность приема формант), равна 15%, что соответствует 25% слоговой и 75% словесной разборчивости (см. табл. 5).

Учитывая сказанное, для минимальной формантной разборчивости можно записать: **А**ф.русск.мин. = 0,05 (1,34***w***1 + 2,5***w***2 + 4,24***w***3 + 5,88***w***4 + 5w5 + 1,04***w***6) = 0,15.

Рассчитаем ***w***i на частоте 1000 Гц, так как на этой частоте обычно приводятся значения коэффициента звукоизоляции ограждающих конструкций.

Суммарной вероятности приема формант **А**ф.русск.мин. = 0,15 соответствует 100% всего частотного диапазона, а участку, который вносит свой вклад в разборчивость в размере 21,2% (на частоте 1000 Гц), соответствует W_{1000} = W3 = 0,05x4,24x0,15 /100 = 3,15/100 = 0,0315. Согласно табл. 4 для W = 0,03 находим Еф = Вр. – Вш. = - 9 дБ. Так как ухо человека обладает свойствами дискретного восприятия по частотному и динамическому диапазонам, то для того, чтобы речь была вообще неразборчива, возьмем предыдущее значение W = 0,02, для которого Еф. = Вр. – Вш. = -10 дБ на частоте 1000 Гц.

Проведя аналогичные действия для остальных пяти октавных полос, а также повторив их для удовлетворительной, хорошей и отличной суммарных вероятностей приема формант для всех шести октавных полос, сведем полученные результаты в табл. 6.

На разборчивость речевых сообщений оказывает влияние эффект реверберации, характеризуемый временем уменьшения уровня звукового давления в помещении на 60 дБ после выключения источника. Этот эффект проявляется в наложении речевых отрезков друг на друга за счет переотражения сигнала от поверхностей конструкций, поэтому если помещение имеет звукопоглощающие поверхности, то время реверберации незначительно, однако в больших гулких помещениях реверберация может существенно исказить речь. Время реверберации менее 0,85 сек. незаметно для слуха. Для большинства кабинетов и помещений с мебелью их объемы и акустическая отделка позволяют не учитывать временные искажения, так как время реверберации в них не превышает 0,6 сек.

При падении звуковых волн с интенсивностью $\mathbf{I}_{пад.}$ на какую-либо перегородку больших размеров в сравнении с длиной волны интенсивность звука с другой стороны перегородки $\mathbf{I}_{пр}$ в условиях отсутствия отражения звука в пространстве за перегородкой будет определяться только звукопроводностью перегородки. Коэффициент звукопроводности $\alpha_{пр} = \mathbf{I}_{пр} / \mathbf{I}_{пад} = \rho^2_{пр} / \rho^2_{пад}$ или в логарифмических единицах (звукоизоляция перегородки) $\mathbf{Q}_{пер} = \mathbf{L}_{пад} - \mathbf{L}_{пр} = 20\boldsymbol{lg}(\rho_{пад}/\rho_{пр})$, где $\mathbf{L}_{пад}$ и $\mathbf{L}_{пр}$ - уровни звукового давления с внутренней и внешней сторон перегородки, $\rho_{пад}$ и $\rho_{пр}$ – поверхностная плотность материала перегородки с внутренней и внешней сторон. Коэффициент звукоизоляции стен $\mathbf{Q}_{пер}$ с различной поверхностной плотностью ρ в децибелах (с учетом только мембранного переноса) для частот 500...1000 Гц может быть определен по формулам:

$$\mathbf{Q}_{пер}, \text{ дБ} = 12{,}5\boldsymbol{lg}\rho + 14 \quad (3)$$

для стен с $\rho < 200$ кг/м^2;

$$\mathbf{Q}_{пер}, \text{ дБ} = 14{,}5\boldsymbol{lg}\rho + 15 \quad (4)$$

для стен с $\rho > 200$ кг/м^2;

$$\mathbf{Q}_{пер}, \text{ дБ} = 14\boldsymbol{lg}\,(\rho_1\rho_1) + 20\,\boldsymbol{lg}\delta - 13 \quad (5)$$

для двойных жестких перегородок с воздушной прослойкой между ними с поверхностной плотностью $\rho = 30...100$ кг/м^2; где $\rho 1$ и $\rho 1$ - поверхностная плотность первой и второй перегородки, δ - толщина воздушного слоя между ними.

Значения $\mathbf{Q}_{пер}$ в формулах 3 - 5 приводятся для частот 500...1000 Гц; для частот 50...250 Гц звукоизоляция будет на 6 дБ меньше, а для частот, равных 4000 Гц и более на 6 дБ больше. Некоторые значения $\mathbf{Q}_{пер}$ приводятся в табл. 7.

Изолирующие свойства перегородки с дверью или окном можно рассчитать по следующей формуле:

$$\mathbf{Q}_{пер} = \mathbf{Q}1 - 10\boldsymbol{lg}[1 + (\mathbf{S}_o/(\mathbf{S}_1 + \mathbf{S}_o))*(10^{0{,}1(\mathbf{Q}1-\mathbf{Q}o)} - 1)], \quad (6)$$

где $\mathbf{Q}_{пер}$ - величина звукоизоляции неоднородной перегородки;

$\mathbf{Q}_1$ - величина звукоизоляции глухой части перегородки (без учета окна или двери);

$\mathbf{Q}_o$ - величина звукоизоляции двери или окна;

$\mathbf{S}_1$ - площадь глухой части стены;

$\mathbf{S}_o$ - площадь двери или окна.

При прохождении через различные строительные конструкции и материалы сигналы ослабевают в зависимости от толщины и поверхностной плотности материала. Уровень акустического сигнала за ограждающей конструкцией (звукоизолирующей перегородкой) $\mathbf{L}_2$ можно определить из следующего выражения:

$$\mathbf{L}_2 = \mathbf{L}_1 + 10\boldsymbol{lg}(\mathbf{S}/\mathbf{A}) - \mathbf{Q}_{пер}, \quad (7)$$

где: $\mathbf{L}_2$ - уровень речевого сигнала за звукоизолирующей перегородкой;

$\mathbf{L}_1$- уровень речевого сигнала в контролируемом помещении;

S - площадь звукоизолирующей перегородки, разделяющей помещения;

A - эквивалентная площадь звукопоглощения, м^2;

$\mathbf{Q}_{пер}$ - коэффициент звукоизоляции различных конструкций для частот 500...1000 Гц.

Для ориентировочной оценки звукоизоляции меблированных помещений величина $10\boldsymbol{lg}(\mathbf{S}/\mathbf{A})$, характеризующая реверберационные свойства помещения, может быть принята равной нулю. С учетом этого, а также предполагая, что в качестве приемника речевых сообщений используется техническое средство,

которое может иметь на низких частотах подъем усиления на 6 дБ, выражение для определения $\mathbf{L}_2$ примет вид:

$$\mathbf{L}_2 = \mathbf{L}_1 + 6 - \mathbf{Q}_{пер}. \qquad (8)$$

Это выражение в дальнейшем будем применять для расчетов уровня речевого сигнала за звукоизолирующей перегородкой.

Таблица 1.

Уровни интенсивности речи в октавных полосах
и предельные спектры шумов

Номер октавы	Средняя частота, *f*р	Уровни речи и предельные спектры шумов, дБ								
		речь	ПС-20	ПС-25	ПС-30	ПС-35	ПС-40	ПС-45	ПС-50	ПС-55
1	250	67,9	31	35	40	45	49	54	59	63
2	500	66,9	24	29	34	39	44	49	54	58
3	1000	61,5	20	25	30	35	40	45	50	55
4	2000	57,0	17	22	27	32	37	42	47	52
5	4000	53,0	14	20	25	30	35	40	44	50
6	6000	48,5	13	18	23	28	33	38	43	49
Суммарные уровни, дБ		71	32,3	36,6	41,6	47	51	60	61	65

ПС-25 - кабинет при одном работающем;
ПС-30 - библиотека;
ПС-35 - комната для сна и отдыха;
ПС-45 - кабинет для умственной работы без собственных шумов;
ПС-50 - кабинет для речевой и телефонной связи;
ПС-55 - кабинет для конторского труда и цеховой администрации

Таблица 2.

Уровни шумов, измеренные на частоте 1000 Гц

Источник шума и место его измерения	Уровень шума, дБ (f = 1000Гц)
акустические шумы вне помещений:	
тихий сад	20
тихая улица (без движения транспорта)	30 - 35
обычный средний шум на улице	55 - 60
шумная улица без трамвайного движения	60 - 75
трамвай на расстоянии 10 -20 м	80 - 85
троллейбус на расстоянии 5 м	77

Продолжение таблицы 2.

грузовой автомобиль в городе на расстоянии 10-20 м	60 - 75
легковой автомобиль в городе на расстоянии 10-20 м	50 - 65
электропоезд на эстакаде на расстоянии 6 м	90
акустические шумы в помещениях:	
обычное учреждение, жилое помещение	40
шепот на расстоянии 1 м	20-25
спокойный разговор 3 человек в комнате средних размеров	45-50
громкая музыка по радио	80
Разговор на расстоянии 1 м: обычный	55 - 60
громкий	65 - 70
громкий разговор по телефону	55
шумное собрание	65 - 70
коридоры	35 - 40
бухгалтерия без посетителей	30 - 35
комната шумная	40 - 50
комната тихая	25 - 30
кабинет при одном работающем	20 - 25

Таблица 3.

Зависимость между формантной (Аф), слоговой (S)
и словесной (W) разборчивостью

Аф, отн. ед.	**S**, %	**W**, %	**А**ф, отн. ед.	**S**, %	**W**, %
0,05	5,0	30,0	0,55	84,0	98,5
0,10	15,0	63,0	0,60	87,0	98,8
0,15	26,0	76,0	0,65	90,0	99,0
0,20	36,0	85,0	0,70	92,5	99,2
0,25	46,0	90,0	0,75	95,2	99,4
0,30	54,0	93,0	0,80	96,5	99,6
0,35	62,5	94,5	0,85	98,0	99,7
0,40	69,0	96,0	0,90	99,0	99,8
0,45	75,0	97,0	0,95	99,5	99,9
0,50	80,0	98,0	1,00	100,0	100,0

Таблица 4.

Значения коэффициентов разборчивости ***w***,
соответствующие определенным уровням ощущения формант **Е**ф

Еф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.
Еф < 15 ***w*** = 0		-8	0,040	9	0,50	26	0,960
		-7	0,050	12	0,60	27	0,970
		-6	0,060	15	0,70	28	0,980
		-5	0,075	18	0,80	29	0,985
-15	0,002	-4	0,095	19	0,83	30	0,990
-14	0,005	-3	0,110	20	0,86	33	0,995
-13	0,007	-2	0,140	21	0,88	36	1,000
-12	0,010	-1	0,17	22	0,900	**Е**ф > 36 ***w*** = 1	
-11	0,015	0	0,20	23	0,915		
-10	0,020	3	0,30	24	0,930		
-9	0,030	6	0,40	25	0,945		

Таблица 5.

