Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра проектирования информационно-компьютерных систем

МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

В двух частях

Часть 1

В. М. Алефиренко

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-39 03 01 «Электронные системы безопасности»

Минск БГУИР 2015

УДК 004.056(075.8)
ББК 32.973.26-018.2я73
М54

Р е ц е н з е н т ы:
кафедра информационных систем и технологий учреждения образования «Белорусский государственный технологический университет» (протокол №5 от 23.12.2014);

профессор кафедры радиоэлектроники учреждения образования «Минский государственный высший радиотехнический колледж», доктор технических наук, профессор Ф. Д. Троян

Методы и технические средства обеспечения безопасности. Лабораторный практикум : пособие. В 2 ч. Ч. 1 : Методы защиты информации / В. М. Алефиренко. – Минск : БГУИР, 2015. – 67 с. : ил.
М54
ISBN 978-985-543-142-9 (ч. 1).

Приводится описание четырех лабораторных работ. Первая работа посвящена изучению метода определения уровня качества технических средств защиты информации. Остальные три работы связаны с изучением методов защиты информации с помощью маскирующих сигналов, криптографии и стеганографии.
Предназначено для студентов всех форм обучения.

УДК 004.056(075.8)
ББК 32.973.26-018.2я73

ISBN 978-985-543-142-9 (ч. 1)
ISBN 978-985-543-141-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В соответствии с учебным планом специальности 1-39 03 01 «Электронные системы безопасности» дисциплина «Методы и технические средства обеспечения безопасности» (МиТСОБ) предусматривает 32 часа лабораторных работ, разбитых на две логические части, соответствующие двум семестрам, в которых изучается дисциплина.

Первая часть данного пособия посвящена изучению методов защиты информации. Вторая часть – изучению технических средств обеспечения безопасности информации и объектов.

Предлагаемый лабораторный практикум включает четыре лабораторные работы. Первая работа посвящена изучению метода определения уровня качества технических средств защиты информации. Вторая работа – изучению метода защиты речевой информации с помощью маскирующих сигналов различных видов. Третья работа связана с изучением криптографических методов защиты текстовой информации. Четвертая работа – с изучением методов компьютерной стеганографии, применяемых для скрытия текстовой информации в различных видах графических файлов.

Все лабораторные работы предусматривают проверку теоретических знаний студентов. Для этого студент должен ответить на определенное количество вопросов, после которых он допускается к выполнению работы. Для всех лабораторных работ разработано оригинальное программное обеспечение, позволяющее проводить индивидуальную проверку теоретических знаний студента, самостоятельно выполнять лабораторную работу и проверять правильность ее выполнения.

Расчетно-аналитический метод определения уровня качества технических средств защиты информации с помощью комплексных показателей, рассмотренный в лабораторной работе №1, может использоваться в дальнейшем при проведении практических занятий для выбора конкретного состава технических средств систем обеспечения безопасности, а также при выполнении дипломных проектов по тематике, связанной с разработкой систем обеспечения безопасности. Этот же метод, а также криптографические методы защиты текстовой информации, рассмотренные в лабораторной работе №3, могут использоваться при формировании заданий по контрольным работам для студентов заочного обучения.

Изучение материала лабораторного практикума и его использование при проведении лабораторных и практических занятий, а также при выполнении контрольных работ позволит студентам закрепить знания и получить навыки по использованию методов, применяемых для защиты различных видов информации.

Автор выражает благодарность Е. Н. Шнейдерову за практическую реализацию идеи дизайна обложки пособия.

Лабораторная работа №1

Определение уровня качества технических средств защиты информации

1.1. Цель работы

Изучение методов определения показателей качества технических средств защиты информации и практическое определение их уровня качества с использованием комплексных показателей.

1.2. Теоретические сведения

1.2.1. Основные понятия, термины и определения теории качества

Технические средства защиты информации (ТСЗИ) в большинстве случаев представляют собой радиоэлектронные устройства (РЭУ), предназначенные для обнаружения и подавления прослушивающих устройств, шифрования и кодирования информации, защиты информации в возможных каналах утечки. К ним относятся индикаторы и анализаторы различных полей, широкополосные приемники, генераторы виброакустических и радиошумов, скремблеры (телефонные кодирующие устройства), блокираторы сотовых телефонов, обнаружители скрытых видеокамер и другие подобные устройства.

Многообразие подобных РЭУ даже одного назначения, имеющих к тому же различные технические характеристики, затрудняет их правильный выбор для оптимального и эффективного решения поставленной задачи по защите информации.

Поэтому знание методов определения уровня качества выпускаемой продукции и умение использовать их на практике является важной задачей как для производителя, так и для потребителя продукции.

Рассмотрим основные понятия и определения теории качества продукции, к которой относятся РЭУ, и в частности ТСЗИ.

Качество продукции – совокупность свойств продукции, обусловливающих ее пригодность удовлетворять определенные потребности в соответствии с ее назначением [1].

Продукция – материализованный результат процесса трудовой деятельности, обладающий полезными свойствами, полученный в определенном месте за определенный интервал времени и предназначенный для использования потребителями в целях удовлетворения их потребностей как общественного, так и личного характера.

Единица продукции – отдельный экземпляр штучной продукции или определенное в установленном порядке количество нештучной или штучной продукции (партия изделий, определенная емкость или объем).

Единицы продукции служат не только для исчисления ее количества. Деление продукции на определенные единицы имеет существенное значение при управлении качеством продукции и, в частности, при оценке ее качества при контроле каждой единицы (сплошной контроль) или некоторых единиц (выборочный контроль).

Изделие – единица промышленной продукции, количество которой может исчисляться в штуках или экземплярах.

Любое РЭУ является частным случаем единицы промышленной продукции. Количество изделий может быть охарактеризовано дискретной величиной, исчисляемой в штуках или экземплярах. Однако в некоторых случаях количество определенных изделий (например крепежных деталей) может характеризоваться непрерывной величиной, применяемой для нештучной продукции, и исчисляться, в частности, в единицах массы. Видами изделий, представляющими объекты конструкторской документации, являются детали, сборочные единицы, комплексы и комплекты.

Свойство продукции – объективная особенность продукции, которая может проявляться при ее создании, эксплуатации или потреблении.

Любая продукция, в том числе и РЭУ, имеет множество различных свойств, которые могут проявляться при разработке, производстве, испытаниях, хранении, транспортировании, техническом обслуживании, ремонте и использовании. Свойства продукции можно разделить на простые и сложные. Примером сложного свойства является надежность изделия, обусловленная такими относительно простыми его свойствами, как безотказность, долговечность, ремонтопригодность и сохраняемость. Деление свойств продукции на технические, экономические и т. п. является неправомерным (неоднозначным), так как одно и то же свойство продукции может быть для различных целей (в разных случаях) охарактеризовано техническим или экономическим показателем. Например, свойство ремонтопригодности можно охарактеризовать как вероятностью выполнения ремонта в заданное время (технический показатель), так и средней стоимостью ремонта (экономический показатель).

Признак продукции – качественная или количественная характеристика любых свойств или состояний продукции.

К качественным признакам, например, относятся цвет материала, форма изделия, вид покрытия детали (защитное, декоративное), способ настройки или регулировки технического устройства (ручной, автоматический). Среди качественных признаков при определении качества продукции большое значение имеют альтернативные признаки, которые могут иметь только два взаимоисключающих варианта, например, наличие или отсутствие дефектов в изделии, возникновение или отсутствие отказа при испытаниях.

Количественный признак продукции является ее параметром.

Параметр продукции – признак продукции, количественно характеризующий любые ее свойства или состояния, в том числе и входящие в состав качества продукции. Следовательно, показатель качества может быть частным случаем параметра продукции.

Многие показатели качества продукции являются функциями ее параметров. Качественный признак продукции может влиять на вид функциональной зависимости показателей качества продукции от ее параметров. Например, способ резервирования (качественный признак) оказывает существенное влияние на вид зависимости показателя безотказности резервирования (структурный параметр).

Связь понятий «признак», «параметр» и «показатель качества продукции» показана на рис. 1.1.

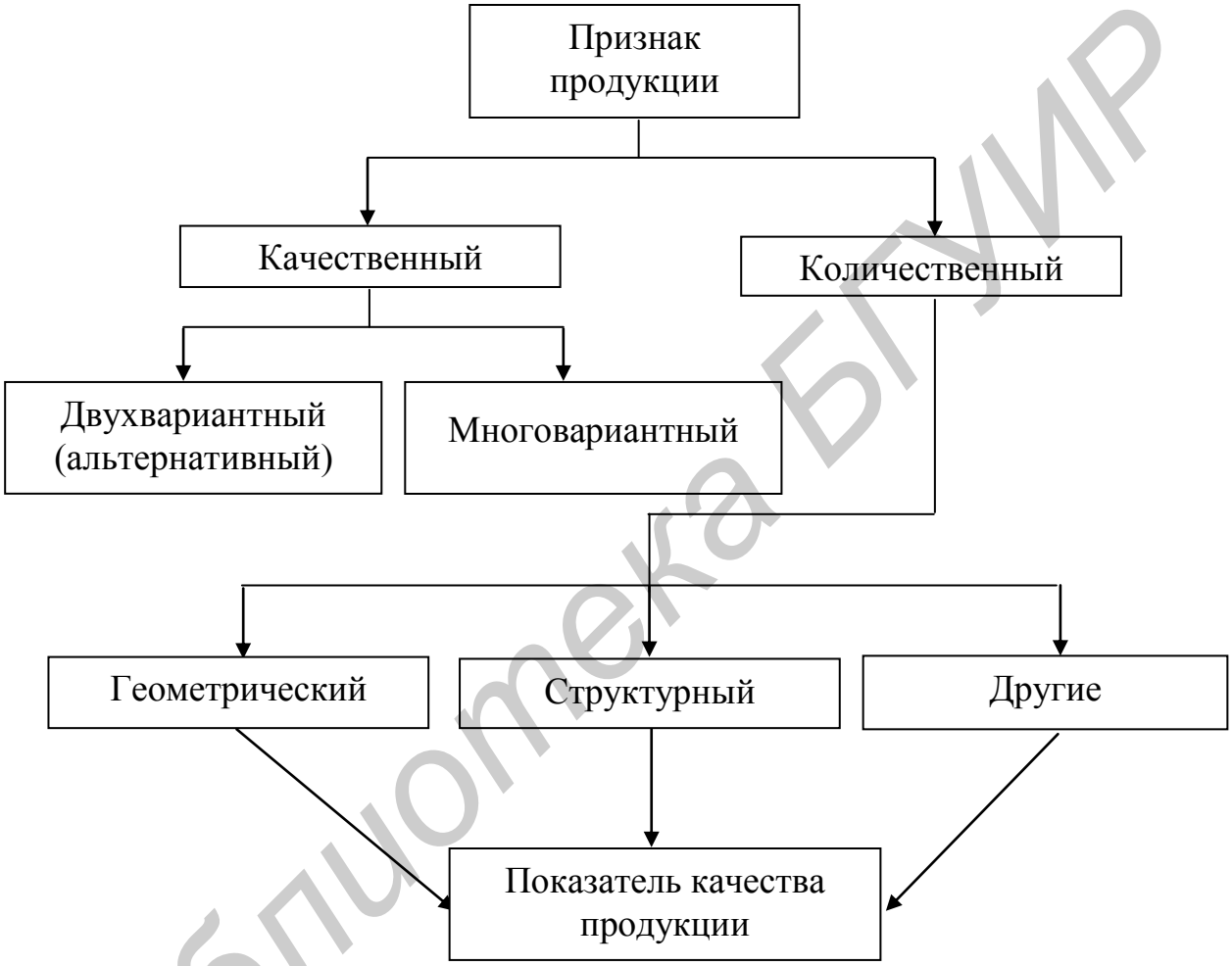

Рис. 1.1. Связь понятий «признак», «параметр» и «показатель качества продукции»

Геометрические параметры продукции обеспечиваются, как правило, конструктивно, а структурные – конструктивно и технологически.

Следует отметить, что иногда бывает сложно установить наличие и вид связи между некоторыми параметрами продукции и показателями ее качества. Например, параметр, характеризующий проницаемость корпуса РЭУ для радиоактивных излучений, устанавливаемого на автомобиле, обычно не принимается в расчет при оценке качества РЭУ. Однако, если автомобиль предназначен

для пересечения местности, зараженной радиоактивными веществами, то указанный параметр следует считать одним из важнейших показателей качества РЭУ.

1.2.2. Единичные показатели качества РЭУ

Для оценки качества РЭУ используются показатели качества, под которыми понимают количественные характеристики одного или нескольких свойств РЭУ, рассматриваемые применительно к определенным условиям его создания и эксплуатации.

Качество РЭУ является многогранным свойством. Для описания различных сторон этого свойства используются единичные показатели качества [1, 2].

Основными единичными показателями качества РЭУ являются следующие.

Входные параметры:
- входное напряжение;
- входное сопротивление;
- диапазон принимаемых частот;
- число принимаемых каналов;
- чувствительность.

Выходные параметры:
- выходное напряжение;
- выходное сопротивление;
- излучаемая мощность;
- диапазон передаваемых частот;
- полоса воспроизводимых частот.

Внутренние параметры:
- объем памяти;
- быстродействие;
- тактовая частота;
- промежуточная частота преобразования;
- время преобразования;
- время задержки.

Параметры энергопотребления:
- напряжение питания;
- частота питающего напряжения;
- ток потребления;
- мощность потребления.

Массогабаритные параметры:
- масса;
- размеры;
- объем;
- занимаемая площадь.

К единичным показателям качества РЭУ могут быть отнесены параметры надежности, технологичности, стоимости и т. п., которые не включают в себя другие параметры.

Многие единичные показатели находятся в противоречивой связи, т. е. улучшение одного показателя ухудшает другой. Например, возрастание надежности РЭУ влечет за собой повышение ее стоимости. Кроме того, большинство показателей выражается разными параметрами и значениями этих параметров. Все это затрудняет объективную оценку качества как существующих, так и вновь разрабатываемых РЭУ.

О качестве РЭУ можно судить не только по абсолютным, но и по относительным показателям. Например, вновь разрабатываемое РЭУ сравнивают с существующим прототипом или с образцом, принятым за эталон. При этом используют метод экспертных оценок и показатели выражают в баллах.

Однако такая оценка даже при высокой квалификации экспертов носит субъективный характер и не может быть абсолютной.

Для преодоления указанных трудностей используют комплексные показатели качества.

1.2.3. Комплексные показатели качества РЭУ

Комплексные показатели качества, в отличие от единичных, характеризуют несколько свойств РЭУ и учитывают единичные показатели [1, 2].

Простым примером комплексного показателя является коэффициент готовности $K_{\Г}$, который вычисляется по формуле

$$K_{\Г} = \frac{T_{\Н}}{T_{\Н} + T_{\В}}, \qquad (1.1)$$

где $T_{\Н}$ – наработка на отказ (показатель безотказности);

$T_{\В}$ – среднее время восстановления (показатель ремонтопригодности).

Как видно из формулы (1.1), коэффициент готовности характеризует два свойства РЭУ – безотказность и ремонтопригодность.

Другим примером комплексного показателя качества является средневзвешенный показатель $K_{\К}$, который вычисляется по формулам, приведенным ниже:

– средневзвешенный арифметический:

$$K_{\К} = \sum_{i=1}^{m} \alpha_{\Н i} K_{\Н i}; \qquad (1.2)$$

– средневзвешенный геометрический:

$$K_{\text{К}} = m\sqrt{\prod_{i=1}^{m} K_{\text{Н}i}^{\alpha_{\text{Н}i}}}; \qquad (1.3)$$

– средневзвешенный гармонический:

$$K_{\text{К}} = \frac{\sum_{i=1}^{m} \alpha_{\text{Н}i}}{\sum_{i=1}^{m} \frac{\alpha_{\text{Н}i}}{K_{\text{Н}i}}}, \qquad (1.4)$$

где $\alpha_{\text{Н}i}$ – нормированный коэффициент, характеризующий вес (значимость, важность) i-го единичного показателя;

$K_{\text{Н}i}$ – нормированный i-й единичный показатель;

m – количество единичных показателей, принятых во внимание.