Градации понятности речи и соответствующие им значения формантной (**А**ф), слоговой (**S**) и словесной (**W**) разборчивости

Понятность	Разбочивость, %		
	форматная (**А**ф)	слоговая (**S**)	словестная (**W**)
Предельно допустимая	15-22	25-40	75-87
Удовлетворительная	22-31	40-56	87-93
Хорошая	31-50	56-80	93-98
Отличная	50 и выше	80 и выше	98 и выше

Таблица 6.

Разборчивость речи и уровни ощущения формант в октавных полосах

Аф.русск. = 0,05*(1,34***w***1 +2,5***w***2 +4,24***w***3 + 5,88 ***w***4 +5***w***5 +1,04***w***6)							
		Средняя частота октавных полос, Гц					
		250	500	1000	2000	4000	6000
		Вклад частот в разборчивость формант, %					
		6,7	12,5	21,2	29,4	25	5,2
Понятность речи	Суммарная разборчивость формант Аф.русск., %	Разборчивость речи в конкретной октавной полосе частот, ***w***i					

Продолжение таблицы 6

		Уровень ощущения формант Еф. = Вр. – Вш. в конкретной октавной полосе, дБ					
Смысл непонятен	< 15	**0 <-12**	**0,015 -11**	**0,02 -10**	**0,03 -9**	**0,03 -9**	**0 <-12**
Предельно допустимая	15 – 22	**0,01 -12**	**0,02 -10**	**0,03 -9**	**0,04 -8**	**0,04 -8**	**0,007 <-12**
Удовлетворительная	22 – 31	**0,015 -11**	**0,03 -9**	**0,04 -8**	**0,06 -6**	**0,05 -7**	**0,011 -12**
Хорошая	31 – 50	**0,02 -10**	**0,04 -8**	**0,06 -6**	**0,09 -4**	**0,077 -5**	**0,016 -11**
Отличная	>= 50	**0,03 -9**	**0,06 -6**	**0,11 -3**	**0,147 -2**	**0,125 -2**	**0,026 -10**

Таблица 7.

Значения коэффициентов звукоизоляции материалов и ограждающих конструкций

Номер п/п	Материал или конструкция	Толщина, мм	Поверхностная плотность, кг/м^2	**Q**$_{пер}$, дБ
1.Стены и перегородки				
Стена из кирпичной кладки без штукатурки (из красного кирпича):				
1.1.	в 0,5 кирпича	120,0	204,0	48,0
1.2.	в 1 кирпич	250,0	425,0	53,0
1.3.	в 1,5 кирпича	380,0	646,0	56,0
1.4.	в 2 кирпича	520,0	884,0	58,0
1.5.	в 2,5 кирпича	640,0	1088,0	59,0
1.6.	Виброкирпичная панель, не оштукатуренная	140,0	240,0	49,5
1.7.	То же	160,0	280,0	50,4
1.8.	Стена из пустотелого кирпича	380,0	-	51,0
1.9.	То же	510,0	-	54,0
1.10.	Стена из железобетона	100,0	240,0	49,0
1.11.	То же	140,0	340,0	51,0
1.12.	То же	160,0	400,0	52,0
1.13.	То же	180,0	430,0	53,0
1.14.	То же	200,0	500,0	54,0
1.15.	То же	300,0	750,0	56,6
1.16.	То же	800,0	2000,0	62,8
1.17.	Гипсобетонная (гипсолитовая) плита	80,0	115,0	39,7
1.18.	То же	95,0	135,0	40,6
1.19.	Газобетонная плита	240,0	270,0	50,25

Продолжение таблицы 7

1.20.	Керамзитобетонная плита	80,0	100,0	39,0
1.21.	То же	100,0	150,0	41,2
1.22.	То же	120,0	195,0	42,6
1.23.	Шлакоблоки, оштукатуренные с двух сторон	220,0	360,0	52,0
	Шлакогипсовые стенные плиты:			
1.24.	2х5 см	130,0	120,0	40,0
1.25.	2х6 см	170,0	150,0	42,0
	Пемзобетонные стенные плиты:			
1.26.	2х6 см	150,0	135,0	40,0
1.27.	2х8,5 см	200,0	185,0	43,0
1.28.	Стены из пемзобетона	140,0	150,0	42,0
1.29.	То же	230,0	250,0	50,0
1.30.	Стена из шлакобетона	140,0	150,0	42,0
1.31.	То же	250,0	400,0	52,7
1.32.	То же из пустотелых пемзобетонных блоков	190,0	190,0	43,0
1.33.	То же	290,0	270,0	50,0
1.34.	Древесно-стружечная плита	20,0	12,0	27,4
1.35.	Перегородка одинарная из досок толщиной 2 см, оштукатуренная с обеих сторон и оклеенная обоями	60,0	70,0	37,0
1.36.	Перегородка одинарная из досок толщиной 2,5 см, оштукатуренная с обеих сторон по войлоку	70,0	76,0	39,0
1.37.	Перегородка двойная из брусков 10 см, обшитых с двух сторон досками толщиной 2,5 см и отштукатуренная с двух сторон	180,0	95,0	45,0
1.38.	То же с оштукатуркой по войлоку	190,0	96,0	47,0
1.39.	Перегородка двойная из фанерных листов толщиной 3 мм с промежутком 2,5 см, заполненным шлаковатой	30,0	8,0	26,0
1.40.	То же с промежутком 5 см	55,0	12,0	29,0
1.41.	То же с промежутком 6,5 см	70,0	14,0	34,0

Продолжение таблицы 7

1.42.	Гипсовые пустотелые камни толщиной 1 см с двумя стенками толщиной по 1,5 см и промежутком 8 см с засыпкой шлаком	110,0	117,0	41,0
2. Окна				
2.1.	Одинарное остекление без уплотнительных прокладок	3,0	-	22,0
2.2.	Тоже	4,0	-	26,0
2.3.	Тоже	6,0	-	26,0
2.4.	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала (нар. - внутр.)	3,0/3,0	-	32,0
2.5.	То же со звукопоглощающим материалом	3,0/3,0	-	42,0
2.6.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	3,0/3,0	-	38,0
2.7.	То же со звукопоглощающим материалом	3,0/3,0	-	43,0
2.8.	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала	4,0/4,0	-	38,0
2.9.	То же со звукопоглощающим материалом	4,0/4,0	-	41,0
2.10.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	4,0/4,0	-	41,0
2.11.	Двойное остекление, расстояние между стеклами 57 см, без звукопоглощающего материала	6,0/3,0	-	35,0
2.12.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	6,0/3,0	-	37,0
2.13.	Двойное остекление, расстояние между стеклами 38 мм, без звукопоглощающего материала	6,0/6,0	-	40,0
2.14.	То же, 190 мм	6,0/6,0	-	45,0
2.15.	То же, 400 мм	6,0/6,0	-	48,0

Продолжение таблицы 7

3. Двери				
	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см:			
3.1.	без уплотняющих прокладок	-	-	18,0
3.2.	с уплотняющими прокладками	-	-	23,0
3.3.	То же, с обвязкой толщиной 2,5 см и филенкой из 3 мм фанеры без уплотняющих прокладок	-	-	10,0
3.4.	То же, оклеенная фанерой размером 90х200 см,без уплотняющих прокладок	-	-	22,0
	Глухая щитовая дверь толщиной 40 мм, облицованная с двух сторон фанерой толщиной 4 мм:			
3.5.	без уплотняющих прокладок	-	-	24,0
3.6.	с уплотняющими прокладками	-	-	32,0
	Щитовая дверь из твердых древесно-волокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненная стекловатой:			
3.7.	без уплотняющих прокладок	-	-	30,0
3.8.	с уплотняющими прокладками	-	-	33,0
	То же, заполненная минеральным войлоком:			
3.9.	без уплотняющих прокладок	-	-	28,0
3.10.	с уплотняющими прокладками	-	-	32,0
3.11.	Тяжелая дубовая дверь размером 90х210 см, плотно пригнанная	-	-	25,0
3.12.	Металлическая дверь (герметичная)	-	-	30,0

Пример расчетов по определению возможности утечки речевых сообщений

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета (рис. 1).

Исходные данные расчетов:

а) смежная комната: предельный спектр шумов - **ПС**-35 (табл. 1); перегородка одинарная из досок (п. 136 табл. 7);

б) внутренний двор здания: предельный спектр шумов - **ПС**-45 (табл. 1); стена из кирпичной кладки (п. 1.5 табл. 7); окно (п. 2.6 табл. 7) занимает 40% стены;

в) коридор: предельный спектр шумов - **ПС**-40 (табл. 1); стена из кирпичной кладки (п.1.1 табл. 7); дверь (п. 3.1 табл. 7) занимает 20% стены;

г) уровень интенсивности речи в октавных полосах берется из табл. 1.

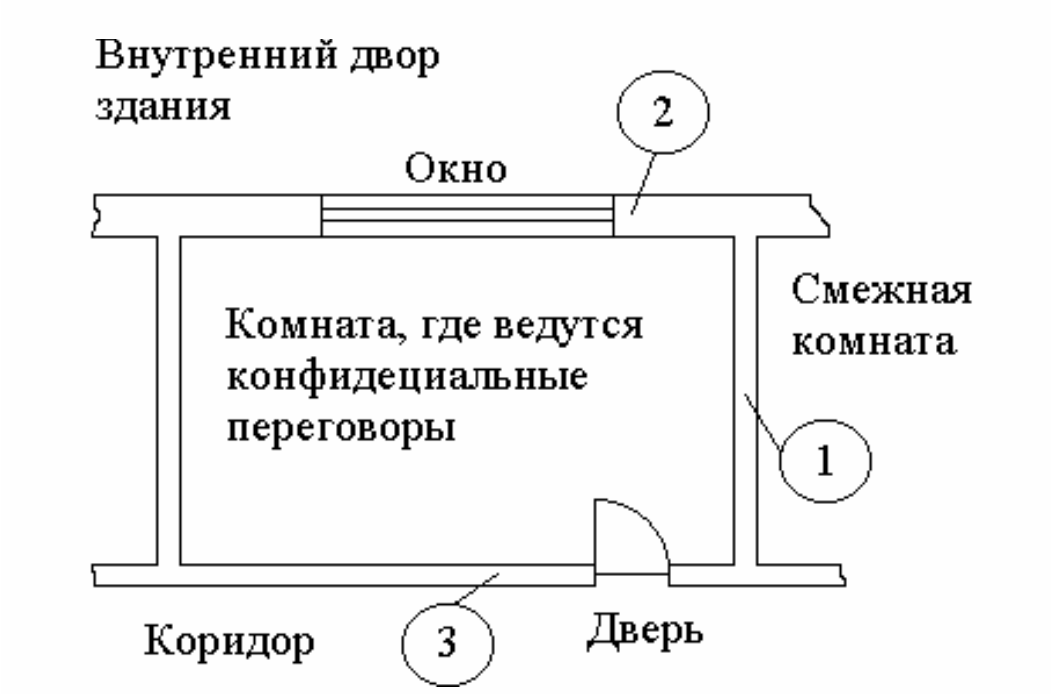

Рис. 1. Схема исследуемого кабинета

Порядок расчета.