Как видно из формул (1.2)–(1.4), средневзвешенный показатель характеризует m различных свойств РЭУ.

Комплексный показатель $K_{\text{Г}}$ имеет определенное физическое содержание, а именно вероятность того, что оцениваемое РЭУ окажется работоспособным (готовым к выполнению заданных функций) в любой произвольно выбранный момент времени в промежутках между периодами планового технического обслуживания.

Комплексный средневзвешенный показатель $K_{\text{К}}$ представляет собой условную величину, выражаемую в условных единицах (в баллах, в относительных единицах), и реального физического содержания не имеет.

Деление показателей качества на единичные и комплексные является условным из-за условности деления свойств изделия на простые и сложные. Так, например, свойство ремонтопригодности по отношению к свойству готовности или к еще более сложному свойству надежности, является простым. Однако его простота является не абсолютной, а относительной, так как сам показатель ремонтопригодности $T_{\text{В}}$ вычисляется в свою очередь по формуле

$$T_{\text{В}} = T_{\text{О}} + T_{\text{У}}, \qquad (1.5)$$

где $T_{\text{О}}$ – среднее время, затрачиваемое на отыскание отказа;

$T_{\text{У}}$ – среднее время, необходимое для устранения отказа.

Как видно из формулы (1.5), ремонтопригодность является сложным свойством РЭУ по отношению к таким более простым ее свойствам, как приспособленность к отысканию отказов и приспособленность к их устранению.

Следовательно, показатель $T_В$ относительно $K_Г$ можно рассматривать как единичный, а относительно $T_О$ и $T_У$ – как комплексный.

В инженерной практике в качестве комплексного показателя качества наиболее часто используются выражения (1.2) и (1.3).

Весовые коэффициенты (коэффициенты значимости) α_i зависят от функционального назначения РЭУ и устанавливаются обычно с позиции заказчика (потребителя) с использованием, например, метода экспертных оценок. При определении коэффициентов значимости экспертным методом обычно применяют методы ранжирования, последовательного сравнения, парного сравнения, расстановки приоритетов и балльный метод.

Метод расстановки приоритетов является модифицированным методом парного сравнения и не требует условия транзитивности (если *а* лучше *в*, а *в* лучше *с*, то и *а* лучше *с*). Поэтому результат парного сравнения этим методом наиболее точно отражает субъективное предпочтение, так как в этом случае на выбор налагаются минимальные ограничения и эксперту не навязываются априорные условия. Кроме того, при отсутствии требований транзитивности эксперт производит сопоставление параметров (показателей) объектов независимо от результатов других сопоставлений и одна допущенная ошибка не столь значительно влияет на результаты расчета значений приоритетов (коэффициентов значимости). Одним из основных недостатков метода парного сравнения является его малая применимость при увеличении числа сравниваемых объектов из-за непропорционально быстрого роста числа единичных парных сравнений.

Коэффициенты значимости α_{Hi} для выражений (1.2) и (1.3) должны выбираться таким образом, чтобы обеспечивалось соответственно одно из условий:

$$\sum_{i=1}^{m} \alpha_{Hi} = 1; \tag{1.6}$$

$$\prod_{i=1}^{m} \alpha_{Hi} = 1. \tag{1.7}$$

То есть нормированные коэффициенты значимости α_{Hi} должны лежать в пределах $0 < \alpha_{Hi} < 1$.

Для получения нормированных (безразмерных) значений единичных показателей K_{Hi} могут использоваться следующие выражения:

$$K_{Hi} = \frac{K_i - K_{кр\,i}}{K_{opt\,i} - K_{кр\,i}}; \tag{1.8}$$

$$K_{Hi} = \frac{K_i}{K_{max\ i}}; \tag{1.9}$$

$$K_{\text{Н}i} = \frac{K_{\min\ i}}{K_i}, \qquad (1.10)$$

где K_i – исходное значение i-го единичного показателя;

$K_{\text{кр}\,i}$ – критическое значение i-го единичного показателя;

$K_{\text{opt}\,i}$ – оптимальное значение i-го показателя;

$K_{\max\,i}$ – максимальное значение i-го показателя;

$K_{\min\,i}$ – минимальное значение i-го показателя.

Если исходные значения K_i лежат в пределах $K_{\text{кр}\,i} < K_i < K_{\text{opt}\,i}$ или $K_{\text{opt}\,i} < K_i < K_{\text{кр}\,i}$, то нормированные значения $K_{\text{Н}i}$ будут лежать в пределах $0 < K_{\text{Н}i} < 1$.

Для определения комплексных показателей качества различных РЭУ (ТСЗИ) в лабораторной работе используются выражения (1.2), (1.3), (1.6), (1.7), (1.8).

1.2.4. Интегральный показатель качества РЭУ

Интегральный показатель качества представляет собой отношение суммарного полезного эффекта от эксплуатации РЭУ к суммарным затратам на его создание и эксплуатацию [1, 2]:

$$K_{\text{И}} = \frac{Q_\Sigma}{Z_\Sigma}, \qquad (1.11)$$

где Q_Σ – полная целевая отдача РЭУ данного типа за период эксплуатации (суммарный полезный эффект от эксплуатации РЭУ);

$Z_\Sigma = Z_{\text{С}} + Z_{\text{Э}}$ – суммарные затраты (издержки) на достижение полной целевой отдачи;

$Z_{\text{С}}$ – суммарные затраты на создание РЭУ;

$Z_{\text{Э}}$ – суммарные затраты на эксплуатацию РЭУ.

Формула (1.11) справедлива для РЭУ, срок службы которого не превышает одного года. В этом случае единовременные и текущие затраты просто суммируются.

Для РЭУ, срок службы которого превышает один год, единовременные затраты $Z_{\text{С}}$ должны быть приведены к последнему году срока службы РЭУ с использованием нормативного коэффициента, учитывающего самоокупаемость РЭУ.

Важное значение для оценки качества РЭУ имеет распределение полной целевой отдачи и суммарных затрат во времени (рис. 1.2).

Полная целевая отдача Q_Σ зависит от многих технических и организационных факторов: форм и методов организации эксплуатации РЭУ, условий его эксплуатации, квалификации обслуживающего персонала и др.

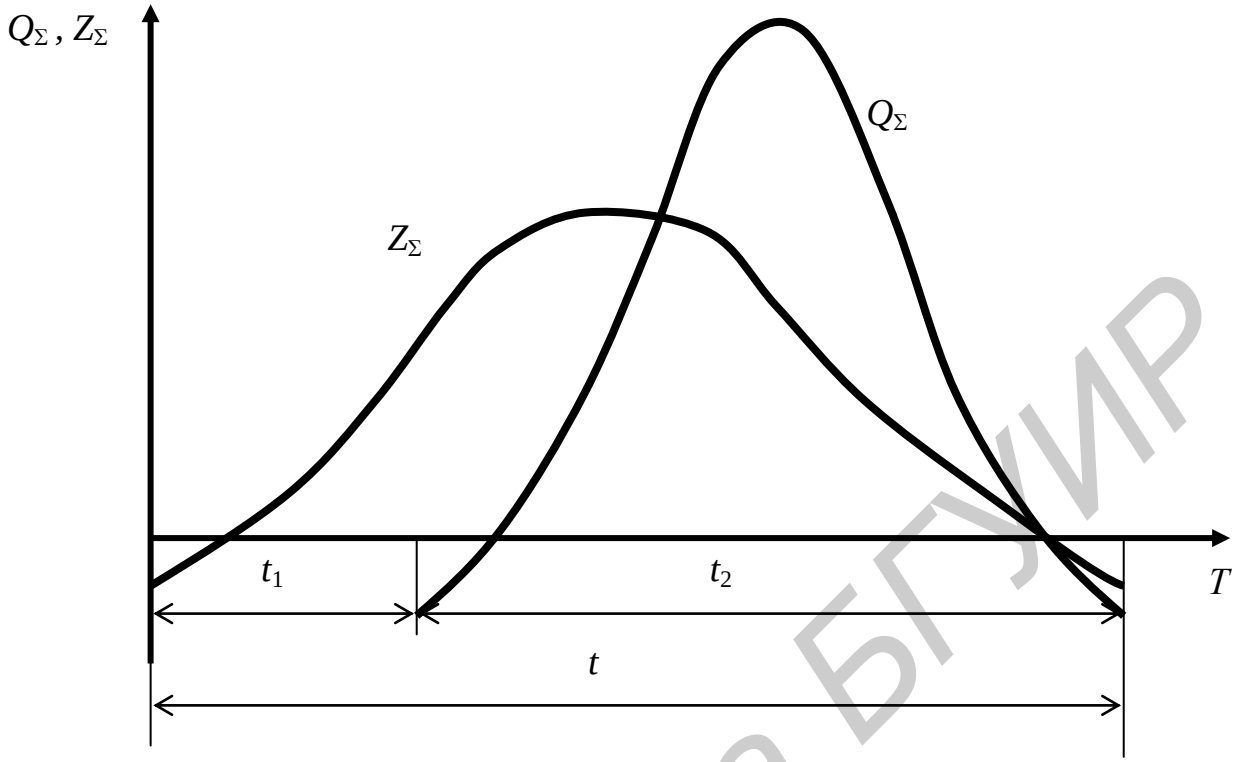

Рис. 1.2. Распределение полной целевой отдачи Q_Σ и суммарных затрат Z_Σ во времени (t_1 – время проектирования, изготовления и подготовки к использованию РЭУ; t_2 – время достижения полной целевой отдачи; t – период времени расходования средств)

Суммарные затраты на достижение полной целевой отдачи Z_Σ зависят от технического уровня предприятия, форм и методов организации производства, профессиональной подготовки кадров, технологичности конструкции РЭУ и др.

От правильного построения математических моделей (выражений) для величин Q_Σ и Z_Σ зависит правильность интегральной оценки качества РЭУ. На практике обычно не только сложно получить модели для расчета Q_Σ и Z_Σ, но иногда неясно, через какие параметры выражать полную целевую отдачу.

В реальных условиях не менее сложно подсчитать и суммарные затраты. Тем не менее общность применения интегрального показателя к различным видам РЭУ облегчает определение их уровня качества.

Наряду с интегральным показателем качества может использоваться величина, обратная ему и называемая удельными затратами на единицу эффекта.

1.2.5. Методы определения показателей качества РЭУ

Существуют следующие методы определения качества РЭУ [1]:

– измерительный;

– регистрационный;
– расчетный;
– органолептический;
– экспертный;
– социологический.

Измерительный метод осуществляется на основе технических средств измерений и базируется на информации, получаемой с использованием этих средств. С помощью измерительного метода определяют значения таких показателей качества РЭУ, как ток потребления, входное сопротивление, сопротивление изоляции, масса (вес) и т. п.

Регистрационный метод осуществляется на основе наблюдения и подсчета числа определенных событий, предметов или затрат. Он базируется на информации, получаемой путем регистрации и подсчета числа определенных событий, например, числа отказов РЭУ или его компонентов при проведении испытаний, подсчета числа дефектных изделий в партии и т. п.

Расчетный метод осуществляется на основе использования теоретических и (или) эмпирических зависимостей показателей качества продукции от ее параметров. Он применяется в основном на стадии проектирования РЭУ, когда оно не может быть объектом экспериментального исследования. Этим же методом могут быть установлены и зависимости между отдельными показателями качества РЭУ. Расчетный метод используется для определения массы (веса), показателей надежности, потребляемой мощности РЭУ и т. п.

Органолептический метод осуществляется на основе анализа восприятий органов чувств человека, которые выдают информацию о получении соответствующих ощущений. Значения показателей качества находят путем анализа полученных ощущений на основе имеющегося опыта. Поэтому точность и достоверность полученной информации зависит от квалификации, навыков и способностей лиц, которые ее определяют. Органолептический метод не исключает возможности использования технических средств (лупа, микроскоп, микрофон и т. п.), повышающих восприимчивость и разрешающие способности органов чувств человека. Этот метод широко применяется для определения качества продукции, использование которой обусловлено или связано с эмоциональным воздействием на потребителей (напитки, кондитерские, табачные, парфюмерные изделия). Однако он может использоваться и для определения качества РЭУ, например такого показателя, как художественное оформление (дизайн РЭУ). Показатели качества, определяемые органолептическим методом, выражаются обычно в баллах (относительных единицах).

Экспертный метод осуществляется на основе решения, принимаемого экспертами, которые дают оценку качественным показателям продукции в баллах (относительных единицах). Экспертный метод используется и для определения коэффициентов весомости показателей качества продукции.

Социологический метод осуществляется на основе сбора и анализа мнений фактических или возможных потребителей продукции. Сбор таких мнений может осуществляться устным способом (непосредственно или с помощью те-

лефона), с помощью распространения анкет-вопросников, путем проведения конференций, совещаний, выставок и т. п. Социологический метод иногда может применяться и для определения коэффициентов значимости показателей качества продукции.

1.2.6. Методы определения качества РЭУ

Для определения качества РЭУ на практике широко используются *дифференциальный*, *комплексный*, *смешанный* и *статистический методы*.

Дифференциальный метод основан на использовании единичных показателей качества РЭУ.

Комплексный метод основан на использовании комплексных показателей качества РЭУ.

Смешанный метод основан на одновременном использовании единичных и комплексных показателей качества РЭУ.

Статистический метод основан на правилах математической статистики.

При решении практических задач по определению качества РЭУ обычно прибегают к сочетанию рассмотренных методов.

1.2.7. Применение экспертных методов для определения качества РЭУ

Экспертные методы (методы экспертных оценок) используются в тех случаях, когда единичные показатели не могут быть явно выражены количественными мерами, например художественное оформление (дизайн) или удобство в техническом обслуживании. Для учета подобных единичных показателей используются методы экспертных оценок. В этих методах единичному показателю дает независимую оценку (например в баллах) группа специалистов-экспертов. Результирующую окончательную оценку обычно получают путем усреднения. В простейшем случае подсчитывают среднее арифметическое значение по формуле

$$k = \frac{\sum_{j=1}^{n} k_j}{n}, \qquad (1.12)$$

где k_j – численное значение оценки, сделанное j-м экспертом;

n – число экспертов, участвующих в процедуре экспертной оценки единичного показателя качества.

Лучшие результаты дает усреднение с учетом весовых коэффициентов, учитывающих значимость мнения (опыт, квалификацию, авторитет и т. п.) j-го эксперта. В этом случае используют формулу

$$k = \frac{\sum_{j=1}^{n} \alpha_j k_j}{\sum_{j=1}^{n} \alpha_j}, \qquad (1.13)$$

где α_j – весовой коэффициент j-го эксперта.

При использовании метода экспертных оценок для определения качества РЭУ важным этапом является правильный выбор экспертов. Принципы отбора потенциальных экспертов основываются на анализе следующих характеристик:

– стаж работы в той области исследований, к которой принадлежит оцениваемое РЭУ;
– научная степень и звание;
– количество публикаций в соответствующей области;
– наличие изобретений в соответствующей области и т. д.

При формировании экспертной группы отбор экспертов проводится на основе качественной и количественной оценки.

При качественной оценке анализируется степень соответствия экспертов предлагаемым требованиям (компетентность, уверенность, объективность, деловитость, заинтересованность).