1. Смежная комната.

По формуле (8) определяем: $\mathbf{L}_2 = \mathbf{L}_1 + 6 - \mathbf{Q}_{пер}$,

где $\mathbf{L}_2$ - уровень речевого сигнала за звукоизолирующей перегородкой;

$\mathbf{L}_1$ - уровень речевого сигнала в контролируемом помещении.

Значение $\mathbf{L}_1$ в октавных полосах будем определять, исходя из суммарного уровня речи 71 дБ (табл. 1). Значение $\mathbf{Q}_{пер}$ берем в табл. 1.

Номер октавы	Ср. частота, $f_р$	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ $\mathbf{Q}_{пер}$	**L**1 + 6 - $\mathbf{Q}_{пер}$, дБ	**L**2 = **L**р, дБ
1.	250	67,9	39-6	67,9 + 6 - (39 - 6)	40,9
2.	500	66,9	39	66,9 + 6 - 39	33,9
3.	1000	61,5	39	61,5 + 6 -39	28,5
4.	2000	57,0	39	57,0 + 6 - 39	24,0
5.	4000	53,0	39+6	53,0 + 6 - (39 + 6)	14,0
6.	6000	48,5	39+6	48,5 + 6 - (39 + 6)	9,5

Уровень ощущения формант $\mathbf{E}_ф$ определяется из выражения:

Eф= **L**р – **L**ш.

Номер октавы	Ср. частота, *f*р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-35, **L**ш, дБ	**E**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости ***w***i по табл. 3
1.	250	40,9	45	-4,1	0,095
2.	500	33,9	39	-5,1	0,075
3.	1000	28,5	35	-6,5	0,06
4.	2000	24,0	32	-8	0,04
5.	4000	14,0	30	-16	0
6.	6000	9,5	28	-18,5	0

По формуле (2) находим суммарную разборчивость формант:

А ф.русск.= 0,05*(1,34***w***1 + 2,5 ***w***2 + 4,24***w***3 +5,88 ***w***4+5***w***5+1,04***w***6) =
= 0,05*(1,34x0,095 + 2,5x0,075 + 4,24x0,06 + 5,88x0,004) =
= 0,04 или (4%)

Выводы: расчетная суммарная разборчивость формант **А**ф.русск. <15%, в соответствии с табл. 6 смысл разговора в смежной комнате будет непонятен.

2. Внешняя стена

По формуле (6) определяем величину звукоизоляции неоднородной перегородки, которыми являются внешняя стена и окно:

Qпер = **Q**1-10***lg***[1+(**S**o/(**S**1 + **S**o))*($10^{0,1(\mathbf{Q}1-\mathbf{Q}o)}$-1)],

где **Q**1 = 59 дБ;
Qo = 38 дБ;
(**S**o/(**S**1 + **S**o)) = 0,4.

Qпер = 59-10***lg***[1+0,4*($10^{0,1(59-38)}$-1)] = 42 Дб.

Уменьшение звукоизоляции стены с окном составило 17 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

Номер октавы	Ср. частота, *f*р	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	42-6	67,9 + 6 - (42 - 6)	37,9
2.	500	66,9	42	66,9 + 6 - 42	30,9
3.	1000	61,5	42	61,5 + 6 -42	25,5
4.	2000	57,0	42	57,0 + 6 - 42	21,0
5.	4000	53,0	42+6	53,0 + 6 - (42 + 6)	11,0
6.	6000	48,5	42+6	48,5 + 6 - (42 + 6)	6,5

Уровень ощущения формант **Е**ф определяется из выражения:
Еф= **L**р – **L**ш.

Номер октавы	Ср. частота, ***f***р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-45, **L**ш, дБ	**Е**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости ***w***i по табл. 3
1.	250	37,9	54	-16,1	0
2.	500	30,9	49	-18,1	0
3.	1000	25,5	45	-19,5	0
4.	2000	21,0	42	-21,0	0
5.	4000	11,0	40	-29,0	0
6.	6000	6,5	38	-31,5	0

По формуле (2) находим суммарную разборчивость формант

А ф.русск.= 0 (0%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. < 15%, в соответствии с табл. 6 смысл разговора за окном не будет понятен.

3. Коридор

По формуле (6) определяем величину звукоизоляции неоднородной перегородки, которыми являются внутренняя стена и дверь:

$\mathbf{Q}пер = \mathbf{Q}1-10\boldsymbol{lg}[1+(\mathbf{S}o/(\mathbf{S}1 + \mathbf{S}o))*(10^{0,1(\mathbf{Q}1-\mathbf{Q}o)}-1)]$,

где $\mathbf{Q}1 = 48$ дБ;

$\mathbf{Q}o = 18$ дБ;

$(\mathbf{S}o/(\mathbf{S}1 + \mathbf{S}o)) = 0,2$.

$\mathbf{Q}пер = 59-10\boldsymbol{lg}[1+0,2*(10^{0,1(48-18)}-1)] = 25$ дБ

Уменьшение звукоизоляции стены с дверью составило 23 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

№ октавы	Ср. частота, ***f***р	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	25-6	67,9 + 6 - (25 - 6)	54,9
2.	500	66,9	25	66,9 + 6 - 25	47,9
3.	1000	61,5	25	61,5 + 6 - 25	42,5

Продолжение таблицы

4.	2000	57,0	25	57,0 + 6 - 25	38
5.	4000	53,0	25+6	53,0 + 6 - (25 + 6)	28
6.	6000	48,5	25+6	48,5 + 6 - (25 + 6)	23,5

Уровень ощущения формант **Е**ф определяется из выражения:
Еф= **L**р – **L**ш.

№ октавы	Ср. частота, ***f***р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-40, **L**ш, дБ	**Е**ф= **L**р – **L**ш, дБ	Значения коэффициентов разборчивости ***w***i по табл. 3
1.	250	54,9	49	5,9	0,4
2.	500	47,9	44	3,9	0,35
3.	1000	42,5	40	2,5	0,3
4.	2000	38	37	1	0,25
5.	4000	28	35	-7	0,05
6.	6000	23,5	33	-9,5	0,03

По формуле (2) находим суммарную разборчивость формант
А ф.русск.= 0,05*(1,34***w***1 + 2,5 ***w***2 + 4,24***w***3 +5,88 ***w***4+5***w***5+1,04***w***6) =
= 0,05*(1,34x0,4 + 2,5x0,35 + 4,24x0,3 + 5,88x0,25 +
+ 5,0x0,05 + 1,04x0,03) = 0,22 (22%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. = 22%. В соответствии с табл. 6 смысл разговора за дверью будет понятен, слышимость удовлетворительная. Необходимо обеспечить звуковую изоляцию стены и двери.

Задание.

В соответствии со схемой (рис. 1) рассчитать суммарную разборчивость формант в смежном помещении, коридоре и за наружной стеной. Сделать выводы о возможности или невозможности утечки звуковой информации.

Уровни интенсивности речи в октавных полосах берутся из табл. 1, для всех вариантов они одинаковы.

Номер варианта	1. Смежное помещение	2. Наружная стена	3. Коридор
1.	Стена (табл. 7 п. 1.1) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.2) Окно (табл. 7 п. 2.1) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.1) Дверь (табл. 7 п. 3.1) **S**o = 20% **ПС**-25 (табл. 1)

Продолжение таблицы

Номер варианта	1. Смежное помещение	2. Наружная стена	3. Коридор
2.	Стена (табл. 7 п. 1.6) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.3) Окно (табл. 7 п. 2.2) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.6) Дверь (табл. 7 п. 3.2) **S**o = 30% **ПС**-30 (табл. 1)
3.	Стена (табл. 7 п. 1.10) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.4) Окно (табл. 7 п. 2.3) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.10) Дверь (табл. 7 п. 3.3) **S**o = 20% **ПС**-35 (табл. 1)
4.	Стена (табл. 7 п. 1.17) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.5) Окно (табл. 7 п. 2.4) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.17) Дверь (табл. 7 п. 3.4) **S**o = 30% **ПС**-25 (табл. 1)
5.	Стена (табл. 7 п. 1.18) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.7) Окно (табл. 7 п. 2.5) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.18) Дверь (табл. 7 п. 3.5) **S**o = 20% **ПС**-30 (табл. 1)
6.	Стена (табл. 7 п. 1.20) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.8) Окно (табл. 7 п. 2.6) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.20) Дверь (табл. 7 п. 3.6) **S**o = 30% **ПС**-35 (табл. 1)
7.	Стена (табл. 7 п. 1.21) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.9) Окно (табл. 7 п. 2.7) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.21) Дверь (табл. 7 п. 3.7) **S**o = 20% **ПС**-25 (табл. 1)
8.	Стена (табл. 7 п. 1.22) **ПС**-30 (табл. 1);	Стена (табл. 7 п. 1.13) Окно (табл. 7 п. 2.8) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.22) Дверь (табл. 7 п. 3.8) **S**o = 30% **ПС**-30 (табл. 1)
9.	Стена (табл. 7 п. 1.24) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.14) Окно (табл. 7 п. 2.9) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.24) Дверь (табл. 7 п. 3.9) **S**o = 20% **ПС**-35 (табл. 1)
10.	Стена (табл. 7 п. 1.25) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.15) Окно (табл. 7 п. 2.10) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.25) Дверь (табл. 7 п. 3.10) **S**o = 30% **ПС**-25 (табл. 1)
11.	Стена (табл. 7 п. 1.26) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.16) Окно (табл. 7 п. 2.11) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.26) Дверь (табл. 7 п. 3.11) **S**o = 20% **ПС**-30 (табл. 1)