При количественной оценке проводится количественная оценка качества экспертов. Наиболее важным свойством, характеризующим качество эксперта, является свойство «компетентность». Поэтому при количественной оценке чаще всего учитывается только это свойство. Количественная оценка может определяться на основе упрощенной комбинированной оценки, зависящей от самооценки и взаимооценки, по формуле

$$K_{\text{Э}} = 0{,}4K_{\text{С}} + 0{,}6K_{\text{В}}, \qquad (1.14)$$

где $K_{\text{С}}$ – самооценка компетентности;

$K_{\text{В}}$ – взаимная оценка компетентности экспертной группы.

Оценивая величину $K_{\text{С}}$, эксперт оценивает свою информированность и степень знакомства с различными аспектами оцениваемой РЭУ. Значение самооценки $K_{\text{С}}$ определяется по формуле

$$K_{\text{С}} = \sum_{i=1}^{p} \beta_i K_{\text{С}i}, \qquad (1.15)$$

где β_i – весомость (значимость) показателей информированности и степени знакомства;

$K_{\text{С}i}$ – значение самооценки по информированности и степени знакомства с i-м показателем;

p – число показателей, по которым проводится расчет самооценки.

Значения β_i и K_{Ci} определяются таким образом, чтобы $\sum_{i=1}^{p} \beta_i = 1$, а $0 \le K_{Ci} \le 10$. Отсюда $0 \le K_C \le 10$.

Взаимооценку K_B члены экспертной группы дают друг другу по профессиональной компетентности, например, по пятибалльной системе. Значение оценки компетентности каждого эксперта определяется как среднее из значений оценок, назначенных всеми остальными экспертами. Взаимооценка менее субъективна, чем самооценка, но имеет специфический недостаток, состоящий в том, что члены экспертной группы могут слабо знать друг друга.

В результате проведенного отбора на основе качественной и количественной оценки в состав экспертной группы включается необходимое количество наиболее квалифицированных экспертов.

1.3. Порядок выполнения работы

1. Изучить теоретическую часть работы.
2. Провести самопроверку теоретических знаний, ответив на поставленные вопросы.
3. Получить вариант задания и ознакомиться с параметрами ТСЗИ, используемыми для определения его качества.
4. Заполнить таблицу недостающими исходными данными (значениями коэффициента значимости) с соответствующим устным или письменным обоснованием принятых значений.
5. Привести к одной величине значения единичных показателей, выраженных несколькими величинами (габаритные размеры, диапазон частот и т. п.).
6. Скорректировать значения единичных показателей, отмеченные звездочками, с соответствующим устным или письменным обоснованием принятых значений.
7. Провести нормировку коэффициентов значимости таким образом, чтобы выполнялись условия (1.6) и (1.7).
8. Провести нормировку единичных показателей, используя выражение (1.8).
9. Провести расчет комплексных показателей качества для предложенного варианта ТСЗИ, используя выражения (1.2) и (1.3).
10. Определить по полученным значениям комплексных показателей вариант ТСЗИ, имеющий наивысший уровень качества.
11. Оформить отчет и защитить работу.

1.4. Описание программы для ЭВМ

Программа позволяет проверять теоретические знания студентов, выдавать варианты заданий индивидуально для каждого студента или группы сту-

дентов, проверять правильность корректировки исходных данных, правильность текущих расчетов и окончательного результата. Имя программы LEVEL.

1.5. Содержание отчета

1. Цель лабораторной работы.
2. Номер варианта задания.
3. Таблица исходных данных в соответствии с заданным вариантом.
4. Таблица скорректированных исходных данных и подробные пояснения полученных значений.
5. Таблица нормированных данных и подробный пример корректировки коэффициентов значимости и единичных показателей для одного прибора.
6. Таблица с результатами расчетов комплексных показателей качества и подробный пример расчета для одного прибора.
7. Выводы по работе.

Литература

1. ГОСТ 15467–79. Управление качеством продукции. Основные понятия, термины и определения. – М. : Изд-во стандартов, 1979. – 26 с.
2. Боровиков, С. М. Теоретические основы конструирования, технологии и надежности / С. М. Боровиков. – Минск : Дизайн ПРО, 1988. – 336 с.

Лабораторная работа №2

Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов

2.1. Цель работы

Изучение метода определения разборчивости речи с помощью артикуляционных измерений и практическое использование его для исследования защиты речевой информации маскирующими сигналами различных видов.

2.2. Теоретические сведения

2.2.1. Параметры и характеристики звукового поля

2.2.1.1. Звуковые волны

Звуковой волной называется процесс распространения деформаций сжатия или растяжения в сплошной среде, происходящий с конечной скоростью [1, 2].

Звуковая волна может возникать и распространяться только в такой среде, которая обладает определенной *упругостью* (сжимаемостью) и *инерционностью* (плотностью). Сплошная среда, обладающая только этими двумя физическими свойствами, называется *идеальной*. В отличие от нее *реальная среда* характеризуется еще и *диссипативными свойствами*, приводящими к потере энергии волнового движения.

Звуковой луч – это направление распространения звуковых волн. А поверхность, включающая смежные точки звукового поля с одинаковыми фазами колебания, называется *фронтом волны.*

Звуковое поле – это пространство, в котором происходит распространение звуковых колебаний. Звуковые колебания среды обычно возбуждаются за счет колебаний различных механических устройств или голоса. Звуковые колебания в жидкой и газообразной среде (воздухе) представляют собой продольные колебания, так как частицы среды колеблются вдоль линии распространения звука. Вследствие этого образуются сгущения и разряжения среды, двигающейся от источника колебаний с определенной скоростью, называемой *скоростью звука*.

2.2.1.2. Скорость звука

Скорость звука является постоянной величиной для данной среды и метеорологических условий и определяется по формуле

$$c = \sqrt{\frac{\gamma \cdot P_{\text{ст}}}{\rho}}, \qquad (2.1)$$

где γ – показатель адиабаты для воздуха (отношение удельных теплоемкостей воздуха при постоянном давлении и постоянном объеме, γ = 1,41);

$P_{\text{СТ}}$ – статическое давление среды ($P_{\text{СТ}}$ = 101325 Па при давлении 760 мм рт. ст.);

ρ – плотность среды (для воздуха при 20 °С и нормальном давлении ρ = 1,22 кг/м^3).

Скорость звука в воздухе при нормальных условиях равна 330 м/с. Для сравнения: скорость звука в воде равна 1500 м/с, а в стали – 6000 м/с. Связь между скоростью звука, длиной волны и частотой (периодом) колебаний определяется соотношением

$$c = \lambda \cdot f = \frac{\lambda}{T}, \qquad (2.2)$$

где λ – длина волны;

f – частота колебаний;

T – период колебаний.

Следует отметить, что данное соотношение справедливо для *плоской* и *сферической формы* фронта звуковой волны.

2.2.1.3. Звуковое давление и интенсивность звука

Звуковое давление. Если считать, что давление среды в отсутствие звуковых колебаний равно $P_{\text{ст}}$ (статическое давление), то при распространении звуковой волны в любой точке звукового поля полное давление будет изменяться, увеличиваясь при прохождении сжатий и уменьшаясь при следовании разряжений. Разность между мгновенным значением полного давления $P_{\text{м}}$ и статическим давлением среды $P_{\text{ст}}$ называется *звуковым давлением*:

$$p = P_{\text{м}} - P_{\text{ст}}.$$

Звуковое давление является знакопеременной величиной и определяется как сила, действующая на единицу площади. Звуковое давление измеряется в паскалях (1 Па = 1 Н/м^2).

Интенсивность звука. Интенсивностью звука называется количество звуковой энергии, проходящей в единицу времени через единицу площади, перпендикулярной к направлению распространения звуковой волны. Интенсивность звука измеряется в ваттах на метр квадратный и связана с действующим значением звукового давления соотношением

$$I = \frac{p^2}{\rho \cdot c}, \qquad (2.3)$$

где $\rho \cdot c$ – удельное акустическое сопротивление среды (для воздуха при нормальных атмосферных условиях $\rho \cdot c$ = 412 кг/м^{2}с).

Среднее количество звуковой энергии, приходящейся на единицу объема, называется *плотностью энергии* и измеряется в джоулях на метр кубический.

Уровни интенсивности звука и звукового давления. Вследствие логарифмического закона восприятия звуковых колебаний (частот) слуховым анализатором (ухом) человека и широкого диапазона интенсивностей слышимых звуков для объективной оценки введено понятие уровня интенсивности:

$$L_I = 10 \cdot \lg(I / I_0), \qquad (2.4)$$

где I – интенсивность исходного звука;

I_0 – нулевой (пороговый) уровень интенсивности звука ($I_0 = 10^{-12}$ Вт/м^2).

В соответствии с квадратичной зависимостью между интенсивностью звука и звуковым давлением (2.3) уровень звукового давления определяется как

$$L_p = 20 \cdot \lg(p / p_0), \qquad (2.5)$$

где p – звуковое давление исходного звука;

p_0 – нулевой (пороговый) уровень звукового давления ($p_0 = 2 \cdot 10^{-5}$ Па).

За пороговый уровень интенсивности звука (звукового давления) принимают уровень звука на частоте 100 Гц, который воспринимается человеком с вероятностью 0,5. Уровни интенсивности звука и звукового давления являются относительными величинами и измеряются в децибелах.

Вычисление уровня интенсивности или звукового давления сложного звука следует производить, суммируя интенсивности (давления) компонент:

$$L_{I\Sigma} = 10\lg(\sum_{i=1}^{n} I_i / I_0);$$

$$L_{p\Sigma} = 20\lg(\sum_{i=1}^{n} p_i / p_0). \qquad (2.6)$$

Если известны уровни звуковых давлений в децибелах нескольких источников звука, то определение общего уровня осуществляется путем внесения соответствующей поправки, определяемой или путем вычисления, или на основе номограммы. Так, например, если L_{p1} = 85 дБ, L_{p2} = 82 дБ, то вначале опреде-

ляется разность $L_{p1} - L_{p2} = 3$ дБ, а затем по номограмме с учетом этой разности определяется соответствующая поправка, которая составляет 1,7 дБ. Тогда общий уровень $L_{p\Sigma}$ = 85 + 1,7 = 86,7 дБ.

2.2.2. Характеристики и свойства слухового анализатора человека

Слуховой анализатор человека состоит из уха, слухового нерва, сложной системы нервных связей и центров мозга. В аппарат, обозначенный термином «ухо», входит наружное (звукоулавливающий аппарат), среднее (звукопередающий аппарат) и внутреннее (звуковоспринимающий аппарат) ухо. Наружное ухо воспринимает определенные частоты звуков благодаря функциональной способности волокон его мембраны к резонансу. Физиологическое значение наружного и среднего уха заключается в проведении и усилении звуков.

Слуховой анализатор человека улавливает форму волны, частотный спектр чистых тонов и шумов, осуществляет анализ и синтез в определенных пределах частотных компонент звуковых раздражений, обнаруживает и опознает звуки в большом диапазоне интенсивностей и частот. Слуховой анализатор позволяет дифференцировать звуковые раздражения и определять направление звука, а также удаленность его от источника.

Слуховой анализатор человека воспринимает как слышимый звук колебания в диапазоне 20 Гц–20 кГц, что соответствует диапазону длин волн в воздухе 17–17 мм. Ухо наиболее чувствительно к колебаниям в области средних частот 1–4 кГц. Звуки частот ниже 20 Гц называются *инфразвуками*, а выше 20 кГц – *ультразвуками*. Инфразвуки и ультразвуки могут также оказывать воздействие на организм, но оно не сопровождается слуховым ощущением. Минимальное звуковое давление, обнаруживаемое нормальным слухом, составляет 20 мкПа, или $2 \cdot 10^{-5}$ Па, что соответствует уровню звукового давления 0 дБ. Максимальный уровень звукового давления, воспринимаемого ухом, составляет 120 дБ, или в 10^6 раз больше, чем минимальное давление. Вот почему удобно использовать логарифмическую шкалу звуковых колебаний, которая позволяет сжать диапазон $1–10^6$ до диапазона шириной 0–120 дБ.

Для справки можно привести уровни звуковых давлений в децибелах хорошо известных человеку звуков.

Звуки природы (лес, птицы)…….....10–20
Библиотека……...30–40
Офис…….....60–70
Речь человека……..…..65–75
Легковой автомобиль…….....80–90
Грузовой автомобиль…….....90–95
Пневматический инструмент……..100–105
Реактивный самолет (взлет)……120–125

К преимуществам логарифмической шкалы относится также то, что она более точно, чем линейная шкала, соответствует субъективному восприятию

относительной громкости звука. Это обусловливается тем, что слух реагирует на процентные изменения интенсивности (давления) звука и, следовательно, на изменения его уровня. Уровень в 1 дБ является наименьшим обнаруживаемым слухом изменением уровня звука, отображающим идентичное относительное изменение в любой точке логарифмической шкалы.

Субъективное ощущение интенсивности звука (звукового давления) называется *громкостью* и измеряется в фонах (Ф). Уровень громкости звука в фонах численно равен интенсивности звука в децибелах для чистого тона частотой 1 кГц, воспринимаемого как равногромкий с данным звуком. Факторы, определяющие субъективную громкость звука, очень сложны. Одним из таких факторов является частотная зависимость чувствительности человеческого слуха, которая имеет максимальное значение в области средних частот и минимальное значение в области низких и высоких частот. Поэтому, чтобы обеспечить постоянную громкость звука, частота которого меняется, необходимо соответственно изменить его интенсивность или уровень звукового давления. Для этого используются графики кривых равной громкости в зависимости от уровня звукового давления и частоты. Так, например, звук с уровнем звукового давления 85 дБ и частотой 50 Гц оценивается как равный по громкости звуку с уровнем звукового давления 70 дБ и частотой 1 кГц. Таким образом, в данном случае повышение частоты компенсируется снижением уровня звукового давления.

Оценка громкости и высоты тона (частоты) очень коротких звуков затруднена. При длительности синусоидального тона 2–3 мс человек лишь отмечает его наличие как «щелчок», но не может определить его качеств. С увеличением длительности звука слуховое ощущение улучшается и человек начинает различать громкость и высоту тона. Минимальное время, необходимое для отчетливого ощущения уровня громкости и высоты тона, составляет примерно 50 мс.

Акустический анализатор позволяет определять расстояние до источника звука и направление на него. Важную роль в оценке изменения расстояния до источника звука играет различение изменений громкости. Звук, громкость которого увеличивается, воспринимается как приближающийся, и наоборот. Другим фактором оценки расстояний на слух является звуковысотное (звукочастотное) различение. При приближении источника звука к человеку частота звуковых колебаний увеличивается, а при его удалении – уменьшается (эффект Доплера). Это отражается в слуховых ощущениях в форме изменения высоты звука. Значительное влияние на оценку расстояния оказывает тембр. Тембрированный звук, имеющий более сложную форму звуковой волны, оценивается как более удаленный, а менее тембрированный – как более близкий.

Точность определения направления зависит от положения источника звука относительно человека и от частоты звука. Наиболее точно определяется направление в горизонтальной плоскости. При этом на первом месте по точности оказывается правое направление, а затем левое. Достаточно хорошо определяется переднее направление. Но с ним часто смешивается верхнее и заднее.

Точность оценки верхнего и заднего направления в два с лишним раза меньше по сравнению с левым и правым.

Для низких частот звука (до 800 Гц) точность определения направления в горизонтальной плоскости составляет около 10°. С увеличением частоты она уменьшается, достигая 20° в районе 3 кГц, а затем вновь увеличивается до 13° в районе 10 кГц.

Главную роль в восприятии направлений звука играет взаимодействие сторон акустического анализатора человека. Благодаря чему возникает бинауральный эффект, который определяется разностью времен прихода звуковой волны к правому и левому уху и отношением амплитуд звуковой волны, поступающих на правое и левое ухо [1–4].

2.2.3. Восприятие речевых сигналов и их характеристики

2.2.3.1. Восприятие речи

Одним из наиболее эффективных исторически сложившихся средств передачи информации человеку является речь. Человеческая речь представляет собой шумоподобный акустический сигнал с амплитудной и частотной модуляцией.