Продолжение таблицы

Номер варианта	1. Смежное помещение	2. Наружная стена	3. Коридор
12.	Стена (табл. 7 п. 1.30) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.19) Окно (табл. 7 п. 2.12) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.30) Дверь (табл. 7 п. 3.1) **S**o = 30% **ПС**-35 (табл. 1)
13.	Стена (табл. 7 п. 1.34) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.27) Окно (табл. 7 п. 2.13) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.34) Дверь (табл. 7 п. 3.2) **S**o = 20% **ПС**-25 (табл. 1)
14.	Стена (табл. 7 п. 1.35) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.31) Окно (табл. 7 п. 2.14) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.35) Дверь (табл. 7 п. 3.3) **S**o = 30% **ПС**-30 (табл. 1)
15.	Стена (табл. 7 п. 1.36) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.23) Окно (табл. 7 п. 2.15) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.36) Дверь (табл. 7 п. 3.4) **S**o = 20% **ПС**-35 (табл. 1)
16.	Стена (табл. 7 п. 1.37) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.32) Окно (табл. 7 п. 2.1) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.37) Дверь (табл. 7 п. 3.5) **S**o = 30% **ПС**-25 (табл. 1)
17.	Стена (табл. 7 п. 1.38) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.3) Окно (табл. 7 п. 2.2) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.38) Дверь (табл. 7 п. 3.6) **S**o = 20% **ПС**-30 (табл. 1)
18.	Стена (табл. 7 п. 1.39) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.32) Окно (табл. 7 п. 2.3) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.39) Дверь (табл. 7 п. 3.7) **S**o = 30% **ПС**-35 (табл. 1)
19.	Стена (табл. 7 п. 1.40) **ПС**-25 (табл. 1)	Стена (табл. 7 п. 1.23) Окно (табл. 7 п. 2.4) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.40) Дверь (табл. 7 п. 3.8) **S**o = 20% **ПС**-25 (табл. 1)
20.	Стена (табл. 7 п. 1.41) **ПС**-30 (табл. 1)	Стена (табл. 7 п. 1.31) Окно (табл. 7 п. 2.5) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7 п. 1.41) Дверь (табл. 7 п. 3.9) **S**o = 30% **ПС**-30 (табл. 1)
21.	Стена (табл. 7 п. 1.42) **ПС**-35 (табл. 1)	Стена (табл. 7 п. 1.19) Окно (табл. 7 п. 2.6) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7 п. 1.42) Дверь (табл. 7 п. 3.10) **S**o = 20% **ПС**-35 (табл. 1)

ЛАБОРАТОРНАЯ РАБОТА 2

ОЦЕНОЧНЫЙ РАСЧЕТ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ

Обобщенный электромагнитный канал (канал побочных электромагнитных излучений и наводок - ПЭМИН) состоит из каналов утечки, причинами возникновения которых являются:

излучения в окружающее пространство (в дальней зоне) электромагнитных полей технических средств (ТС) и соединяющих их линий связи (например, электромагнитное поле монитора и других устройств ПЭВМ);

излучение в окружающее пространство (в ближней зоне) электрической составляющей электромагнитного поля ТС (например, электрическое поле, излучаемое клавиатурой);

излучение в окружающее пространство (в ближней зоне) магнитной составляющей электромагнитного поля ТС (например, магнитное поле усилителя звуковой частоты);

паразитные наводки на отходящие и проходящие вблизи от ТС провода и кабели, на расположенные рядом внешние технические средства связи, взаимные наводки между линиями связи, обусловленные:

а) непосредственными электрической и магнитной паразитными связями в ближней зоне (например, наводки на провода электропитания, заземления (зануления), выходящие из ПЭВМ линии связи - сетевой адаптер, модем);

б) емкостной и индуктивной паразитными связями по посторонним проводам, проходящим рядом с ПЭВМ (например: проходящие вблизи ПЭВМ телефонные провода и стоящих рядом телефонные аппараты, провода и кабели от других устройств и т.п.);

в) паразитной связью через электромагнитное поле излучения в дальней зоне (например, наводки на провода, кабели ТС, расположенные на значительном удалении от ПЭВМ, но проходящие в непосредственной близости от линий передачи данных (телефонных проводов и кабелей ЛВС) и проводов электропитания, выходящих из ПЭВМ);

г) паразитными связями через общее полное сопротивление (например, наводки на провода электропитания, осуществляются через элементы фильтров питания).

Наличие сигналов, несущих конфидециальные сообщения, на границе и за пределами контролируемой зоны (КЗ) создает условия для утечки сообщений за счет перехвата этих сигналов злоумышленниками.

Совокупность источника информативного сигнала, среды распространения этого сигнала и приемника перехвата злоумышленника представляет собой “канал утечки” сообщений, эффективность которого определяется следующими факторами:

уровень информативного сигнала от источника;

ослабление и искажение сигнала в среде его распространения;

технические характеристики приемного устройства, используемого злоумышленником.

Чем ближе приемник сигнала к источнику, тем эффективнее работает канал утечки. Системным показателем качества канала утечки является отношение сигнал/помеха на входе приемника перехвата, которое определяется соотношениями параметров всех элементов канала утечки.

При организации защитных мероприятий исходят из того, что приемное устройство для перехвата информативных сигналов реализует потенциальную помехоустойчивость и может быть размещено в любом месте за пределами контролируемой зоны, вплоть до ее границы. При этом считается, что наблюдение и перехват могут осуществляться непрерывно в течение времени любой продолжительности.

Определяющий вид помех в канале утечки сообщений - аддитивные помехи, характеризующиеся тем, что смесь сигнала ***s(t)*** и помехи ***n(t)*** на входе приемника представляет собой их сумму: ***x(t) = s(t) + n(t).***

Примером аддитивных помех являются:

атмосферные помехи, обусловленные электрическими процессами в атмосфере, прежде всего грозовыми разрядами;

космические помехи, вызванные радиоизлучением Солнца и других небесных тел;

внутренние шумы радиоприемника, обусловленные хаотическим движением носителей заряда в самом приемнике;

индустриальные помехи, обусловленные работой электрических устройств и агрегатов;

помехи от посторонних радиостанций.

Атмосферные помехи - тот вид помех, который всегда присутствует в окружающем пространстве, поэтому при определении дальности распространения сообщений по каналу ПЭМИН необходимо учитывать не только естественное затухание сигнала, но и искажения, вносимые этими помехами. Остальные виды помех в данной лабораторной работе не учитываются.

Для расчета среднеквадратического значения напряженности поля $\mathbf{E}_а$ атмосферных помех используется следующая формула:

$$\mathbf{E}_а = 10\mathbf{lg}(\boldsymbol{T}_а/\boldsymbol{T}_о) - 95{,}5 + 20\mathbf{lg}\boldsymbol{f} + 10\mathbf{lg}\boldsymbol{f}_{экв}, \text{ дБ}, \qquad (1)$$

где $\boldsymbol{f}$ **-** частота (Мгц);

$\boldsymbol{f}_{экв}$ -ширина полосы пропускания приемника (Гц);

$\boldsymbol{T}_а$ - эквивалентная шумовая температура, характеризующая интенсивность помех;

$\boldsymbol{T}_о = 273^{o}$K.

Ширина полосы пропускания приемника $\boldsymbol{f}_{экв}$ в диапазоне частот выше 30 МГц должна быть не менее 40 кГц, что соответствует характеристикам цело-

го ряда устройств, предназначенных для осуществления съема и анализа информации с ПЭВМ.

В соответствии с выражением (1) и значениях $\mathbf{T}_a$ = 293°K, $f_{экв}$=40 Мгц расчитаем среднеквадратическую напряженность поля $\mathbf{E}_a$:

на частоте 100 Мгц - $\mathbf{E}_a$ = -9,2 дБ (0,346 мкВ/м);

на частоте 500 Мгц - $\mathbf{E}_a$ = 4,8 дБ (1,738 мкВ/м);

на частоте 1000 Мгц - $\mathbf{E}_a$ = 10,8 дБ (3,467 мкВ/м).

Электромагнитное поле, создаваемое промышленными ВЧ-установками, затухает со средним коэффициентом:

$$\mathbf{k}_з = 1 / \mathbf{r}^n, \qquad (2)$$

где **r** - расстояние от источника;

n = 1,3 - 2,8 (**n** = 1,3 - для открытых сельских районов; **n** = 2,8 - для интенсивно застроенных городских районов).

Напряженность электромагнитного поля, создаваемого ПЭВМ, сертифицированной по ЭМС в соответствии с требованиями CISPR, не должна превышать:

в диапазоне 30 - 230 МГц - 630,5 мкВ/м;

в диапазоне 230 - 1000 МГц - 1412,5 мкВ/м.

Электромагнитное поле также затухает с коэффициентом $k_{экр}$ при распространении через ограждающие конструкции. Значения коэффициентов экранирования некоторых ограждающих конструкций приведены в табл. 1.

Таблица 1

Значения коэффициентов экранирования некоторых ограждающих конструкций на частотах 100, 500 и 1000 МГц

Номер п/п	Тип здания	Экранирование (дБ) (коэффициент экранирования $k_{экр}$) на частотах:		
		100 Мгц	500 МГц	1000 МГц
	Деревянное здание с толщиной стен 20 см:			
1.	окно без решетки	5-7 (1,8-2,2)	7-9 (2,2-2,8)	9-11 (2,8-3,5)
2.	окно закрыто решеткой с ячейкой 5 см	6-8 (2,0-2,5)	10-12 (3,2-4,0)	12-14 (4,0-5,0)
	Кирпичное здание с толщиной кирпичной стены 1,5 кирпича:			
3.	окно без решетки	13-15 (4,5-5,6)	15-17 (5,6-7,0)	16-19 (6,3-8,9)

Продолжение таблицы 1

4.	окно закрыто решеткой с ячейкой 5 см	17-19 (7,0-8,9)	20-22 (10,0-12,6)	22-25 (12,6-17,8)
	Железобетонные здания с ячейкой арматуры 15х15 см и толщиной 160 мм:			
5.	окно без решетки	20-25 (10,0-17,8)	18-19 (8,0-8,9)	15-17 (5,6-7,0)
6.	окно закрыто решеткой с ячейкой 5 см	28-32 (25,1-39,8)	23-27 (14,1-22,4)	20-25 (10,0-17,8)
Примечание: оконный проем составляет не более 30% от площади стены.				

Напряженность электромагнитного поля **E** на границе контролируемой зоны вычисляется по следующей формуле:

$$\mathbf{E}_{кз} = \mathbf{E}^* \mathbf{k}_з * \mathbf{k}_{экр} \text{ (мкВ/м)}, \qquad (3)$$

где **E** - напряженность электромагнитного поля непосредственно у ПЭВМ;

$\mathbf{k}_з$ - коэффициент затухания (2);

$\mathbf{k}_{экр}$ - коэффициент экранирования (табл. 1).

Для обнаружения сигналов известной формы в шумах наибольшее распространение получил критерий максимума отношения пикового значения сигнала ***s(t)*** к среднеквадратическому значению σ шума на выходе оптимального фильтра, которое определяется отношением полной энергии входного сигнала к спектральной плотности мощности входного белого шума (атмосферные помехи):

$$\Delta = \frac{S(t)_{вых}}{\sigma_{вых}} = \sqrt{\frac{2Q_{вх}}{N_{0вх}}}, \qquad (4)$$

где **Q** - полная энергия сигнала на входе приемника перехвата;

$\mathbf{N}_0/2$ - спектральная плотность мощности белого шума (атмосферной помехи) на входе приемника;

s(t) - пиковое значение сигнала на выходе фильтра приемника;

σ - среднеквадратическое значение помехи на выходе фильтра приемника.