Речь состоит из звуков, слогов, фраз и т. д. Наименьшим элементом речи является звук, который, как правило, в изолированном виде не существует, за исключением нескольких союзов и междометий. Точного определения понятия звука не существует. Так, в зависимости от произношения (почерка) звук может иметь много оттенков, причем из-за индивидуальности произношения на слух он может не отличаться от другого звука.

Типизированные звуки речи в технике передачи речи называются *фонемами*. В русском языке насчитывается свыше 40 фонем. Таким образом, фонем несколько больше, чем букв, так как многие из согласных букв соответствуют двум звукам – твердому и мягкому. В то же время почти половина гласных букв представляет из себя двойной звук (й + гласный). Каждая из фонем имеет свои характерные признаки, легко различимые на слух. Однако даже при самом точном произношении ее в связной речи, вследствие влияния соседних звуков, она может приобретать те или иные оттенки. Речевой звук является сложным. Он включает ряд обертонов (гармоник), находящихся в гармоническом отношении к основному тону. Важным условием восприятия речи является различение длительности произнесения отдельных звуков и их комбинаций. Среднее время длительности произнесения гласных равно примерно 0,35 с, а согласных – 0,02–0,3 с. При восприятии потока речи особенно важно различение интервалов между словами или группами слов. Исключение пауз или их неверная расстановка может привести к искажению смысла воспринимаемой речи. Восприятие и понимание речевых сообщений (аудирование) в значительной мере зависит от темпа их передачи. Оптимальным считается темп 120 слов/мин.

При восприятии отдельных слогов и слов существенное влияние оказывают фонетические закономерности. При восприятии словосочетаний в действие вступают синтаксические закономерности, а фонетические отступают на второй план. При переходе к фразам слушатель начинает ориентироваться уже не на отдельные элементы предложения, а на весь их сложный грамматический каркас.

Таким образом, *аудирование* представляет собой многоуровневый процесс, сочетающий фонетический (звуковой), синтаксический (словосочетательный) и семантический (смысловой) уровни. При этом вышележащие уровни играют ведущую роль, определяя ход всего процесса аудирования, что необходимо иметь в виду при организации речевых сообщений [1–4].

2.2.3.2. Характеристики речевого сигнала

Звуковое давление речи – это сила, с которой звуковая волна, вызываемая звуками речи, давит на единицу площади поверхности, расположенной перпендикулярно губам говорящего на расстоянии 1 м от него. Уровни звукового давления речи лежат в диапазоне 0–65 дБ (негромкая речь) и 0–80 дБ (громкая речь, усиленная техническими средствами). С увеличением расстояния от говорящего уровень звукового давления речи падает. Так, например, увеличение расстояния в два раза приводит к уменьшению уровня на 6 дБ, в четыре раза – на 12 дБ, в восемь раз – на 18 дБ и т. д.

Частота основного тона. Формирование значительной части звуков речи происходит с участием голоса. Голосообразование, или фонация, связано с работой голосовых связок, колебания которых вызывают периодические изменения площади голосовой щели. Так как голосовые связки обладают определенной инерцией, обусловленной их массой, то для их размыкания и смыкания требуется определенное время. Отрезок времени, необходимый для полного цикла колебаний голосовых связок, называется *периодом колебаний*. Он определяет так называемую *частоту основного тона* голоса речи, которая в свою очередь обусловливает *высоту голоса*. Эта частота для всех голосов лежит в пределах 70–450 Гц. При произнесении речи она непрерывно меняется в соответствии с ударением, подчеркиванием звуков и слов, а также при проявлении эмоций. Изменение частоты основного тона называют интонацией. У каждого человека свой диапазон изменения частоты основного тона и своя интонация. Основной тон, интонация, устный «почерк» и тембр (окраска) голоса могут служить для опознания человека. Частота основного тона определяет *спектральный состав* (гармоники) голоса конкретного человека.

Спектральная плотность. Речевой сигнал представляет собой шумоподобный сигнал. Он состоит из звуковых волн различных частот с различными интенсивностями, которые представляют собой *спектр сигнала*. *Спектральной плотностью* интенсивности речевого сигнала называется отношение средней интенсивности сигнала в заданной полосе частот $\Delta I_{\text{ср}}$ к ширине этой полосы

Δf : $W = \Delta I_{\text{ср}} / \Delta f$. Спектральная плотность измеряется в ваттах на метр квадратный на герц (Вт/м²/Гц) и численно равна интенсивности шума в полосе частот шириной 1 Гц.

«***Белый шум***» представляет собой случайный процесс, спектр которого равномерен по интенсивности шума в полосе частот от нуля до бесконечности, т. е. спектральная плотность которого не зависит от частоты (в заданной полосе частот). Практически достаточно, чтобы это требование выдерживалось в полосе слышимых частот, если такой шум используется для исследований в данной области частот.

«***Розовый шум***» представляет собой случайный процесс, огибающая спектра которого спадает в сторону высоких частот со скоростью 3 дБ на октаву. Спектральный состав такого шума наиболее близок к спектральному составу речевого сигнала.

Высота звука (голоса) – это субъективная оценка восприятия звука по частотному диапазону. За объективную единицу высоты звука, приближенно отражающей субъективное восприятие, принята *октава*, которая характеризуется двукратным отношением частот – 1, 2, 4, 8, 16 и т. д. На практике октава может делиться на *полуоктавы* и *третьоктавы*. Если октавные частоты расположить на равных расстояниях по оси частот, то получится логарифмический масштаб, который соответствует субъективному восприятию звуков по частоте слуховым анализатором.

Динамический диапазон. В процессе произношения любого речевого сообщения уровень акустического сигнала непрерывно изменяется. Зависимость уровня сигнала от времени называется *уровнеграммой. Динамический диапазон* определяется как разность между максимальным и минимальным уровнем сигнала: $D = L_{\max} - L_{\min}$. Динамический диапазон речи человека составляет 25–35 дБ, а телефонных разговоров – 35–45 дБ.

Пик-фактор определяется как разность между максимальным и средним уровнем сигнала: $P = L_{\max} - L_{\text{ср}}$.

Форманты – это области концентрации энергии в речевом частотном диапазоне, получающиеся при произнесении каких-либо звуков речи. Обычно форманты полностью заполняют весь частотный диапазон речи от 125 до 8000 Гц. Но в зависимости от частоты повторения звука речи частота встречаемости формант в определенной полосе частот различна. Каждая из формант дает свою часть информации о звуке речи, и эти части независимы друг от друга. Это дает возможность арифметически суммировать вероятности появления формант. Спектр гласных определяется двумя-тремя формантами. Первая имеет диапазон 300–1000 Гц, вторая – 900–2300 Гц, третья – 2200–2500 Гц. Спектр согласных чаще всего имеет один достаточно расплывчатый минимум.

Слитность звучания. Слуховое ощущение звука исчезает не сразу, а постепенно, плавно уменьшаясь до нуля. Длительность задержки слухового ощущения характеризуется постоянной времени слуха, которая в среднем равна

150–200 мс. Вследствие этого свойства наблюдается интегрирование кратковременных звуковых импульсов в слитное восприятие звуков, запаздывающих друг относительно друга. Для слитного восприятия двух звуков необходимо, чтобы последующий звук запаздывал относительно предыдущего на промежуток времени не более 50 мс. Но и при большем запаздывании слитность звучания может не нарушаться, если последующий звук имеет уровень значительно ниже первого. Приближенно считается, что интенсивность звуков, запаздывающих на 60 мс и менее, полностью суммируется с интенсивностью основного звука, а звуки, запаздывающие более чем на 60 мс, полностью являются помехой. При больших интервалах запаздывания ощущение от первого звука уже становится малым и не маскирует второй. Поэтому оба звука воспринимаются раздельно.

Прямое и диффузное звучание. При распространении звуков речи в помещении звук, выходя из источника, распространяется прямолинейно до тех пор, пока не достигнет поверхности, от которой он отражается. Звук, распространяющийся прямолинейно до момента своего отражения, называется *прямым звуком*, а звуковое поле – *свободным звуковым полем.* В то же время звук, многократно отражающийся от поверхностей, создает в каждой точке звукового поля помещения звуковую энергию, одинаковую во всех направлениях. Такое звуковое поле и звуки в нем называются *диффузными***.**

Индекс направленности слуха. При перпендикулярном падении звуковой волны на ухо имеет место отражение волны и ее дифракция. Соотношение между интенсивностями отраженной и дифрагирующей волн зависит от отношения длины звуковой волны и размера головы. Так как волна отражается от головы, то звуковое давление у уха повышается. Это повышение может составлять 1–6 дБ в зависимости от частоты. В случае падения звуковой волны спереди явление отражения почти не сказывается. При падении звуковой волны под различными углами, как это свойственно диффузному полю, на низких частотах звуковое давление возле ушей примерно равно звуковому давлению диффузного поля, а на высоких частотах это давление удваивается. Величина повышения звукового давления у уха слушателя, выраженная в децибелах, по сравнению с диффузным звуком в помещении называется индексом направленности слуха [1, 2].

2.2.3.3. Эффект маскировки речевых сигналов

Маскировкой речевого сигнала называется явление, выражающееся в том, что восприятие звуков, несущих определенную информацию, ухудшается при одновременном звучании других мешающих звуков. В результате возникает потеря части или даже всей информации. Использование этого явления и лежит в основе одного из методов защиты речевой информации. Маскировка может быть нескольких видов: одновременная (помехой, действующей одновременно с сигналом), последовательная, или остаточная (помехой, предшествующей сигналу), обратная (помехой, следующей после сигнала).

Количественно маскировка оценивается путем определения порога слышимости синусоидальных звуков в присутствии мешающего звука. Если изменять частоту испытательного тона и определять на каждой частоте уровень интенсивности, при которой он начинает прослушиваться наряду с мешающим звуком, то можно получить *кривую порога слышимости* при наличии маскировки.

Эффект маскировки определяется разностью порогов слышимости (для чистого тона заданной частоты) в шумах и в тишине:

$$M = b_{\text{Ш}} - b_{\text{Т}}, \tag{2.7}$$

где $b_{\text{Ш}} = 10 \cdot \lg(I_{\text{Ш}} / I_0)$ – уровень порога слышимости в шумах;

$b_{\text{Т}} = 10 \cdot \lg(I_{\text{Т}} / I_0)$ – уровень порога слышимости в тишине;

$I_{\text{Ш}}$ – интенсивность шума;

$I_{\text{Т}}$ – интенсивность звука в тишине (без шума);

I_0 – нулевой уровень ($2 \cdot 10^{-5}$ Па).

Эффект маскировки зависит от ряда факторов. В первую очередь он определяется уровнем маскирующего звука. Существенное влияние имеет и форма огибающей спектра шумов: низкочастотные составляющие шумов маскируют звуки высокой частоты лучше, чем высокочастотные составляющие шумов – звуки низкой частоты. Наиболее распространенным видом помехи является «белый шум». Его маскирующее действие в основном определяется относительно узкой полосой частот, лежащих вблизи маскируемого тона. Когда общая энергия, приходящаяся на критический участок «белого шума», равна энергии тона, происходит полное подавление полезного сигнала.

В случае дискретных шумовых спектров эффект маскировки получается наибольшим для звуков, частотные составляющие которых располагаются вблизи частот маскирующих составляющих. На этом основаны методы зашумления речи с помощью маскирующих сигналов. При тональной помехе маскирующее действие выражается тем больше, чем ближе ее частота к частоте сигнала.

Специфическим видом маскировки является речевая смесь (речевой хор, речевой коктейль), при которой на речевой сигнал накладывается несколько других речевых сигналов (разговор двух или нескольких человек одновременно).

Чтобы речевые звуки были понятными, их интенсивность должна превышать интенсивность шумов в общем случае примерно на 6 дБ. Однако обнаружить звуки можно даже в том случае, когда интенсивность речи меньше интенсивности шума (примерно также на 6 дБ).

Понимание слов на фоне «белого шума» зависит от ряда факторов. Многосложные слова понимаются лучше, чем односложные. Это объясняется тем, что более длинное слово обладает большим числом опознавательных призна-

ков, чем короткое. Слова, начинающиеся с гласного звука, понимаются лучше, чем начинающиеся с согласного. Определенное влияние на понимание оказывает место ударного слога. Слово понимается значительно лучше, если ударение находится в конце него. Длина фразы не влияет на понимание до уровня примерно в 11 слов, после чего понимание ухудшается. С увеличением глубины фразы понимание ухудшается, даже если длина фразы остается неизменной. При этом критической величиной является глубина фразы в 5–9 слов. Понимание в условиях «речевой смеси» обусловлено также рядом факторов. Ухо способно различать нужный голос среди двух-трех абонентов. Из двух одновременных сообщений точнее воспринимается поступившее на 0,2–0,4 с раньше. Дифференцирование сообщений возможно разделением по смыслу, по индивидуальным голосовым характеристикам, по направлению звука на правое и левое ухо, использованием дополнительных визуальных индикаторов [1, 3, 4].

2.2.3.4. Разборчивость речи

Разборчивость речи при защите речевой информации должна рассматриваться в двух аспектах. С одной стороны, при озвучивании какого-либо сообщения, предназначенного для определенных слушателей, необходимо стремиться к тому, чтобы оно было услышано и точно понято. В этом случае разборчивость речи должна быть максимальной. С другой стороны, для обеспечения защиты речевой информации от возможного перехвата необходимо сделать речевой сигнал минимально разборчивым. При этом уменьшение разборчивости необходимо обеспечивать в местах возможной установки прослушивающих устройств, куда будет падать звуковая волна речевого сигнала. При этом необходимо иметь в виду, что приемником речевого сигнала является слух человека, имеющий характеристики, которые отличаются от характеристик обычно используемых приемников сигналов.

При анализе условий передачи речи необходимо учитывать разницу в проведении ее оценки. В одних случаях речь оценивают только с точки зрения ее понятности, а в других – с точки зрения разборчивости и качества звучания, поскольку кроме понятности речи необходима и узнаваемость голоса.

Разборчивостью речи называется относительное или процентное количество принятых специально подготовленными слушателями элементов речи из общего количества переданных по тракту. В качестве элементов речи принимают слоги, звуки, слова, фразы (команды) и цифры. Соответственно этому различают слоговую, звуковую, смысловую и цифровую разборчивость. В соответствии с измеренной разборчивостью устанавливаются классы качества разборчивости речи и нормы разборчивости звуков и односложных слов. В частности, для радио- и телефонной аппаратуры установлены пять классов качества по нормам разборчивости [5]. Классы качества и их характеристики приведены в табл. 2.1

Таблица 2.1

Классы качества и нормы разборчивости речи
(в соответствии с ГОСТ Р50840–95)

Класс качества	Характеристика класса качества	Норма слоговой разборчивости речи, %
Высший	Понимание передаваемой речи без малейшего напряжения внимания	Более 93
I	Понимание передаваемой речи без затруднений	86–93
II	Понимание передаваемой речи с напряжением внимания без переспросов и повторений	76–85
III	Понимание передаваемой речи с некоторым напряжением внимания, с редкими переспросами и повторениями	61–75
IV	Понимание передаваемой речи с большим напряжением, частыми переспросами и повторениями	45–60

Таким образом, для надежной защиты речевой информации в местах возможного ее перехвата необходимо обеспечивать разборчивость слов менее 60 %.

2.2.3.5. Основные методы измерения разборчивости речи

Для измерения разборчивости речи используются следующие методы:

– метод артикуляционных измерений;

– расчетный метод остаточной разборчивости речи по формантной разборчивости;

– метод спектрального анализа речевого сигнала.

Метод артикуляционных измерений заключается в том, что слушатели воспринимают на слух определенное число односложных слов, фиксируют их, после чего проводится сравнение полученного результата с исходным текстом и определяется процент правильно принятых слов [1, 2, 5, 6].