Для практического применения формулы (4) необходимо определить максимальное значение Δ, при котором исключается определение злоумышленником содержания (смысла) перехваченного сообщения, т.е. определить смысловой критерий безопасности сообщений.

Было показано, что значение Δ не должно превышать:

$\Delta \le 1$ (для важных информации); (5)

$\Delta \le 0{,}7$ (для весьма важной информации). (6)

При приеме методом накопления, отношение сигнал/помеха Δ_Σ на входе решающего устройства ($2\mathbf{Q}/\mathbf{N}_O$) возрастает в **n** (количество повторений) раз по сравнению с отношением сигнал/помеха на входе приемника при однократном отсчете, т.е.:

$$\Delta_\Sigma = \sqrt{\frac{2Q}{N_0}} = \Delta\sqrt{n} \le 1. \quad (7)$$

Чтобы это соотношение выполнялось, Δ_Σ должно быть в $\sqrt{n}$ раз меньше Δ, определенной без учета повторений.

$$\Delta_\Sigma \le \frac{\Delta}{\sqrt{n}}. \quad (8)$$

Величину **n** можно установить из следующих соображений. При просмотре изображения на экране дисплея в течение t сек. изображение появляется $f_{\text{разв}}\mathbf{t}/2$ раз при чересстрочной кадровой развертке. С учетом сказанного, выражение (8) принимает следующий вид:

$$\Delta_\Sigma = \Delta\sqrt{\frac{2}{f_{\text{раз в}}t}}. \quad (9)$$

В соответствии с формулой (9) при частоте кадровой развертки 85 Гц и просмотре изображения в течение 15 сек. отношение сигнал/шум Δ на границе контролируемой зоны должно быть не более 0,04. Время, равное 15 сек. выбрано из тех соображений, что устройства, осуществляющие накопление сигналов на фоне помех, эффективно работают только в течение первых 10-15 сек. после перехвата сообщений.

Приведем пример расчета защищенности помещения от утечки информации по электромагнитному каналу. В качестве источника электромагнитного излучения возьмем ПЭВМ, расположенную на некотором удалении от контролируемой зоны (рис.1).

Пример расчета.

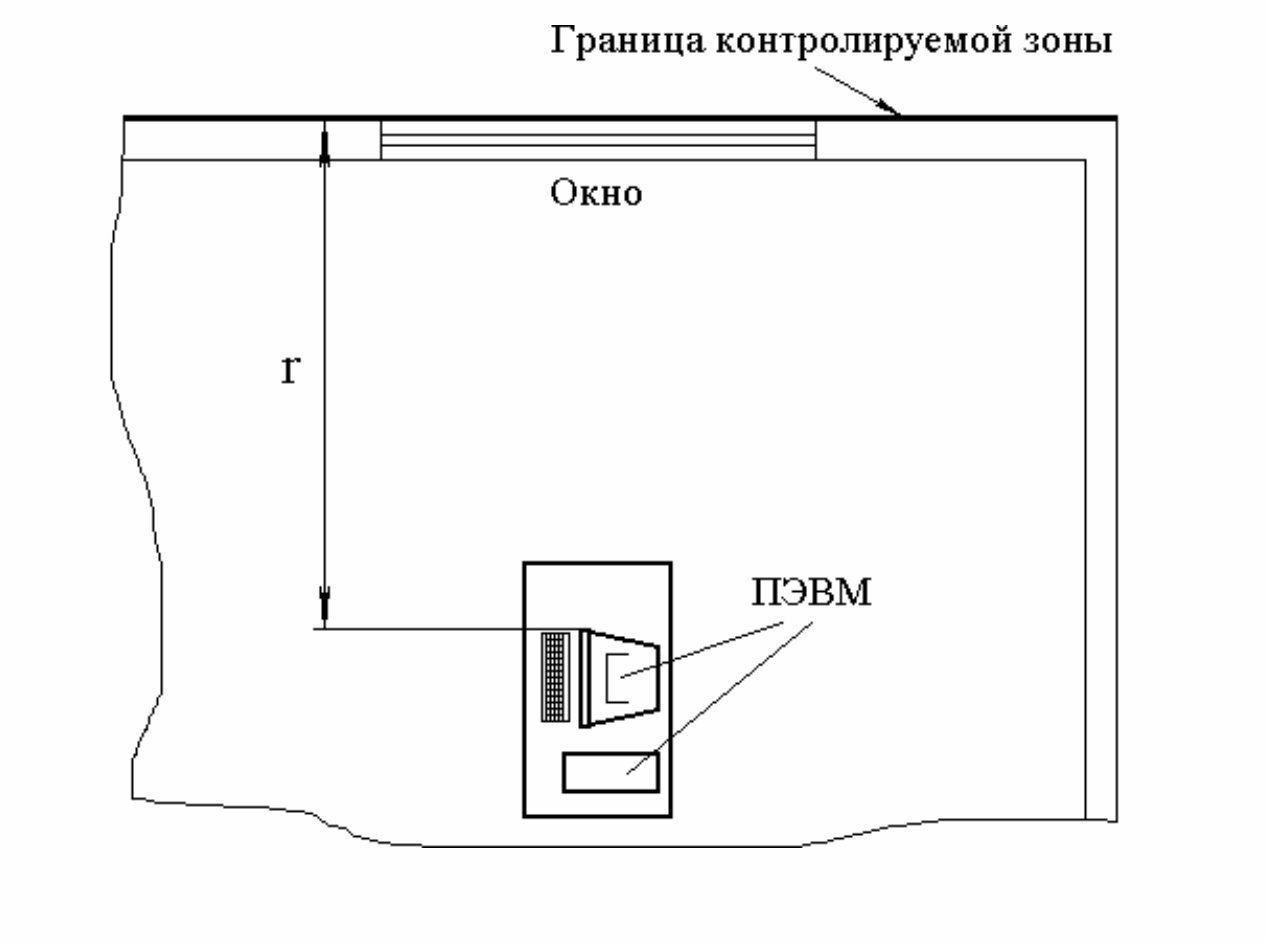

Рис. 2. Схема помещения для проведения расчетов

Таблица 2

Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ

Номер п/п	Значения электромагнитного поля **E** (мкВ/м) на частотах		
	100 МГц	500 МГц	1000 МГц
1.	630	1400	1400
2.	610	1370	1390
3.	620	1420	1400
4.	610	1360	1400
5.	600	1360	1390
6.	630	1410	1400

Исходные данные.

В помещении расположена ПЭВМ (рис.1), на которой обрабатываются конфидециальные данные. Расстояни от ПЭВМ до контролируемой зоны со-

ставляет r = 15 м. Граница контролируемой зоны проходит по периметру железобетонной стены толщиной 160 мм, в стене имеется оконный проем, не превыщающий 30% площади стены. Окно закрыто металлической решеткой с ячейкой 5 см (табл. 1, п. 6). Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ на частотах 100 МГц, 500МГц и 1000 МГц, берем из табл. 2, п. 6. При определении коэффициента затухания принимаем **n**=1,4. В качестве кретерия защищенности помещения от утечки информации на границе контролируемой зоны отношение сигнал / шум принимаем равным $\Delta \leq 1$.

Результаты расчета сводим в таблицу:

Ход вычислений	Данные, полученные из таблиц или в результате расчетов, на частотах		
	100 МГц	500 МГц	1000 МГц
Из табл. 2, п. 6 выбираем значения электромагнитного поля **E**, создаваемого ПЭВМ, мкВ/м	610	1370	1390
Определяем коэффициент затухания по формуле $\mathbf{k}_з = 1 / \mathbf{r}^n$, **r** = 15, **n** = 1,4	0,0226		
Выбираем из табл. 2, п. 6 максимальные значения коэффициента экранирования $\mathbf{k}_{экр}$	39,8	22,4	17,8
Определяем напряженность электромагнитного поля на границе контролируемой зоны по формуле (2) $\mathbf{E}_{кз} = \mathbf{E}^* \mathbf{k}_з * \mathbf{k}_{экр}$, мкВ/м	0,346	1,38	1,76
Определяем среднеквадратическое значение напряженности поля $\mathbf{E}_a$ атмосферных помех по формуле (1), принимая $\mathbf{T}_a = 293^oK$, $\boldsymbol{f}_{экв}$=40 МГц	0,346	1,738	3,467
Определяем отношение сигнал/шум на границе контролируемой зоны по формуле $\Delta = \mathbf{E}_{кз} / \mathbf{E}_a$	0,999≈1	0,79	0,51

Расчеты показали, что на всех частотах значение $\Delta \leq 1$. Следовательно, расстояние до границы контролируемой зоны достаточно для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ. Дополнительных мер по обеспечению защиты помещения от утечки информации не требуется.

Задание

1. В соответствии со схемой (рис. 1) произвести расчеты защищенности помещения от утечки информации по электромагнитному каналу.

Среднеквадратические значения напряженности поля $\mathbf{E}_a$ атмосферных помех не расчитывать, считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
$\mathbf{E}_a$, мкВ/м ($\mathbf{T}_a$=293°K, fэкв=40 Мгц)	0,346	1,738	3,467

Варианты:

Номер варианта	$\mathbf{k}_з = 1 / \mathbf{r}^n$		$\mathbf{k}_{экр}$ Таб. 1, пункт	**E** Таб. 2, пункт	**Δ**
	r	**n**			
1.	15	1,3	1	1	1
2.	20	1,4	2	2	1
3.	15	1,5	3	3	1
4.	20	1,6	4	4	1
5.	15	1,7	5	5	1
6.	20	1,8	6	6	1
7.	15	1,4	1	2	1
8.	20	1,5	2	3	1
9.	15	1,6	3	4	1
10.	20	1,7	4	5	1
11.	15	1,8	5	6	1
12.	20	1,3	6	1	0,7
13.	15	1,5	1	3	0,7
14.	20	1,6	2	4	0,7
15.	15	1,7	3	5	0,7
16.	20	1,8	4	6	0,7
17.	15	1,3	5	1	0,7
18.	20	1,4	6	2	0,7
19.	15	1,6	1	4	0,7
20.	20	1,7	2	5	0,7
21.	15	1,8	3	6	0,7

2. По заданным значениям **Δ** рассчитать **r** для частот 100, 500 и 1000 МГц.

ЛАБОРАТОРНАЯ РАБОТА 3

ИЗУЧЕНИЕ ТРАДИЦИОННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ. ШИФРЫ ПЕРЕСТАНОВКИ

1. Основные понятия и определения

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования – расшифровки.