Расчетный метод остаточной разборчивости речи по формантной разборчивости основан на том, что формантная разборчивость имеет однозначную связь со словесной разборчивостью для каждого конкретного языка. Поэтому, оценивая с помощью соответствующего расчета или измерения уровня ощущения формант, можно достаточно точно определить разборчивость речи в конкретных условиях ее произношения [1, 6].

Метод спектрального анализа речевого сигнала основан на том, что разборчивость формант определяется законами распределения вероятности

формант по частотному и динамическому диапазону речи. Поэтому величина формантной разборчивости в практических условиях с достаточной степенью точности может быть определена произведением ширины частотного диапазона (в герцах) и средней величины эффективного динамического диапазона речи (в децибелах). После чего по формуле связи между словесной и формантной разборчивостями или по соответствующей таблице определяется словесная разборчивость.

Метод артикуляционных измерений является наиболее простым и не требует большого объема измерений и вычислений. Поэтому для определения разборчивости речи при исследовании защиты речевой информации с помощью маскирующих сигналов в данной лабораторной работе используется указанный метод. Рассмотрим его более подробно.

2.2.3.6. Метод артикуляционных измерений

Для реализации этого метода необходимо наличие группы слушателей в составе не менее трех человек, трех и более дикторов, звукозаписывающей аппаратуры, источников маскирующих сигналов и шумомера для измерения уровней речи и шума. Слушатели принимают на слух некоторое число таблиц. Такие таблицы состоят из 50 односложных слов, например, «год», «док», «ток», «куб», «миг», «час» и т. п. Примеры таблиц приведены в [5, 6].

Перед проведением контрольных измерений слушатели должны провести пробный прием нескольких таблиц слов с целью адаптации и освоения метода измерений. Методика разборчивости слов заключается в следующем [5, 6].

Воспроизводятся записанные предварительно на магнитный или другой носитель таблицы слов с соответствующим видом и уровнем маскирующих сигналов. Слова должны произноситься со скоростью 1 таблица за 3 мин ровным голосом без подчеркивания начальных и конечных согласных. В одном измерении не допускается повторное чтение одной и той же таблицы. Воспроизведение слов таблиц следует проводить при среднем уровне звукового давления 70 дБ, измеренного на расстоянии, на котором находятся слушатели от акустической системы. Уровни звукового давления маскирующих сигналов должны измеряться на том же расстоянии и меняться ступенчато через 3 дБ в диапазоне 60–80 дБ. При необходимости этот диапазон может быть расширен.

Слушатели записывают принятые слова в таблицы, в которых указывается номер таблицы, фамилия слушателя, дата, уровень полезного и маскирующего сигнала, вид маскирующего сигнала и, при необходимости, другие данные. Для удобства обработки таблиц слова необходимо записывать под своими порядковыми номерами. Пример такой таблицы приведен в [5, 6].

Проводится определение правильности записанных слов путем сравнения таблицы принятых слов и исходной таблицы.

Определяется разборчивость слов для каждой таблицы, принятой одним слушателем, по формуле

$$S_i = (N_{\text{П}} / N) \cdot 100\ \%, \tag{2.8}$$

где $N_{\text{П}}$ – количество правильно записанных слов;

N – общее количество воспроизведенных (записанных) слов.

Определяется среднее значение разборчивости слов и среднее квадратическое отклонение по формулам

$$S_{\text{ср}} = \frac{\sum_{i=1}^{n} S_i}{n}; \tag{2.9}$$

$$\sigma_s = \sqrt{\frac{\sum_{i=1}^{n} (S_i - S_{\text{ср}})^2}{n-1}}, \tag{2.10}$$

где $n = m \cdot k$ – общее число таблиц, принятых всеми слушателями;

m – число слушателей;

k – число переданных таблиц.

Если $|S_i - S_{\text{ср}}| > 2\sigma_S$, то данные результаты измерений исключаются и повторно проводятся вычисления по формулам (2.8)–(2.10) с учетом уменьшенного числа измерений [6].

2.3. Порядок выполнения работы

1. Изучить теоретическую часть работы.
2. Провести самопроверку теоретических знаний, ответив на поставленные вопросы.
3. Провести запись воспроизводимых слов таблиц для различных уровней полезного и маскирующих сигналов и их видов.
4. Определить число правильно принятых слов путем сравнения полученных результатов с исходными данными.
5. Провести расчет разборчивости слов по формулам (2.8)–(2.10).
6. Определить по полученным результатам вид маскирующего сигнала, наиболее подходящего для защиты речевой информации.
7. Оформить отчет и защитить работу.

2.4. Описание программы для ЭВМ

Программа позволяет проверять теоретические знания студентов, определять количество правильно принятых слов, рассчитывать необходимые пара-

метры разборчивости слов и проверять правильность выбора маскирующего сигнала, обеспечивающего наилучшую защиту речевой информации, для каждой группы аудиторов и соответствующих вариантов, включающих различные комбинации экспериментов. Имя программы SPEECH.

2.5. Содержание отчета

1. Цель лабораторной работы.
2. Таблицы с распознанными словами для различных уровней полезного и маскирующих сигналов и их видов.
3. Таблицы с результатами расчетов разборчивости речи для различных уровней полезного и маскирующих сигналов и их видов для каждого аудитора и с результатами средних значений для группы аудиторов.
4. Выводы по работе.

Литература

1. Сапожков, М. А. Электроакустика / М. А. Сапожков. – М. : Связь, 1978. – 272 с.
2. Вахитов, Я. Ш. Теоретические основы электроакустики и электроакустическая аппаратура / Я. Ш. Вахитов. – М. : Искусство, 1982. – 415 с.
3. Основы инженерной психологии / Б. А. Душков [и др.] ; под ред. Б. Ф. Ломова. – М. : Высш. шк., 1986. – 448 с.
4. Справочник по инженерной психологии / С. В. Борисов [и др.] ; под ред. Б. Ф. Ломова. – М. : Машиностроение, 1982. – 368 с.
5. ГОСТ Р50840–95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – М. : Госстандарт России, 1995. – 230 с.
6. Алефиренко, В. М. Расчет и измерение разборчивости речи для акустических устройств РЭС : метод. указания к практ. занятиям по курсу «Конструирование РЭС» для студ. спец. «Проектирование и производство РЭС» / В. М. Алефиренко, Г. В. Давыдов, Ю. В. Шамгин. – Минск : БГУИР, 1998. – 32 с.

Лабораторная работа №3

Исследование криптографических методов защиты информации

3.1. Цель работы

Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.

3.2. Теоретические сведения

3.2.1. Основные понятия, термины и определения криптографии

Слово «*криптография*» произошло от древнегреческих слов «cryptos» – тайный и «graphos» – письмо. Таким образом, криптография – это тайнопись. Криптографическая защита информации (данных) с помощью кодов и шифров является одним из важнейших решений проблемы ее безопасности. Зашифрованные данные становятся доступными только тому, кто знает, как их расшифровать. Поэтому похищение зашифрованных данных бессмысленно для несанкционированных пользователей.

Различные коды и шифры используются давно. С теоретической точки зрения между ними не существует четкого различия. Однако в современной практике использования криптографии различие между ними определено достаточно четко [1, 2].

Кодирование – это процесс замены элементов открытого текста (символов, комбинаций символов, слов и т. п.) кодами. *Коды* оперируют лингвистическими элементами, разделяя кодируемый текст на такие смысловые элементы, как слова и слоги.

Шифрование – это процесс зашифрования или расшифрования. В этом процессе криптографическому преобразованию подвергается каждый символ текста. В шифровании всегда используются два элемента: алгоритм и ключ.

Алгоритм шифрования – это последовательность определенных действий над открытым текстом, в результате которых получается зашифрованный текст (шифротекст). Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Ключ – это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из всей совокупности возможных вариантов для данного алгоритма.

Шифр – это совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Зашифрование – это процесс преобразования открытых данных в зашифрованные с помощью шифра.

Расшифрование – это процесс преобразования закрытых данных в открытые данные с помощью шифра.

Дешифрование – это процесс преобразования закрытых данных в открытые данные при неизвестном ключе и, возможно, неизвестном алгоритме.

Гаммирование – это процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – это псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых данных и расшифрования зашифрованных данных.

Уравнение зашифрования – это соотношение, описывающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Уравнение расшифрования – это соотношение, описывающее процесс образования открытых данных из зашифрованных данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Имитозащита – это защита системы шифрованной связи от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка.

Имитовставка – это отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа, добавленный к зашифрованным данным для обеспечения имитозащиты.

Криптографическая защита – это защита данных с помощью криптографического преобразования.

Криптографическое преобразование – это преобразование данных с помощью шифрования и (или) выработки имитовставки.

Криптостойкость шифра – это характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

3.2.2. Методы криптографии

3.2.2.1. Классификация методов

Методы криптографии можно разделить на две группы: *с секретными ключами* и *с открытыми ключа*ми [1].

Методы криптографии ***с секретными (закрытыми) ключами*** предусматривают один ключ, который используется как в процессе зашифрования, так и в процессе расшифрования. Этот ключ известен только тем, кто зашифровывает и расшифровывает данные. Так как в этих методах используется только один ключ, они называются *симметричными методами*.

Методы криптографии *с открытыми ключами* предусматривают два ключа. Первый ключ используется для зашифрования и не является секретным.

Он может быть известен всем пользователям системы, которые зашифровывают данные. Расшифрование данных с помощью известного ключа невозможно. Для расшифрования используется второй ключ, который является секретным. Так как в этих методах используются два различных ключа, они называются *несимметричными методами*.

В свою очередь методы с секретными ключами делятся на *методы замены (подстановки)*, *методы перестановки* и *методы перемешивания*.

Метод замены (подстановки) основан на том, что каждый символ открытого текста заменяется другим символом того же алфавита. Конкретный вид замены определяет секретный ключ. Замена может быть *моноалфавитная*, *гомофоническая*, *полиалфавитная* и *полиграммная*. Для реализации метода замены может быть использован датчик (генератор) псевдослучайных чисел.

Метод замены с использованием датчика псевдослучайных чисел основан на генерации гаммы шифра с помощью генератора псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом. Расшифрование данных сводится к повторной генерации гаммы шифра при известном ключе и наложению этой гаммы на зашифрованные данные.

Метод перестановки основан на изменении порядка следования символов открытого текста. Порядок перестановки определяет секретный ключ. Перестановка может быть *простая* и *усложненная*.

Метод перемешивания основан на том, что изменение одного символа открытого текста приводит к изменению многих символов шифротекста.

3.2.2.2. Методы криптографии с секретными ключами

Общие положения

Классическим подходом в криптографии является использование секретных ключей. При этом подходе полагается, что криптоаналитик противника знает методику шифрования и секретность шифра определяется только секретностью ключа. Структурная схема шифрования с секретным ключом (симметричное шифрование) показана на рис. 3.1.

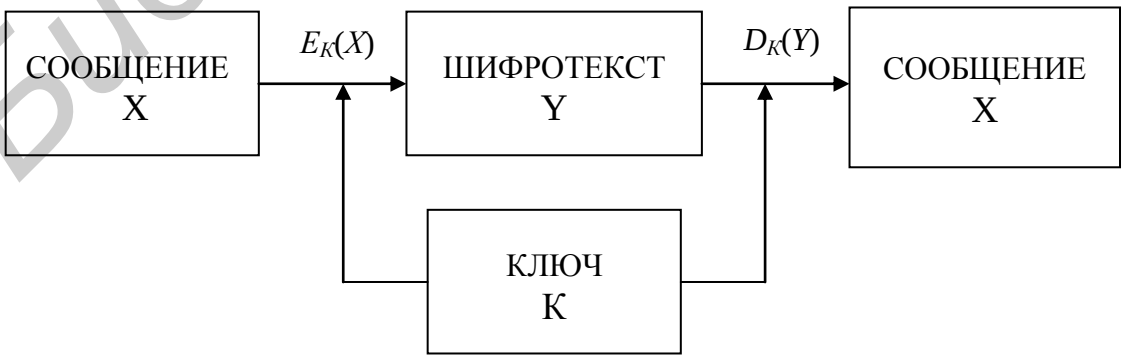

Рис. 3.1. Симметричное шифрование

Уравнение зашифрования может быть представлено в следующем виде:

$$X = E_K(X), \tag{3.1}$$

где E_K – символ, означающий алгоритм шифрования по секретному ключу K.

Уравнение расшифрования принимает тогда следующий вид:

$$X = D_K(Y), \tag{3.2}$$

где D_K – символ, означающий алгоритм расшифрования по секретному ключу K.

Таким образом, зашифрование и расшифрование проводится с помощью только одного секретного ключа [3].

Метод замены

Шифрование методом замены (подстановки) основано на алгебраической операции, называемой *подстановкой*. ***Подстановкой*** называется взаимно однозначное отображение некоторого конечного множества M на себя. Число N элементов этого множества называется *степенью подстановки*. Природа множества M роли не играет, поэтому можно сказать, что $M = 1, 2, N$.

В криптографии рассматриваются четыре типа подстановки (замены): *моноалфавитная*, *гомофоническая*, *полиалфавитная* и *полиграммная* [1]. Подстановка может быть реализована с использованием датчика псевдослучайных чисел.

Моноалфавитная замена. При моноалфавитной замене каждый символ алфавита открытого текста заменяется символом шифротекста из того же алфавита.

Общая формула моноалфавитной замены выглядит следующим образом:

$$Y_i = (K_1 \cdot X_i + K_2) \bmod n, \tag{3.3}$$

где Y_i – i-й символ шифротекста;
X_i – i-й символ открытого текста;
K_1 и K_2 – константы;
n – длина алфавита.

Под результатом операции $(K_1 \cdot X_i + K_2) \bmod n$ понимают остаток от целочисленного деления суммы $(K_1 \cdot X_i + K_2)$ на число n, если сумма больше длины алфавита.

Для описания алгоритма шифрования обычно вместо символов открытого и шифротекста используют их цифровые эквиваленты. Пример цифрового эквивалента букв русского алфавита (без знаков препинания) приведен в табл. 3.1.

Таблица 3.1

Цифровые эквиваленты букв русского алфавита

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Цифровой эквивалент	1	2	3	4	5	6	7	8	9	10	11	12
Буква	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Цифровой эквивалент	13	14	15	16	17	18	19	20	21	22	23	24
Буква	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_ (ПРОБЕЛ)			
Цифровой эквивалент	25	26	27	28	29	30	31	32	33			

Общее число символов алфавита $n = 33$.

Пример 1. Открытый текст: «ШИФРОВАНИЕ ЗАМЕНОЙ». Подстновка задана табл. 3.2.

Таблица 3.2

Пример подстановки алфавита для шифрования моноалфавитной заменой

Алфавит открытого текста	А	Б	В	Г	Д	…	Ь	Э	Ю	Я	_
Алфавит шифротекста	–	Я	Ю	Э	Ь	…	Д	Г	В	Б	А

Шифротекст: «ИШМРТЮ_УШЫАЩ_ФЫУТЧ».

Основным недостатком рассмотренного метода является то, что статистические свойства открытого текста (частоты появления букв) сохраняются и в шифротексте. Этого недостатка лишены шифры Вижинера и Бофора.

Шифр Вижинера. Шифр Вижинера задается формулой

$$Y_i = (X_i + K_i) \bmod n, \qquad (3.4)$$

где K_i – i-й символ ключа, в качестве которого используется слово или фраза.

Пример 2. Открытый текст: «ЗАМЕНА». В качестве ключа используется слово «КЛЮЧ». Подстановка задана табл. 3.3.

Таблица 3.3

Подстановка шифра Вижинера

З	А	М	Е	Н	А
К	Л	Ю	Ч	К	Л

В соответствии с табл. 3.1 записываем:

$$Y_1 = (8 + 11) \bmod 33 = 19 \rightarrow \text{Т};$$
$$Y_2 = (1 + 12) \bmod 33 = 13 \rightarrow \text{М};$$
$$Y_3 = (13 + 31) \bmod 33 = 11 \rightarrow \text{К};$$
$$Y_4 = (6 + 24) \bmod 33 = 30 \rightarrow \text{Э};$$
$$Y_5 = (14 + 11) \bmod 33 = 25 \rightarrow \text{Ш};$$
$$Y_6 = (1 + 12) \bmod 33 = 13 \rightarrow \text{М}.$$

Шифротекст: «ТМКЭШМ».

Шифр Вижинера с неограниченным неповторяющимся ключом называют шифром Вернама.

Шифры Бофора. Шифры Бофора задаются формулами

$$Y_i = (K_i - X_i) \bmod n;$$
$$Y_i = (X_i - K_i) \bmod n. \qquad (3.5)$$

Так как при использовании шифров Бофора возможны случаи, когда разность может быть равна нулю, то нумерацию символов алфавита необходимо начинать с нуля. Тогда в табл. 3.1 буква А будет соответствовать 0, Б – 1, В – 2 и т. д.

При рассмотрении этих видов шифров видно, что чем больше длина ключа, тем лучше шифр. Существенного улучшения свойств шифротекста можно достигнуть при использовании *шифров с автоключом*.

Шифр, в котором сам открытый текст или получающаяся криптограмма используется в качестве ключа, называется ***шифром с автоключом***. Шифрование в этом случае начинается с ключа, называемого первичным, и продолжается с помощью открытого текста или криптограммы, смещенных на длину первичного ключа.

Пример 3. Открытый текст: «ШИФРОВАНИЕ ЗАМЕНОЙ». Первичный ключ: «КЛЮЧ». Схема шифрования с автоключом при использовании открытого текста представлена в табл. 3.4.

Таблица 3.4

Схема шифрования с автоключом при использовании открытого текста

Ш	И	Ф	Р	О	В	А	Н	И	Е	_	З	А	М	Е	Н	О	Й
К	Л	Ю	Ч	Ш	И	Ф	Р	О	В	А	Н	И	Е	_	З	А	М
36	21	52	41	40	12	22	31	24	9	34	22	10	19	39	22	16	23
В	Ф	Т	З	Ж	Л	Х	Ю	Ч	И	А	Х	Й	Т	Е	Х	П	Ц

Шифротекст: «ВФТЗЖЛХЮЧИАХЙТЕХПЦ».

Схема шифрования с автоключом при использовании криптограммы представлена в табл. 3.5.

Таблица 3.5

Схема шифрования с автоключом при использовании криптограммы

Ш	И	Ф	Р	О	В	А	Н	И	Е	_	З	А	М	Е	Н	О	Й
К	Л	Ю	Ч	В	Ф	Т	З	С	Ч	У	Х	Ъ	Э	У	Э	Ы	Й
36	21	52	41	18	24	20	22	27	30	53	30	28	43	26	44	43	20
В	Ф	Т	З	С	Ч	У	Х	Ъ	Э	У	Э	Ы	Й	Щ	К	Й	У

Шифротекст: «ВФТЗСЧУХЪЭУЭЫЙЩКЙУ».

Гомофоническая замена. При гомофонической замене каждый символ алфавита открытого текста заменяется в определенном порядке несколькими символами шифротекста из этого же алфавита. Этот метод применяется для искажения статистических свойств шифротекста.

Пример 4. Открытый текст: «ЗАМЕНА». Подстановка задана табл. 3.6.

Таблица 3.6

Пример подстановки алфавита для шифрования гомофонической заменой

Алфавит открытого текста	А	Б	…	Е	Ж	З	…	М	Н	…
Алфавит шифротекста	17 31 48	23 44 63	… … …	97 51 15	47 67 33	76 19 59	… … …	32 28 61	55 84 34	… … …

Каждая буква открытого текста заменяется по очереди цифрами соответствующего столбца.

Шифротекст: «76 17 32 97 55 31».

Полиалфавитная замена. При полиалфавитной замене используется несколько алфавитов шифротекста. Пусть используется k алфавитов. Тогда открытый текст

$$X = X_1 X_2 \ldots X_k X_{k+1} \ldots X_{2k} X_{2k+1} \ldots \qquad (3.6)$$

заменяется шифротекстом

$$Y = F_1(X_1)F_2(\mathrm{X}_2)\ldots F_k(X_k)F_1(X_{k+1})\ldots F_k(X_{2k})F_1(X_{2k+1})\ldots, \qquad (3.7)$$

где $F_i(X_j)$ – символ шифротекста алфавита i для символа открытого текста X_j.

Пример 5. Открытый текст: «ЗАМЕНА». $K = 3$. Замена задана табл. 3.6, в которой каждая строка цифр соответствует своему алфавиту шифротекста.

Шифротекст: «76 31 61 97 84 48».

Полиграммная замена. Полиграммная замена формируется из одного алфавита с помощью специальных правил. Примером полиграммной замены может служить шифр Плэйфера.

Шифр Плэйфера. В этом шифре алфавит располагается в матрице. Открытый текст разбивается на пары символов X_i, X_{i+1}. Каждая пара символов открытого текста заменяется на пару символов из матрицы по следующим правилам:

– если символы находятся в одной строке, то каждый из символов пары заменяется на стоящий правее от него (за последним символом в строке следует первый);

– если символы находятся в одном столбце, то каждый символ пары заменяется на символ, расположенный ниже его в столбце (за последним нижним символом следует верхний);

– если символы пары находятся в разных строках и столбцах, то они считаются противоположными углами прямоугольника. Символ, находящийся в левом углу, заменяется на символ, стоящий в другом левом углу. Замена символа, находящегося в правом углу, осуществляется аналогично;

– если в открытом тексте встречаются два одинаковых символа подряд, то перед шифрованием между ними вставляется специальный символ (например тире).

Пример 6. Открытый текст: «ШИФР ПЛЭЙФЕРА». Матрица алфавита задана табл. 3.7.

Таблица 3.7

Матрица алфавита шифра Плэйфера

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

Шифротекст: «РДИЫ,–СТ–И.ХЧС».

Метод замены с использованием датчика псевдослучайных чисел. Шифрование этим методом заключается в генерации гаммы шифра датчиком псевдослучайных чисел с последующим наложением полученной гаммы на открытые данные обратимым способом (например, путем поразрядного сложения по модулю 2 с использовнием логической операции «исключающее ИЛИ»: 0 + + 0 = 0; 1 + 0 = 1; 0 + 1 = 1; 1 + 1 = 0).

Таким образом, открытый текст, ключ и шифротекст представляются в виде двоичных последовательностей. Ключевая последовательность формируется датчиком псевдослучайных чисел, который запускается начальным значением ключа.

Расшифрование данных осуществляется путем повторной генерации ключевой последовательности при известном начальном значении ключа и наложения ее на шифротекст [1].

Зашифрованное сообщение будет достаточно трудно дешифровать, если гамма шифра не содержит повторяющихся битовых последовательностей или если период гаммы превышает длину всего зашифрованного сообщения и неизвестна никакая часть исходного текста. Шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Для получения линейных последовательностей элементов гаммы шифра, длина которых превышает размер шифруемых сообщений, используется генератор псевдослучайных чисел. Линейные последовательности псевдослучайных чисел, вырабатываемые таким генератором, описываются соотношением:

$$T(i+1) = [\,AT(i) + C\,] \bmod M, \qquad (3.8)$$

где A и C – константы;

$T(i)$ – исходная величина, выбранная в качестве порождающего числа (входного ключа).

Генератор вырабатывает псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений A и C. Значение M обычно устанавливается равным 2^l, где l – длина последовательности (длина слова в ЭВМ) в битах.

Различают методы *конечной* и *бесконечной гаммы*. В качестве ***конечной гаммы*** может использоваться фраза, а в качестве ***бесконечной гаммы*** – последовательность, вырабатываемая генератором псевдослучайных чисел.

Пример 7. Открытый текст: «ПРИКАЗ» («16 17 09 11 01 08» согласно табл. 3.1).

Гамма: «ГАММА» («04 01 13 13 01» согласно табл. 3.1)

Операция: сложение по mod 33:

$Y_1 = (16 + 4) \bmod 33 = 20 \rightarrow$ У;
$Y_2 = (17 + 1) \bmod 33 = 18 \rightarrow$ С;
$Y_3 = (9 + 13) \bmod 33 = 22 \rightarrow$ Х;
$Y_4 = (11 + 13) \bmod 33 = 24 \rightarrow$ Ч;
$Y_5 = (1 + 1) \bmod 33 = 2 \rightarrow$ Б;
$Y_6 = (8 + 4) \bmod 33 = 12 \rightarrow$ Л.

Шифротекст: «УСХЧБЛ».

Пример 8. Открытый текст: «ПРИКАЗ» («16 17 09 11 01 08» согласно табл. 3.1).

Первые значения датчика: «2 1 7 9 4 5 6 7».

Операция: сложение по mod 2 с использованием логической операции «исключающее ИЛИ».

Запишем код (цифру) каждой буквы открытого текста в двоичном виде, используя пять разрядов, а каждую цифру гаммы – используя четыре разряда, и проведем операцию сложения по mod 2:

```
10000(16)  10001(17)  01001(09)  01011(11)  00001(01)  01000(08)
⊕
00010(2)   00001(1)   00111(7)   01001(9)   00100(4)   00101(5)
-----------------------------------------------------------------

10010(18)  10000(16)  01110(14)  00010(02)  00101(05)  01101(13)
```

Шифротекст: «СПНБДМ» («18 16 14 02 05 13»).

Шифрование заменой необязательно предполагает замену символов открытого текста символами того же алфавита или цифрами. В качестве алфавита шифротекста возможно использование символов псевдографики или, например, музыкальных нот. Основным недостатком методов замены является взаимное соответствие положения открытого текста и шифротекста.

Метод перестановки

Шифрование методом перестановки основано на перестановке символов открытого текста, порядок которой определяет ключ.

Существует большое количество различных способов перестановки. В качестве примера рассмотрим *простую* и *усложненную перестановки* [1].

Простая перестановка. При простой перестановке осуществляется перестановка групп символов алфавита открытого текста в определенном порядке.

Пример 9. Открытый текст: «ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ». Ключ (правило перестановки): буквы в группах из восьми букв с порядковыми номерами 1, 2, …, 8 переставить в порядок 3, 8, 1, 5, 2, 7, 6, 4.

Шифротекст: «ФНШОИАВР_СИЕЕЕРПНЙТВАОКО».

Усложненная перестановка. При усложненной перестановке открытый текст записывается в матрицу по определенному ключу K_1. Шифротекст образуется при считывании из этой матрицы по ключу K_2.

Пример 10. Открытый текст: «ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ». Матрица из четырех столбцов приведена в табл. 3.8, где запись открытого текста проведена по строкам в соответствии с ключом K_1: 5, 3, 1, 2, 4, 6, а чтение – по столбцам в соответствии с ключом K_2: 4, 2, 3, 1.

Таблица 3.8

Матрица алфавита с перестановкой из четырех столбцов

1	И	Е	_	П
2	Е	Р	Е	С
3	О	В	А	Н
4	Т	А	Н	О
5	Ш	И	Ф	Р
6	В	К	О	Й
K_1/K_2	1	2	3	4

Шифротекст: «ПСНОРЙЕРВАИК_ЕАНФОИЕОТШВ».

Более сложные перестановки осуществляются с использованием графа по так называемым гамильтоновым путям, которых в графе может быть несколько.

Пример 11. Открытый текст:

«ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ». Ключ – гамильтонов путь на графе рис. 3.2.

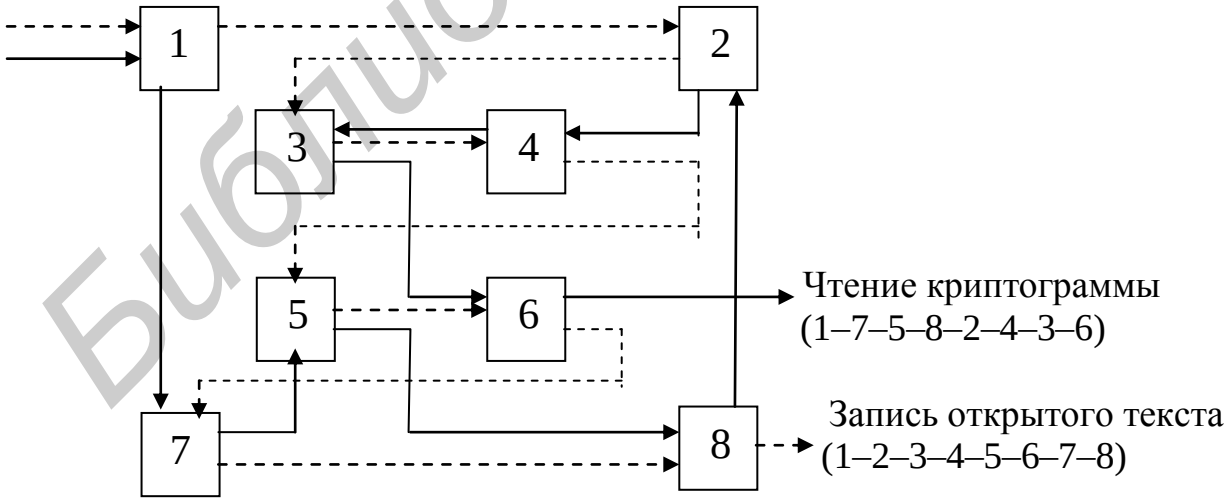

Рис. 3.2. Гамильтонов путь на графе

Шифротекст: «ШАОНИРФВИЕЕСЕП_РТОВЙАОНК».

Необходимо отметить, что для данного графа из восьми вершин можно предложить несколько маршрутов записи открытого текста и несколько гамильтоновых путей для чтения криптограмм.

Еще более сложные перестановки основаны на принципах, заложенных в логической игре «Кубик Рубика». При использовании такой схемы открытый текст записывается в ячейки граней куба по строкам. После осуществления заданного числа поворотов слоев куба считывание шифротекста осуществляется по столбцам. Сложность расшифрования в этом случае определяется числом ячеек на гранях куба и сложностью выполненных поворотов слоев куба. Перестановка, основанная на кубике Рубика, получила название *объемной (многомерной) перестановки*. Усовершенствованная схема такой перестановки, в которой наряду с открытым текстом перестановке подвергаются и функциональные элементы самого алгоритма шифрования, легла в основу секретной системы «Рубикон». В этой системе в качестве прообразов пространственных многомерных структур, на основании которых осуществляются перестановки, используются трехмерный куб и тетраэдр.

Основным недостатком методов перестановки является сохранение частотных свойств символов открытого текста в шифротексте.

Метод перемешивания

Метод перемешивания основан на совместном использовании методов замены (подстановки) и перестановки. При этом существенно нарушаются статистические связи шифротекста с открытым текстом. В стандартах шифрования часто применяются специальные меры, обеспечивающие расширение влияния каждого символа открытого текста на группу символов шифротекста [2]. В результате этого при замене любого одного символа открытого текста изменяется значительная группа символов шифротекста.

В практических шифрах используются два основных принципа Шеннона: *рассеивание* и *перемешивание*. ***Рассеивание*** – это распространение влияния одного знака открытого текста на множество знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. ***Перемешивание*** – это использование взаимосвязи статистических свойств открытого и шифротекста.

Шифр должен не только затруднять раскрытие, но и обеспечивать легкость зашифрования и расшифрования при известном секретном ключе. Поэтому принята идея использовать произведение простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемешивание. В таких составных шифрах в качестве элементарных составляющих чаще всего используются простые подстановки (замены) и перестановки [1].