В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является *криптостойкость,* которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия *шифра*.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

достаточная криптостойкость (надежность закрытия данных);

простота процедур шифрования и расшифровки;

незначительная избыточность информации за счет шифрования;

нечувствительность к небольшим ошибкам шифрования и др.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифры перестановки самые простые и, вероятно, самые древние шифры.

Шифр перестановки "скитала"

Известно, что в V в. до н. э. правители Спарты, наиболее воинственного из древнегреческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью **скитала**. - первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался скитала, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения (рис.1). Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Такой же результат можно получить, если буквы сообщения писать по кольцу

не подряд, а через определенное число позиций до тех пор, пока не будет исчерпан весь текст.

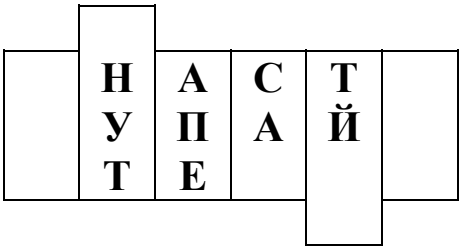

Рис. 1. Шифр "скитала"

Сообщение "НАСТУПАЙТЕ" при размещении его по окружности стержня по три буквы дает шифртекст:

НУТАПЕСА_ТЙ

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто. Шифр "скитала" в последующие времена многократно совершенствовался.

Шифрующие таблицы

В эпоху Возрождения (с конца XIV в.) начала возрождаться и криптография. Наряду с традиционными вариантами применения криптографии в политике, дипломатии и военном деле появляются и другие - защита интеллектуальной собственности от инквизиции или от злоумышленников. В разработанных шифрах того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

размер таблицы;

слово или фраза, задающие перестановку;

особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром "скитала". Например, сообщение:

"ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ"

записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рис. 2.

Т	**Н**	**П**	**В**	**Е**	**Г**	**Л**
Е	**А**	**Р**	**А**	**Д**	**О**	**Н**
Р	**Т**	**И**	**Е**	**Ь**	**В**	**О**
М	**О**	**Б**	**Т**	**М**	**П**	**Ч**
И	**Р**	**Ы**	**С**	**О**	**О**	**Ь**

Рис. 2. Заполнение таблицы из 5 строк и 7 столбцов

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровке действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый "одиночная перестановка по ключу". Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово:

"ПЕЛИКАН",

а текст сообщения возьмем из предыдущего примера. На рис. 3 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая - после перестановки.

КЛЮЧ
→

П	**Е**	**Л**	**И**	**К**	**А**	**Н**
7	**2**	**5**	**3**	**4**	**1**	**6**
Т	**Н**	**П**	**В**	**Е**	**Г**	**Л**
Е	**А**	**Р**	**А**	**Д**	**О**	**Н**
Р	**Т**	**И**	**Е**	**Ь**	**В**	**О**
М	**О**	**Б**	**Т**	**М**	**П**	**Ч**
И	**Р**	**Ы**	**С**	**О**	**О**	**Ь**

До перестановки

А	**Е**	**И**	**К**	**Л**	**Н**	**П**
1	**2**	**3**	**4**	**5**	**6**	**7**
Г	**Н**	**В**	**Е**	**П**	**Л**	**Т**
О	**А**	**А**	**Д**	**Р**	**Н**	**Е**
В	**Т**	**Е**	**Ь**	**И**	**О**	**Р**
П	**О**	**Т**	**М**	**Б**	**Ч**	**М**
О	**Р**	**С**	**О**	**Ы**	**Ь**	**И**

После перестановки

Рис 3. Таблицы, заполненные ключевым словом и текстом сообщения

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были понумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется **двойной перестановкой**. В этом случае перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рис. 4. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТЮАЕ ООГМ РЛИП ОЬСВ

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

	4	1	3	2
3	**П**	**Р**	**И**	**Л**
1	**Е**	**Т**	**А**	**Ю**
4	**В**	**О**	**С**	**Ь**
2	**М**	**О**	**Г**	**О**

Исходная таблица

	1	2	3	4
3	**Р**	**Л**	**И**	**П**
1	**Т**	**Ю**	**А**	**Е**
4	**О**	**Ь**	**С**	**В**
2	**О**	**О**	**Г**	**М**

Перестановка столбцов

	1	2	3	4
1	**Т**	**Ю**	**А**	**Е**
2	**О**	**О**	**Г**	**М**
3	**Р**	**Л**	**И**	**П**
4	**О**	**Ь**	**С**	**В**

Перестановка строк

Рис. 4. Пример выполнения шифрования методом двойной перестановки

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

для таблицы 3x3 - 36 вариантов;

для таблицы 4x4 - 576 вариантов;

для таблицы 5x5 - 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто "взламывается" при любом размере таблицы шифрования.

Магические квадраты

В средние века для шифрования перестановкой применялись "магические квадраты". Так называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в "магические квадраты" в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью "магических квадратов" шифртексты охраняет не только ключ, но и магическая сила.

Пример "магического квадрата" и его заполнения сообщением **"ПРИЛЕТАЮ ВОСЬМОГО"** показан на рис. 5.

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

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рис 5. Пример "магического квадрата" 4x4 и его заполнения

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Число "магических квадратов" быстро возрастает с увеличением размера квадрата. Существует только один "магический квадрат" размером 3x3 (если не учитывать его повороты). Количество "магических квадратов" 4x4 составляет уже 880, а количество магических квадратов 5x5 - около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную перебор всех вариантов для такого шифра.

Задание.

1. Зашифровать 81 символ текста методом одиночной перестановки по ключу (см. рис. 3). Нумерацию символов ключевого слова проводить по табл. 1. Знаки препинания и пробелы не учитывать.

2. Поменяться с соседом зашифрованными текстами и ключами. Расшифровать текст.

Таблица 1

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

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

Номер варианта	Текст	Ключевое слов
1.	ДУМАЕТСЯ, ЧТО КАЖДОМУ ЧИТАТЕЛЮ ДАННОГО ПОСОБИЯ ДОВОДИЛОСЬ СДАВАТЬ КАКИЕ-ЛИБО ЭКЗАМЕНЫ И ВЫ ВСЕ БОЛЕЕ ИЛИ МЕНЕЕ ПРЕДСТАВЛЯЕТЕ СЕБЕ, ЧТО ЭТО ТАКОЕ.	ДИПЛОМАНТ
2.	ТЕМ НЕ МЕНЕЕ, ДЛЯ РАЗРАБОТКИ ПОДЛИННО НАУЧНОГО ПОДХОДА НЕОБХОДИМО ТОЧНОЕ ОПРЕДЕЛЕНИЕ ИЗУЧАЕМОГО ЯВЛЕНИЯ.	КИМБЕРЛИТ
3.	БУДЬ Я МИНИСТРОМ ОБРАЗОВАНИЯ, ВО ВСЕХ ВУЗАХ ВВЕЛ БЫ В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ ИЗУЧЕНИЕ МЕТОДОВ ОТЛЫНИВАНИЯ, ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ШПАРГАЛОК И ИСКУССТВА ЛИТЬ ВОДУ, ПРИЧЕМ С ОБЯЗАТЕЛЬНЫМ ЭКЗАМЕНОМ	КРОНШТЕЙН
4.	ВООБРАЗИТЕ ОТРАДНУЮ КАРТИНУ: СТУДЕНТ, ИЗГОТОВЛЯЮЩИЙ "ШПОРЫ" НА ЭКЗАМЕН ПО ШПАРГАЛКОВЕДЕНИЮ	КРУПОЗНЫЙ
5.	И ДЕЙСТВИТЕЛЬНО, В ПРОЦЕССЕ ЭКЗАМЕНА ИСПЫТЫВАЮТСЯ САМЫЕ РАЗНООБРАЗНЫЕ КАЧЕСТВА СТУДЕНТА - ОТ ОРАТОРСКОГО МАСТЕРСТВА ДО ИСКУССТВА ПАНТОМИМЫ	МАССАЖИСТ
6.	СРАЗУ ХОЧУ ОТМЕТИТЬ МОЕ ПРИНЦИПИАЛЬНОЕ НЕСОГЛАСИЕ С ОБЩЕПРИНЯТЫМИ ТРАКТОВКАМИ, В КОТОРЫХ СТУДЕНТ ВЫСТУПАЕТ ПАССИВНЫМ ОБЪЕКТОМ, НАД КОТОРЫМ ЭКЗАМЕНАТОРЫ ПРОДЕЛЫВАЮТ КАКИЕ-ЛИБО ТОЛЬКО ИМ ПОДКОНТРОЛЬНЫЕ ДЕЙСТВИЯ	КРУПЧАТКА
7.	НАПРОТИВ, ИДЕАЛЬНЫЙ ЭКЗАМЕНАТОР ВЫПОЛНЯЕТ РОЛЬ БЕСПРИСТРАСТНОГО ИЗМЕРИТЕЛЯ	ЛАНДКАРТА