3.2.2.3. Методы криптографии с открытыми ключами

Наиболее перспективными системами криптографической защиты информации являются системы с открытыми ключами [1]. В таких системах для

зашифрования данных используется один (открытый) ключ, а для расшифрования – другой (секретный). Первый ключ не является секретным и может быть известен всем пользователям системы, которые зашифровывают данные. Расшифрование данных с помощью известного ключа невозможно. Для расшифрования данных используется второй ключ, который является секретным. Ключ расшифрования не может быть определен из ключа зашифрования [3].

Структурная схема шифрования с открытым ключом (несимметричное шифрование) показана на рис. 3.3.

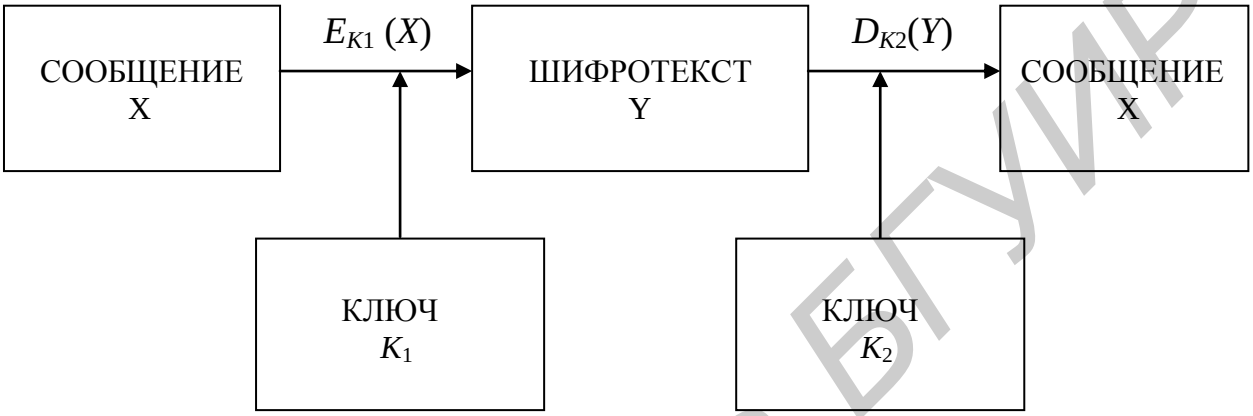

Рис. 3.3. Несимметричное шифрование

Криптосистема с открытым ключом должна содержать следующие элементы:

– рандомизированный алгоритм генерации открытого ключа K_1 и соответствующего ему секретного ключа K_2;

– алгоритм зашифрования, который по сообщению X, используя открытый ключ K_1, формирует шифротекст $Y = E_{K1}(X)$;

– алгоритм расшифрования, который по шифротексту Y, используя секретный ключ K_2, восстанавливает исходное сообщение $X = D_{K2}(Y)$.

Наиболее перспективным методом криптографической защиты информации с открытым ключом является алгоритм RSA (назван по начальным буквам фамилии его изобретателей – **R**ivest, **S**hamir и **A**dleman). При рассмотрении алгоритма RSA необходимо вспомнить некоторые математические термины.

Под *простым числом* понимают такое число, которое делится только на 1 и на само себя. *Взаимно простыми числами* называют такие числа, которые не имеют ни одного общего делителя, кроме 1. Под результатом операции $i \bmod j$ понимают остаток от целочисленного деления i на j.

Чтобы использовать алгоритм RSA, необходимо сначала сгенерировать открытый и секретный (закрытый) ключи, выполнив следующее:

– выбрать два очень больших простых числа p и q;

– определить n как результат умножения p на q ($n = pq$);

– выбрать большое случайное число d. Оно должно быть взаимно простым с числом, определяемым как результат умножения чисел $(p - 1)(q - 1)$;

– определить такое число e, для которого является истинным следующее соотношение: $ed \bmod ((p - 1)(q - 1)) = 1$;

– считать открытым ключом числа e и n, а секретным ключом – числа d и n.

Для того чтобы зашифровать данные по известному ключу $\{ e, n \}$, необходимо разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа M_i от 0 до $n - 1$.

Затем зашифровать текст, рассматриваемый как последовательность чисел M_i, выполнив вычисления $Y_i = M_i^e \bmod n$.

Чтобы расшифровать эти данные, используя секретный ключ $\{ d, n \}$, необходимо выполнить вычисления $M_i = Y_i^d \bmod n$. В результате будет получено множество чисел M_i, которое представляет собой исходный текст.

Пример 12. Открытый текст «ЕДА».

Для простоты будем использовать «маленькие» числа.

Выберем два простых числа $p = 3$ и $q = 11$.

Определим $n = 3 \circ 11 = 33$.

Найдем $(p - 1)(q - 1) = 20$.

Следовательно, в качестве секретного ключа d нужно выбрать любое число, которое является взаимно простым с числом 20, например $d = 3$.

Выберем значение открытого ключа e. В качестве такого числа может быть использовано любое число, для которого справедливо соотношение $(e \circ 3) \bmod 20 = 1$. Например, $e = 7$.

Таким образом, открытый ключ составляют числа $e = 7$ и $n = 33$, а секретный – числа $d = 3$ и $n = 33$.

Представим шифруемое сообщение как последовательность целых чисел в диапазоне 0–32, число которых не превышает $n = 33$. Тогда буква Е изображается числом 6, буква Д – числом 5, буква А – числом 1, а слово «ЕДА» представляется последовательностью цифровых эквивалентов (чисел) как 651.

Зашифруем сообщение, используя открытый ключ {7, 33}:

$$Y_1 = 6^7 \bmod 33 = 279936 \bmod 33 = 30;$$
$$Y_2 = 5^7 \bmod 33 = 78125 \bmod 33 = 14;$$
$$Y_3 = 1^7 \bmod 33 = 1 \bmod 33 = 1.$$

Шифротекст: «30 14 1».

Расшифруем сообщение «30 14 1», полученное в результате зашифрования по известному ключу, на основе секретного ключа {3, 33}:

$$M_1 = 30^3 \bmod 33 = 27000 \bmod 33 = 6;$$
$$M_2 = 14^3 \bmod 33 = 2744 \bmod 33 = 5;$$
$$M_3 = 1^3 \bmod 33 = 1 \bmod 33 = 1.$$

Таким образом, в результате расшифрования сообщения получено исходное сообщение «ЕДА» («651»).

Криптостойкость алгоритма RSA основывается на предположении, что исключительно трудно определить секретный ключ по известному, так как для этого необходимо решить задачу о существовании делителей целого числа. Данная задача до настоящего времени не имеет эффективного (полиноминального) решения.

3.3. Порядок выполнения работы

1. Изучить теоретическую часть работы.
2. Провести самопроверку теоретических знаний, ответив на поставленные вопросы.
3. Получить вариант задания на зашифрование и расшифрование текста.
4. Осуществить зашифрование и расшифрование текста соответствующим методом, используя необходимые табл. 3.9 и 3.10 и соответствующий алгоритм.
5. Провести проверку правильности результатов зашифрования и расшифрования текста.
6. Оформить отчет и защитить работу.

Таблица 3.9

Подстановка алфавита для шифрования моноалфавитной заменой

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Цифровой эквивалент	1	2	3	4	5	6	7	8	9	10	11	12
Буква	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Цифровой эквивалент	13	14	15	16	17	18	19	20	21	22	23	24
Буква	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_ (ПРОБЕЛ)			
Цифровой эквивалент	25	26	27	28	29	30	31	32	33			

Таблица 3.10

Подстановка алфавита для шифрования полиалфавитной заменой
(количество алфавитов шифротекста k = 3)

Алфавит открытого текста	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Алфавит шифро-текста	1	2	3	4	5	6	7	8	9	10	11	12
	34	35	36	37	38	39	40	41	42	43	44	45
	67	68	69	70	71	72	73	74	75	76	77	78
Алфавит открытого текста	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Алфавит шифро-текста	13	14	15	16	17	18	19	20	21	22	23	24
	46	47	48	49	50	51	52	53	54	55	56	57
	79	80	81	82	83	84	85	86	87	88	89	90
Алфавит открытого текста	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_ (ПРОБЕЛ)			
Алфавит шифро-текста	25	26	27	28	29	30	31	32	33			
	58	59	60	61	62	63	64	65	66			
	91	92	93	94	95	96	97	98	99			

Алгоритм зашифрования: О + К = Ш.
Если (О + К) > 33, то Ш = О + К – 33.
Если (О + К) ≤ 33, то Ш = О + К.
Алгоритм расшифрования: Ш – К = О.
Если (Ш – К) > 0, то О = Ш – К.
Если (Ш – К) ≤ 0, то О = 33 + (Ш – К).
О – открытый текст. К – ключ. Ш – шифротекст.

3.4. Описание программы для ЭВМ

Программа позволяет осуществлять проверку теоретических знаний студентов, выдавать варианты заданий и проверять правильность результатов зашифрования и расшифрования текста по всем вариантам заданий. Имя программы CRYPT.

3.5. Содержание отчета

1. Цель лабораторной работы.
2. Вариант задания.
3. Исходные тексты и задания по методам их зашифрования и расшифрования.
4. Подробные пояснения зашифрования и расшифрования текстов.
5. Выводы по работе.

Литература

1. Петраков, А. В. Основы практической защиты информации / А. В. Петраков. – М. : Радио и связь, 2000. – 368 с.

2. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М. : Изд-во стандартов, 1989. – 26 с.

3. Панасенко, С. П. Криптографические методы защиты информации для российских корпоративных систем / С. П. Панасенко, С. А. Петренко // Конфидент. – 2001. – №5.

Лабораторная работа №4

Исследование метода компьютерной стеганографии для защиты информации

4.1. Цель работы

Исследование метода замены младших бит, используемого в компьютерной стеганографии для защиты информации.

4.2. Теоретические сведения

4.2.1. Основные понятия, термины и определения компьютерной стеганографии

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. В отличие от криптографии, где противник точно может определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в открытые послания таким образом, чтобы было невозможным заподозрить существование самого встроенного послания [1, 2].

Таким образом, если цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений, то цель стеганографии – в скрытии самого факта существования секретного сообщения.

При необходимости оба способа могут быть объединены и использованы для повышения эффективности защиты информации.

Слово «*стеганография*» в переводе с греческого означает «тайнопись» («steganos» – секрет, тайна, «graphy» – запись). К ней относится большое число секретных средств связи, таких, как невидимые чернила, микрофотоснимки, условное расположение знаков, средства радиосвязи на плавающих частотах и т. д.

Развитие вычислительной техники и новых каналов передачи информации привело к появлению новых методов стеганографии, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Этот вид стеганографии получил название *компьютерной стеганографии*.

Компьютерная стеганография базируется *на двух основных принципах*.

Первый принцип заключается в том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери их функциональности в отличие от других типов данных, требующих абсолютной точности.

Второй принцип заключается в неспособности органов чувств человека различать незначительные изменения в цвете изображения или качестве звука.

Этот принцип особенно легко применять к изображению или звуку, несущему избыточную информацию.

Так как компьютерная стеганография является молодым направлением в области защиты информации и до недавнего времени не имела своей терминологии, то в 1996 г. было предложено использовать единую терминологию.

Стеганографическая система, или ***стегосистема*** – это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. При построении стегосистемы должны учитываться следующие положения:

– методы скрытия должны обеспечивать аутентичность и целостность информации, в которой скрывается сообщение;

– противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержания скрытого сообщения;

– если противник каким-то образом узнает о факте существования скрытого сообщения, то это не должно позволить ему извлечь скрытую информацию из других данных до тех пор, пока ключ хранится в тайне;

– потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания скрытых сообщений.

Структурная схема стегосистемы представлена на рис. 4.1.

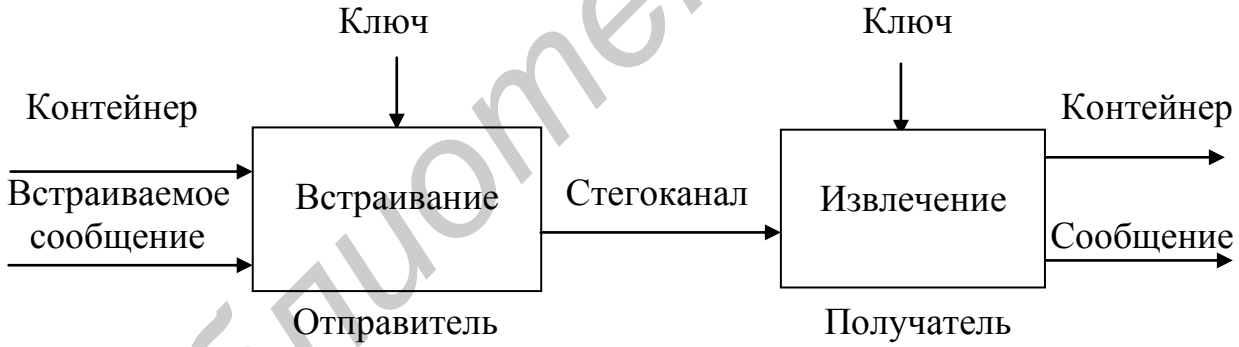

Рис. 4.1. Структурная схема стегосистемы

Сообщение – это любая информация, подлежащая скрытой передаче. В качестве сообщения может использоваться любой вид информации: текст, изображение, аудиосигнал.

Встроенное (скрытое) сообщение – это сообщение, встроенное в контейнер.

Контейнер – это любая информация, предназначенная для скрытия сообщения. Выбор вида контейнера оказывает существенное влияние на надежность стегосистемы и возможность обнаружения факта передачи скрытого сообщения. По размеру (протяженности) контейнеры можно разделить на два типа: *непрерывные (потоковые)* и *ограниченной (фиксированной) длины*.

Особенностью ***потокового контейнера*** является то, что невозможно определить его начало и конец. В таком контейнере биты информации, используемые для скрытия сообщения, включаются в общий поток в реальном масштабе времени и выбираются с помощью специального генератора, задающего расстояния между ними. В непрерывном потоке данных самая большая трудность для получателя – определить, когда начинается скрытое сообщение. При наличии в потоковом контейнере сигналов синхронизации или границ пакета, скрытое сообщение начинается сразу после одного из них. В свою очередь, для отправителя сообщения возможны проблемы, если он не уверен в том, что поток контейнера будет достаточно длинным для размещения всего сообщения.

При использовании ***контейнера ограниченной длины*** отправитель заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности. С другой стороны, такие контейнеры имеют ограниченный объем и встраиваемое сообщение иногда может не поместиться в файл-контейнер. Другой недостаток заключается в том, что расстояния между скрывающими битами равномерно распределены между наиболее короткими и наиболее длинными заданными расстояниями, в то время как истинный случайный шум будет иметь экспоненциальное распределение длин интервала. При необходимости можно задать псевдослучайные экспоненциально распределённые числа, однако этот путь наиболее трудоемкий. На практике чаще всего используются контейнеры ограниченной длины как наиболее распространенные и доступные.

Возможны следующие варианты контейнеров:

– контейнер генерируется самой стегосистемой. Такой подход называется ***конструирующей стеганографией***;

– контейнер выбирается из некоторого множества генерируемых стегосистемой контейнеров. Такой подход называется ***селектирующей стеганографией***;

– контейнер поступает извне стегосистемы. Такой подход называется ***безальтернативной стеганографией***.

В зависимости от вида информации, используемой для встраивания сообщений, контейнеры могут быть визуальные, звуковые и текстовые.

Визуальный контейнер представляет собой картинку или фотографию, в которой для встраивания сообщений используются небольшие изменения яркости заранее определенных точек растра изображения.

Звуковой контейнер представляет собой речевой или музыкальный сигнал, в котором для встраивания сообщений используются младшие биты аудиосигнала, что практически не отражается на качестве звука.