Номер варианта	Текст	Ключевое слов
	УРОВНЯ ЗНАНИЙ СТУДЕНТА	
8.	СЛЕДУЕТ ПРИЗНАТЬ, ЧТО ТАКОЙ ТИП В ПРИРОДЕ НЕ ВСТРЕЧАЕТСЯ. ЭКЗАМЕНАТОР МОЖЕТ БЫТЬ НАСТРОЕН ПО ОТНОШЕНИЮ К СТУДЕНТУ ПОЛОЖИТЕЛЬНО ИЛИ ОТРИЦАТЕЛЬНО, НО ВЕДЬ ТАКИМ ЕГО ДЕЛАЕТ САМ СТУДЕНТ	ЛАМАРКИЗМ
9.	СЛЕДОВАТЕЛЬНО, ЭКЗАМЕН НАЧИНАЕТСЯ НЕ ТОГДА, КОГДА ВАША ДРОЖАЩАЯ РУКА ТЯНЕТСЯ ЗА БИЛЕТОМ, А ЕЩЕ ПРИ ПЕРВОЙ ВСТРЕЧЕ СТУДЕНТА С БУДУЩИМ ЭКЗАМЕНАТОРОМ	ЛАКРИНЧИК
10.	ЭКЗАМЕН МОЖНО ОПРЕДЕЛИТЬ КАК СОВОКУПНОСТЬ ДЕЙСТВИЙ СТУДЕНТА, НАПРАВЛЕННЫХ НА ТО, ЧТОБЫ ЭКЗАМЕНАТОР ПОСЧИТАЛ ЕГО ДОСТОЙНЫМ КАК МОЖНО БОЛЕЕ ВЫСОКОЙ ОЦЕНКИ	ОРТОПЕДИЯ
11.	ДО СИХ ПОР Я ЧАСТО ВСПОМИНАЮ СВОЙ ПОСЛЕДНИЙ ШКОЛЬНЫЙ ЭКЗАМЕН ПО ФИЗИКЕ. ПРИНИМАЛА ЕГО УЧИТЕЛЬНИЦА, ТВЕРДО УВЕРЕННАЯ В МОИХ ГЛУБОКИХ ПОЗНАНИЯХ В ЭТОЙ ОБЛАСТИ	СЕРПОВИЩЕ
12.	ВОЛЕЙ СУДЕБ МНЕ ПРИШЛОСЬ ОТВЕЧАТЬ НА ВОПРОС О ФИЛОСОФСКИХ КОНЦЕПЦИЯХ, ПРИМЕНИМЫХ В ФИЗИКЕ. ОБ ЭТОМ Я НЕ ЗНАЛ АБСОЛЮТНО НИЧЕГО	СУСПЕНЗИЯ
13.	ДЛЯ ТОГО, ЧТОБЫ РАССМАТРИВАТЬ В ДАЛЬНЕЙШЕМ ВОПРОСЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ, НЕОБХОДИМО НАПОМНИТЬ ОСНОВНЫЕ ПОНЯТИЯ, КОТОРЫМИ ОПЕРИРУЕТ ТЕОРИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	ОБРАБОТКА
14.	ОСНОВНОЙ ОСОБЕННОСТЬЮ ЛЮБОЙ СЕТЕВОЙ СИСТЕМЫ ЯВЛЯЕТСЯ ТО, ЧТО ЕЕ КОМПОНЕНТЫ РАСПРЕДЕЛЕНЫ В ПРОСТРАНСТВЕ И СВЯЗЬ МЕЖДУ НИМИ ФИЗИЧЕСКИ ОСУЩЕСТВЛЯЕТСЯ ПРИ ПОМОЩИ СЕТЕВЫХ СОЕДИНЕНИЙ	ОПАСНОСТЬ
15.	УГРОЗА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО ПОТЕНЦИАЛЬНО ВОЗМОЖНОЕ ПРОИСШЕСТВИЕ, НЕВАЖНО, ПРЕДНАМЕРЕННОЕ ИЛИ НЕТ, КОТОРОЕ МОЖЕТ ОКАЗАТЬ НЕЖЕЛАТЕЛЬНОЕ ВОЗДЕЙСТВИЕ НА САМУ СИСТЕМУ, А ТАКЖЕ НА ИНФОРМАЦИЮ, ХРАНЯЩУЮСЯ В НЕЙ	СОВЕТСКИЙ
16.	УЯЗВИМОСТЬ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО НЕКАЯ ЕЕ НЕУДАЧНАЯ ХАРАКТЕРИСТИКА, КОТОРАЯ ДЕЛАЕТ ВОЗМОЖНЫМ ВОЗНИКНОВЕНИЕ УГРОЗЫ	ОТНОШЕНИЕ
17.	УГРОЗА ОТКАЗА В ОБСЛУЖИВАНИИ ВОЗНИКАЕТ ВСЯКИЙ РАЗ, КОГДА В РЕЗУЛЬТАТЕ НЕКОТОРЫХ	

Номер варианта	Текст	Ключевое слов
	ДЕЙСТВИЙ БЛОКИРУЕТСЯ ДОСТУП К НЕКОТОРОМУ РЕСУРСУ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ	ИЕРУСАЛИМ
18.	АТАКА НА КОМПЬЮТЕРНУЮ СИСТЕМУ - ЭТО ДЕЙСТВИЕ, ПРЕДПРИНИМАЕМОЕ ЗЛОУМЫШЛЕННИКОМ, КОТОРОЕ ЗАКЛЮЧАЕТСЯ В ПОИСКЕ И ИСПОЛЬЗОВАНИИ ТОЙ ИЛИ ИНОЙ УЯЗВИМОСТИ	НАЧАЛЬНИК
19.	ИССЛЕДОВАТЕЛИ ОБЫЧНО ВЫДЕЛЯЮТ ТРИ ОСНОВНЫХ ВИДА УГРОЗ БЕЗОПАСНОСТИ - ЭТО УГРОЗЫ РАСКРЫТИЯ, ЦЕЛОСТНОСТИ И ОТКАЗА В ОБСЛУЖИВАНИИ	ПОКОЛЕНИЕ
20.	В ТЕРМИНАХ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УГРОЗА РАСКРЫТИЯ ИМЕЕТ МЕСТО ВСЯКИЙ РАЗ, КОГДА ПОЛУЧЕН ДОСТУП К НЕКОТОРОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМОЙ ОТ ОДНОЙ СИСТЕМЫ К ДРУГОЙ	КОНЦЕПЦИЯ
21.	УГРОЗА ЦЕЛОСТНОСТИ ВКЛЮЧАЕТ В СЕБЯ ЛЮБОЕ УМЫШЛЕННОЕ ИЗМЕНЕНИЕ ДАННЫХ, ХРАНЯЩИХСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМЫХ ИЗ ОДНОЙ СИСТЕМЫ В ДРУГУЮ	ОТНОШЕНИЕ

ЛАБОРАТОРНАЯ РАБОТА 4

ИЗУЧЕНИЕ ТРАДИЦИОННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ. ШИФРЫ ЗАМЕНЫ

1. Шифры простой замены

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Полибианский квадрат.

Одним из первых шифров простой замены считается так называемый *полибианский квадрат.* За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5x5, заполненную буквами греческого алфавита в случайном порядке (рис. 1).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	x
χ	ν		φ	ι

Рис. 1. Полибианский квадрат, заполненный случайным образом 24 буквами греческого алфавита и пробелом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова:

ταυροσ

получается шифртекст

χφδμτξ

Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

Система шифрования Цезаря.

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название он получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на **К** букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении **К = 3**. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для **К = 3** показана в табл. 1.

Таблица 1

Одноалфавитные подстановки (К = 3, m = 26).

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

Например, послание Цезаря

"VENI VIDI VICI"

(в переводе на русский означает "Пришел, Увидел, Победил"), направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело бы в зашифрован ном виде так:

YHQL YLGL YLFL

Достоинством системы шифрования Цезаря является простота шифрования и расшифровки. К недостаткам системы Цезаря следует отнести следующие:

подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;

сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения **К** изменяются только начальные позиции такой последовательности;

число возможных ключей **К** мало;

шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте.

Криптоаналитическая атака против системы одноалфавитной замены начинается с подсчета частот появления символов: определяется число появлений каждой буквы в шифртексте. Затем полученное распределение частот букв в шифртексте сравнивается с распределением частот букв в алфавите исходных сообщений, например, в английском. Буква с наивысшей частотой по явления в шифртексте заменяется на букву с наивысшей частотой появления в английском языке и т.д. Вероятность успешного вскрытия системы шифрования повышается с увеличением длины шифртекста.

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

Система Цезаря с ключевым словом

Система шифрования Цезаря с ключевым словом является одноалфавитной системой подстановки. Особенность этой системы - использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки.

Выберем некоторое число **k, 0 ≤ k ≤ 25** и слово или короткую фразу в качестве ***ключевого слова***. Желательно, чтобы все буквы ключевого слова были различными. Пусть выбраны слово **DIPLOMAT** в качестве ключевого слова и число **k = 5**.

Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом **k**:

0	1	2	3	4	5					10					15					20					25
A	B	C	D		F	H	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
					D	I	P	L	O	M	A	T													

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

0	1	2	3	4	5					10					15					20					25
A	B	C	D		F	H	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B	C	E	F	G	H	J	K	N	Q	R	S	U

Теперь мы имеем подстановку для каждой буквы произвольного сообщения.

Исходное сообщение **SEND MORE MONEY** шифруется как **HZBY TCGZ TCBZS.**

Следует отметить, что требование о различии всех букв ключевого слова не обязательно. Можно просто записать ключевое слово (или фразу) без повторения одинаковых букв. Например, ключевая фраза: "**КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН"** и число **k = 3** порождают следующую таблицу подстановок:

0	1	2	3		5				10										20						25					30
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	Ь	Ы	Ъ	Э	Ю	Я
Ъ	Э	Ю	К	А	Д	Ы	М	О	Т	Е	Ч	С	В	Н	Л	И	П	Р	Я	Б	Г	Ж	З	Й	У	Ф	Х	Ц	Ш	Щ	Ь

Несомненное достоинство системы Цезаря с ключевым словом - то, что количество возможных ключевых слов практически неисчерпаемо. Недостатком этой системы является возможность взлома шифртекста на основе анализа частот появления букв.

Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В ней он впервые систематизировал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифровки.

Поясним этот метод шифрования на примере. Для русско го алфавита шифрующая таблица может иметь размер 4х8. Берем в качестве ключа слово "БАНДЕРОЛЬ". Шифрующая таблица с таким ключом показана на рис. 2.

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

Рис. 2. Шифрующая таблица с ключевым словом "БАНДЕРОЛЬ"

Как и в случае полибианского квадрата, при шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца. Например, при шифровании с помощью этой таблицы сообщения:

"ВЫЛЕТАЕМПЯТОГО"

получаем шифртекст:

"ПДКЗЫВЗЧШЛЫЙСЙ".

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются ***биграммными.***

Биграммный шифр Плейфейра.

Шифр Плейфейра, изобретенный в 1854 г. - наиболее известный биграммный шифр замены. Он применялся Великобританией во время первой мировой войны. Основой шифра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущего раздела (см. рис 2.)

Процедура шифрования включает следующие этапы.

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв, и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

а) если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и И в табл. на рис.2), тогда находят буквы в углах прямоугольника, определяемого данной парой букв (в нашем примере это буквы АЙОВ. Пара букв АЙ отображается в пару 0В. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста);

б) если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними (например, биграмма НС дает биграмму шифртекста ГЩ); если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца (например, биграмма ВШ дает биграмму шифртекста ПА);

в) если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них (например, биграмма НО дает биграмму шифртекста ДЛ); если при этом буква от крытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке (например, биграмма ФЦ дает биграмму шифртекста ХМ.).

Зашифруем текст:

"ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ"

Разбиение этого текста на биграммы дает:

"ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ"

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы (см. рис. 2.8) в следующую последовательность биграмм шифртекста:

"ГП ДУ 0В ДЛ НУ ПД ДР ЦЫ ГА ЧТ".

При расшифровке применяется обратный порядок действий.

Следует отметить, что шифрование биграммами резко повышает стойкость шифров к вскрытию. Хотя книга И. Трисемуса "Полиграфия" была относительно доступной, описанные в ней идеи получили признание лишь спустя три столетия. По всей вероятности, это было обусловлено плохой осведомленностью криптографов о работах богослова и библиофила Трисемуса в области криптографии.

2. Шифры сложной замены

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свои шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты.

При **r** - алфавитной подстановке символ $\mathbf{x_0}$ исходного сообщения заменяется символом $\mathbf{y_0}$ из алфавита $\mathbf{B_0}$, символ $\mathbf{x_i}$ -символом **yi**, из алфавита $\mathbf{B_1}$, и так далее, символ $\mathbf{x}_{r-1}$ заменяется символом $\mathbf{y}_{r-1}$ из алфавита $\mathbf{B}_{r-1}$, символ $\mathbf{x}_r$ заменяется символом $\mathbf{y}_r$ снова из алфавита $\mathbf{B_0}$, и т.д.

Общая схема многоалфавитной подстановки для случая r = 4 показана на рис.3.

Входной символ	$\mathbf{X_0}$	$\mathbf{X_1}$	$\mathbf{X_2}$	$\mathbf{X_3}$	$\mathbf{X_4}$	$\mathbf{X_5}$	$\mathbf{X_6}$	$\mathbf{X_7}$	$\mathbf{X_8}$	$\mathbf{X_9}$
Алфавит Подстановки	$\mathbf{B_0}$	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_0}$	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_0}$	$\mathbf{B_1}$

Рид. 3. **Схема r**-алфавитной подстановки для случая **r = 4**

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита **A** может быть преобразован в несколько различных символов шифровальных алфавитов $\mathbf{B_j}$. Степень обеспечиваемой защиты теоретически пропорциональна длине периода **r** в последовательности используемых алфавитов $\mathbf{B_j}$.

Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти, который также был известным архитектором и теоретиком искусства. Его книга "Трактат о шифре", написанная в 1566 г.,

представляла собой первый в Европе научный труд по криптологии. Кроме шифра многоалфавитной замены, Альберти подробно описал устройства из вращающихся колес для его реализации. Во всем мире Л.Альберти почитается основоположником криптологии.

Шифр Гронсфельда

Этот шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом. Под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа **е** (основания натуральных логарифмов – 2718), получаем для исходного сообщения "**ВОСТОЧНЫЙ ЭКСПРЕСС"** следующий шифртекст:

Сообщение	**В**	**О**	**С**	**Т**	**О**	**Ч**	**Н**	**Ы**	**Й**	**Э**	**К**	**С**	**П**	**Р**	**Е**	**С**	**С**
Ключ	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**
Шифртекст	**Д**	**Х**	**Т**	**Ь**	**Р**	**Ю**	**О**	**Г**	**Л**	**Д**	**Л**	**Щ**	**С**	**Ч**	**Ж**	**Щ**	**У**

Чтобы зашифровать первую букву сообщения (В), используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В в алфавите В-Г-Д; получается первая буква шифртекста - Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит есть лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

По существу шифр Гронсфельда представляет собой частный случай системы шифрования Вижинера.

Система шифрования Вижинера

Система Вижинера, впервые опубликованная в 1586 г., является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI в. Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рис. 4 показана таблица Вижинера для русского алфавита.

Таблица Вижинера используется для зашифрования и расшифровки. Таблица имеет два входа:

верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

крайний левый столбец ключа.

Ключ	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	Ь	Ы	Ъ	Э	Ю	Я
0	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	Ь	Ы	Ъ	Э	Ю	Я
1	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	Ь	Ы	Ъ	Э	Ю	Я	А
2	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б
3	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В
4	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г
5	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д
6	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е
7	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
8	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
9	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
10	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
11	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
12	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
13	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
14	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
15	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
16	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
17	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
18	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
19	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
20	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
21	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
22	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
23	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
24	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
25	Щ	Ь	Ы	Ъ	Э	Ю	Я	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
26	Ь	Ы	Ъ	Э	Ю	Я	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
27	Ы	Ъ	Э	Ю	Я	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	Ь
28	Ъ	Э	Ю	Я	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	Ь	Ы
29	Э	Ю	Я	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	Ь	Ы	Ъ
30	Ю	Я	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	Ь	Ы	Ъ	Э
31	Я	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	Ь	Ы	Ъ	Э	Ю

Рис. 4. Таблица Вижинера

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Таблица Вижинера для английского алфавита составляется аналогичным образом.

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово "АМБРОЗИЯ". Необходимо зашифровать сообщение "ПРИЛЕТАЮ СЕДЬМОГО".

Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера.

Сообщение	П	Р	И	Л	Е	Т	А	Ю	С	Е	Д	Ь	М	О	Г	О
Ключ	А	М	Б	Р	О	З	И	Я	А	М	Б	Р	О	З	И	Я
Шифртекст	П	Ъ	Й	Ы	У	Щ	И	Э	С	С	Е	К	Ь	Х	Л	Н

Шифр "двойной квадрат" Уитстона

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом". Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним на примере процедуру шифрования этим шифром. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами (рис. 5). Перед шифрованием исходное сообщение разбивают на биграммы. Каждая из них шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую - в правой. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

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

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

Рис. 5. Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат"

Предположим, что шифруется биграмма исходного текста "ИЛ". Буква И находится в столбце 1 и строке 2 левой таблицы, буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста 0В.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из той же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения; вторая буква берется из правой таблицы в столбце, со ответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение	П	Р		И	Л		Е	Т		А	Ю			Ш		Е	С		Т	О		Г	О
Шифртекст	П	Е		О	В		Щ	Н		Ф	М		Е	Ш		Р	Ф		Б	Ж		Д	Ц

Шифрование методом "двойного квадрата" дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее 30 строк.

Задание

1. Зашифровать текст при помощи таблицы Вижинера (см. рис. 4), используя ключевое слово.

2. Обменяться с партнером зашифрованными тестами и ключевыми словами. Расшифровать текст.

Номер варианта	Текст	Ключевое слово
1.	СТЕГАНОГРАФИЯ СЛУЖИТ ДЛЯ ПЕРЕДАЧИ СЕКРЕТОВ В ДРУГИХ СООБЩЕНИЯХ	АБОНЕНТ
2.	КАК ПРАВИЛО ОТПРАВИТЕЛЬ ПИШЕТ КАКОЕ-НИБУДЬ НЕПРИМЕТНОЕ СООБЩЕНИЕ	СИСТЕМА
3.	ПРИЕМЫ ВКЛЮЧАЮТ НЕВИДИМЫЕ ЧЕРНИЛА, МАЛОПРИМЕТНЫЕ ПОМЕТКИ У БУКВ	РЕШЕНИЕ
4.	В НАСТОЯЩЕЕ ВРЕМЯ ЛЮДИ НАЧАЛИ ПРЯТАТЬ СЕКРЕТЫ В ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЯХ	ТЕХНИКА
5.	В ПЕРЕСТАНОВОЧНОМ ШИФРЕ МЕНЯЕТСЯ НЕ ОТКРЫТЫЙ ТЕКСТ, А ПОРЯДОК СИМВОЛОВ	ПАРТНЕР
6.	КРИПТОГРАФИЯ РЕШАЕТ ПРОБЛЕМЫ СЕКРЕТНО-	ФИНАНСЫ

Номер варианта	Текст	Ключевое слово
	СТИ, ПРОВЕРКИ ПОДЛИННОСТИ, ЦЕЛОСТНОСТИ	
7.	ПРОТОКОЛ - ЭТО ПОРЯДОК ДЕЙСТВИЙ, ПРЕДПРИНИМАЕМЫХ ДВУМЯ ИЛИ БОЛЕЕ СТОРОНАМИ	АУКЦИОН
8.	ДЕЙСТВИЕ ДОЛЖНО ВЫПОЛНЯТЬСЯ В СВОЮ ОЧЕРЕДЬ И ПОСЛЕ ОКОНЧАНИЯ ПРЕДЫДУЩЕГО	УСЛОВИЕ
9.	КАЖДЫЙ УЧАСТНИК ПРОТОКОЛА ДОЛЖЕН СОГЛАСИТЬСЯ СЛЕДОВАТЬ ПРОТОКОЛУ	ДЕВУШКА
10.	КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ - ЭТО ПРОТОКОЛ, ИСПОЛЬЗУЮЩИЙ КРИПТОГРАФИЮ	ПРИНЦИП
11.	ПОНЯТИЕ ОДНОНАПРАВЛЕННОЙ ФУНКЦИИ ЯВЛЯЕТСЯ ЦЕНТРАЛЬНЫМ В КРИПТОГРАФИИ	ЭКСПЕРТ
12.	ЗНАЮЩИЙ КОМБИНАЦИЮ ЧЕЛОВЕК МОЖЕТ ОТКРЫТЬ СЕЙФ, ПОЛОЖИТЬ В НЕГО ДОКУМЕНТ	ПОЛИЦИЯ
13.	ВСКРЫТИЕ С ВЫБРАННЫМ ОТКРЫТЫМ ТЕКСТОМ МОЖЕТ БЫТЬ ОСОБЕННО ЭФФЕКТИВНЫМ	БУДУЩЕЕ
14.	ИЗ-ЗА НЕДОСТАТКОВ СИСТЕМЫ СИНХРОНИЗАЦИЯ ЧАСОВ МОЖЕТ БЫТЬ НАРУШЕНА	УГЛЕКОП
15.	ОБЫЧНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ ИСПОЛЬЗУЕТ ДВА КЛЮЧА	НАПИТОК
16.	ХАКЕР НЕ ПРЕНЕБРЕГАЕТ ОПЕРАТИВНО-ТЕХНИЧЕСКИМИ И АГЕНТУРНЫМИ МЕТОДАМИ	БОТИНОК
17.	ЕСЛИ ВНЕДРЕНИЕ ЗАКЛАДКИ ПРОХОДИТ УСПЕШНО, ВТОРАЯ АТАКА УЖЕ НЕ ТРЕБУЕТСЯ	ДЕРЗКИЙ
18.	ХАКЕР ЗАРАНЕЕ ПРОДУМЫВАЕТ ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ НЕУДАЧИ	СИМПТОМ
19.	ПРОГРАММНАЯ ЗАКЛАДКА, ВНЕДРЕННАЯ В СИСТЕМУ, ЗАМЕТНА ТОЛЬКО ХАКЕРУ	ЧЕМОДАН
20.	С ТОЧКИ ЗРЕНИЯ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМА РАБОТАЕТ КАК ОБЫЧНО	ЭСКУЛАП
21.	ЕСЛИ АТАКА НЕ УДАЛАСЬ, ХАКЕР СТАРАЕТСЯ ОСТАВИТЬ ЛОЖНЫЙ СЛЕД	ВПАДИНА

Библиографический список
1. Волобуев С.В. Безопасность социотехнических систем. Обнинск: “Викинг”, 2000. 340 с.
2. Романцев Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ Под ред. В.Ф. Шаньгина. М.: Радио и связь, 1999. 328 с.

СОДЕРЖАНИЕ

Игорь Николаевич Кузьмин,
доцент кафедры ИиУС АмГУ,
канд. техн. наук.

Защита информации и информационная безопасность: Учебно-методическое пособие

Изд-во АмГУ. Подписано к печати 04.09.02. Усл. печ. л. 2,79,
уч.-изд. л. 3. Тираж 100.Заказ 110