Текстовый контейнер представляет собой текстовый файл, подготовленный к печати на принтере, в котором для встраивания сообщений используются небольшие изменения стандартов печати (расстояния между буквами, словами и строками, размеры букв, строк и др.).

При выборе того или иного вида контейнера необходимо иметь в виду, что при увеличении объема встраиваемого сообщения снижается надежность

стегосистемы (при неизменном размере контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемого сообщения.

Пустой контейнер – это контейнер без встроенного сообщения.

Заполненный контейнер, или ***стегоконтейнер*** – это контейнер, содержащий встроенную информацию.

Стеганографический канал (стегоканал) – это канал передачи скрытого сообщения.

Ключ (стегоключ) – это секретный ключ, необходимый для скрытия сообщения. В зависимости от количества уровней защиты в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией по типу стегоключа стегосистемы подразделяются на два вида: *с секретным ключом* и *с открытым ключом*.

В стегосистеме ***с секретным ключом*** используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме ***с открытым ключом*** для встраивания и извлечения сообщения используются разные ключи, различие которых состоит в том, что с помощью вычислений невозможно определить один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи.

Любая стегосистема должна отвечать следующим требованиям:

– свойства контейнера должны быть модифицированы таким образом, чтобы изменение невозможно было выявить при визуальном контроле;

– стегосообщение должно быть устойчиво к искажениям, которые могут иметь место при его передаче, включая и различные трансформации (уменьшение, увеличение, преобразование в другой формат, сжатие без потери информации, сжатие с потерей информации и т. д.);

– для сохранения целостности встраиваемого сообщения необходимо использовать коды с исправлением ошибок;

– для повышения надежности встраиваемое сообщение должно быть продублировано [2].

4.2.2. Методы компьютерной стеганографии

4.2.2.1. Классификация методов

Методы компьютерной стеганографии можно разделить в целом на два вида:

– методы, основанные на избыточности визуальной и аудиоинформации;

– методы, основанные на использовании специальных свойств компьютерных форматов.

Методы, основанные на избыточности визуальной и аудиоинформации, для скрытия информации используют младшие разряды цифровых отсче-

тов цифрового изображения и звука, которые содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации.

Преимуществом этих методов является возможность скрытой передачи большого объема информации и возможность защиты авторского права путем создания скрытого изображения товарной марки, регистрационного номера и т. п.

Недостаток метода состоит в том, что за счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик.

Методы, основанные на использовании специальных свойств компьютерных форматов, делятся на:

– методы использования зарезервированных для расширения полей компьютерных форматов данных;

– методы специального форматирования текстовых файлов;

– методы скрытия в неиспользуемых местах компакт-дисков;

– методы использования имитирующих функций;

– методы удаления идентифицирующего файл заголовка.

Методы использования зарезервированных для расширения полей компьютерных форматов данных основаны на том, что многие мультимедийные форматы имеют поля расширения, которые заполняются нулевой информацией и не учитываются программой. В эти поля и записывается скрываемая информация.

Методы специального форматирования текстовых файлов в свою очередь делятся на:

– методы использования известного смещения строк, слов, предложений, абзацев;

– методы выбора определенных позиций букв;

– методы использования специальных свойств, не отображаемых на экране полей форматов.

Методы использования известного смещения строк, слов, предложений, абзацев основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами.

Методы выбора определенных позиций букв используют принцип *нулевого шифра*. *Акростих* является частным случаем этого метода, когда, например, начальные буквы каждой строки образуют сообщение.

Методы использования специальных свойств, не отображаемых на экране полей форматов, основаны на использовании специальных скрытых полей для организации сносок и ссылок, например использование черного шрифта на черном фоне.

Методы скрытия в неиспользуемых местах компакт-дисков основаны на том, что скрываемая информация записывается в обычно неиспользуемых местах дисков (например в нулевой дорожке).

Методы использования имитирующих функций основаны на генерации осмысленного текста, скрывающего информацию.

Методы удаления идентифицирующего файл заголовка основаны на том, что скрываемая информация шифруется и в нем удаляется идентифицирующий заголовок, который заранее известен пользователю.

Преимуществом этих методов является простота их реализации, а недостатком – низкая степень скрытности и передача небольших объемов информации [1].

4.2.2.2. Метод замены младших бит

Одним из наиболее распространенных методов стеганографии, использующих психофизические особенности человека, является метод замены младших бит информации, или LSB-метод (**L**east **S**ignificant **B**its). Распространенность этого метода обусловлена функциональной простотой, большой емкостью и высокой степенью защищенности от стегоанализа [3].

Суть метода состоит в замене нескольких младших бит в байтах данных. Он применяется в графических файлах, использующих для формирования цвета каждого элемента изображения (пиксела) значения некоторых составляющих (например, значения составляющих основных цветов – красного, зеленого и синего), или в звуковых файлах, использующих для формирования звука значения дискретизированных амплитуд сигнала.

При оцифровке изображения или звука всегда существует погрешность дискретизации, которая обычно находится на уровне младшего значащего бита. Это значит, что фактически неизвестно, что будет стоять в младшем значащем разряде цифрового представления цвета или звука. Поэтому при замене только самого младшего значащего бита говорить о каком-либо искажении изображения или звука не имеет смысла. Однако при замене только одного младшего бита такой метод имеет достаточно малую емкость, порядка 10 % от объема файла-контейнера, поэтому на практике используют замену более одного бита.

Рассмотрим использование данного метода на примере формата BMP (BitMaP), хранящего изображение в True Color (естественных цветах) и являющегося основным форматом растровой графики для системы Windows. Такие графические файлы имеют расширение BMP, однако некоторые из них могут иметь расширение RLE (**LE**nth enco**R**ding), что указывает на то, что произведено сжатие растровой информации, хранящейся в файле BMP-формата.

В файлах BMP информация о цвете каждого пиксела задается тремя байтами (1 байт = 8 битам). Каждый байт содержит одну из трех составляющих цвета RGB: красную (**R**ed), зеленую (**G**reen) и синюю (**B**lue). Интенсивность каждой составляющей лежит в пределах от 0 до 255, т. е. каждая составляющая имеет 256 оттенков. Варьируя интенсивность каждой составляющей, можно

изменять цвет от черного, когда интенсивность всех составляющих равна нулю, до белого, когда интенсивность всех составляющих максимальна. При промежуточных комбинациях значений составляющих будут получаться различные хроматические (цветные) цвета и оттенки.

Максимальное количество возможных цветов составляет более 16 млн. Однако следует иметь в виду, что глаз человека способен различать только около 4 тыс. цветов. Для кодирования такого количества цветов достаточно всего 4 бита ($\log_2 \sqrt[3]{4000} \approx 4$).

Размер файла изображения напрямую зависит от числа пикселов и точности представления цвета. Так, 8-разрядное (1 байт) цветное изображение размером 640×480 пикселов будет занимать 300 Кбайт (640×480×1 байт), а 24-разрядное изображение размером 1024×768 пикселов займет уже 2,25 Мбайт (1024×768×3 байт); (1 Кбайт = 2^{10} = 1024 байт; 1 Мбайт = 2^{10} = 1024 Кбайт).

Степень упаковки несущего изображения зависит от того, сколько бит младших разрядов в одном байте используется для скрытия информации.

При использовании 1 бита на байт графической информации, т. е. 3 бита на пиксел, для упаковки одного скрываемого байта используется 3 пиксела. Степень упаковки составляет 1/9 (скрываемые биты представлены единицей и выделены полужирным шрифтом):

R (1 байт)	G (1 байт)	B (1 байт)	
0000000**1**	0000000**1**	0000000**1**	1 пиксел (3 байта)
0000000**1**	0000000**1**	0000000**1**	1 пиксел (3 байта)
0000000**1**	0000000**1**	00000001	1 пиксел (3 байта)

При использовании 2 бит на байт графической информации, т. е. 6 бит на пиксел, для упаковки одного скрываемого байта используются 2 пиксела. Степень упаковки составляет 1/6:

R (1 байт)	G (1 байт)	B (1 байт)	
0000000**11**	0000000**11**	0000000**11**	1 пиксел (3 байта)
0000000**11**	00000000	00000000	1 пиксел (3 байта)

При использовании 3 бит на байт графической информации можно упаковать 9 бит на пиксел, но для скрытия одного байта используется 8 бит на пиксел. Степень упаковки составляет 1/3:

R (1 байт)	G (1 байт)	B (1 байт)	
0000000**11**	0000000**111**	0000000**111**	1 пиксел (3 байта)

При использовании 4 бит на байт графической информации можно упаковать 12 бит на пиксел, но для скрытия одного байта используется 8 бит на пиксел. Степень упаковки составляет 1/3:

R (1 байт)	G (1 байт)	B (1 байт)	
0000**1111**	0000**1111**	00000000	1 пиксел (3 байта)

Если для записи скрываемой информации использовать 4 младших бита на каждый байт блока данных, то максимальное искажение цвета при этом составит 6,25 % ($2^4/2^8 = 16/256 = 0{,}0625$). При использовании 24-разрядного изображения, которое широко применяется для описания цвета страниц в Internet в формате HTML (**H**yper-**T**ext **M**arkup **L**anguage), это искажение будет еще меньше и составит всего $9{,}53\cdot10^{-5}$ % ($2^4/2^{24} = 16/16777216 = 0{,}953\cdot10^{-6}$).

Такие искажения в изображении будут практически незаметны для глаза. Однако при скрытии информации в графическом изображении необходимо учитывать, что чувствительность глаза к различным составляющим цвета неодинакова. Так, к зеленому спектру глаз более чувствителен, чем к красному и синему. Поэтому для практического использования данного метода рекомендуется скрывать в красной и синей составляющей по 3 бита, а в зеленой составляющей 2 бита информации. В этом случае в одном пикселе изображения может храниться один байт скрываемой информации и ее объем можно определить по формуле

$$V = W \cdot H, \qquad (4.1)$$

где W – ширина изображения в пикселах;

H – высота изображения в пикселах.

Полезная емкость при этом составляет порядка 30 %.

Следует отметить, что реально искажения изображения будут еще меньше, так как меняются только те биты, которые не совпадают с битами скрываемой информации. Так, для скрытия девяти бит данных, например 101101101, в 24-разрядном изображении необходимо изменить максимум 3 пиксела (9 байт). Пусть 3 пиксела 24-разрядного изображения представлены в следующем виде:

R (1 байт)	G (1 байт)	B (1 байт)	
10010101	00001101	11001001	1 пиксел (3 байта)
10010110	00001111	11001010	1 пиксел (3 байта)
10011111	00010000	11001011	1 пиксел (3 байта)

Меняя младший разряд слева направо и сверху вниз, получаем следующий результат (измененные разряды выделены полужирным шрифтом):

R (1 байт)	G (1 байт)	B (1 байт)	
10010101	0000110**0**	11001001	1 пиксел (3 байта)
1001011**1**	0000111**0**	1100101**1**	1 пиксел (3 байта)
10011111	00010000	11001011	1 пиксел (3 байта)

Таким образом, для скрытия 9 бит данных потребовалось заменить всего 4 бита только в 2 пикселах исходного изображения, что составляет менее 50 % младших разрядов, используемых для этой цели.

Такой же метод можно использовать и для скрытия информации в черно-белых изображениях.

4.2.2.3. Метод замены цветовой палитры

Метод основан на использовании специфических особенностей формата файла-контейнера и предназначен для скрытия текстовой информации в графических файлах, использующих цветовые палитры. Такими файлами являются, например, файлы BMP, PCX и GIF [3].

Палитра представляет собой некоторое число триад байт (не более 256), которые описывают цвет точки по тому же принципу, что и в файлах True Color. За палитрой следует массив байт, каждый из которых описывает одну точку изображения и содержит в себе номер цвета в палитре.

При использовании этого метода в качестве контейнера следует выбирать файлы, содержащие некоторый цвет в избытке. Например, это могут быть схемы, рисунки, текст черного цвета на белом фоне. Такое сочетание цветов является оптимальным для реализации данного метода, однако можно использовать и другие цвета.

В качестве примера возьмем изображение, содержащее черный рисунок на белом фоне. Фон занимает большую часть изображения, т. е. имеется избыток белого цвета.

Вначале создается алфавит, содержащий символы, которые используются в файле сообщения, например все 33 буквы русского алфавита от А до Я, цифры от 0 до 9, специальные знаки и знаки пунктуации – всего 51 символ:

Код	0	1	2	3	4	…	49	50
Символ	А	Б	В	Г	Д	…	%	;

Далее проводится замена цветов палитры. Для этого первому 51 цвету палитры назначается черный цвет (цвет рисунка). Следующему 51 цвету палитры назначается белый цвет (цвет фона). Если рисунок содержит 3–5 цветов, то

можно переназначить следующие группы по 51 цвету в соответствующие цвета. Тогда в нашем случае измененная палитра цветов будет иметь в шестнадцатеричном представлении следующий вид:

Черный цвет

Код	0	1	2	…	49	50
Цвет	00 00 00	00 00 00	00 00 00	…	00 00 00	00 00 00

Белый цвет

Код	51	52	53	…	100	101
Цвет	FF FF FF	FF FF FF	FF FF FF	…	FF FF FF	FF FF FF

Черный цвет в данном случае имеет нулевой уровень, что для одного байта соответствует 0 в десятичной системе счисления, 00000000 в двоичной и 00 в шестнадцатеричной, а белый цвет имеет уровень 255, что соответствует 255 в десятичной, 11111111 в двоичной и FF в шестнадцатеричной системе счисления. Для скрытия информации берется первая точка изображения, анализируется ее принадлежность к определенной цветовой группе, например к группе черного цвета, затем этой точке присваивается код текущего символа из файла-сообщения с учетом выбранной цветовой группы. Например, для символа Б черной точке будет назначен цвет с кодом 1, а белой точке – цвет с кодом 52.

Объем скрываемой этим методом информации определяется по формуле (4.1). Метод является самым емким для скрытия информации в графических файлах и позволяет оставлять изображение без изменений. Его можно использовать для любого алфавита с числом символов не более 128.

Однако информация, скрытая этим методом, легко выявляется статистическим анализом, например просмотром гистограммы графического файла в редакторе Photoshop.

4.2.2.4. Метод сортировки цветовой палитры

Метод основан как на использовании особенностей формата контейнера, так и на использовании психофизических особенностей восприятия цвета человеком. При этом методе в качестве контейнера используются файлы с индексированными цветами, содержащими монохромное (обычно градации серого) изображение. Суть метода заключается в специальной предварительной подготовке файла-контейнера [3].

Палитра файла упорядочивается таким образом, чтобы цвета с соседними номерами минимально отличались друг от друга и равномерно изменялись от черного цвета для нулевого номера до белого цвета для 255-го номера. После этого скрываемая информация заносится в младшие разряды точек изображения. То есть искажаются не сами цвета, а номера цветов, но благодаря предва-

рительно отсортированной палитре цвет точки заменяется на похожий, который практически невозможно отличить от исходного из-за их малого различия.

Информация, скрытая данным методом, также легко выявляется средствами программного анализа.

Описанные выше методы не увеличивают размер файла-контейнера, но их применение ограничено растровыми форматами, использующими сжатие информации без потери качества, например RLE- или LZW-сжатие.

4.2.2.5. Методы компьютерной стеганографии в JPEG-файлах

Цветные изображения, представленные в цифровой форме, достаточно велики и занимают большой объем памяти (до нескольких мегабайт). Поэтому для их сжатия существует ряд методов. Так, форматы BMP и GIF используют алгоритмы сжатия без потерь, обеспечивающие точное восстановление исходного изображения. Существуют также алгоритмы сжатия с потерей (искажением) информации. Таким примером может служить формат JPEG (**J**oint **P**hotographic **E**xperts **G**roup) [4].

В общем случае методы обработки (сжатия) изображений можно разделить на две группы: *непосредственные* и *спектральные*. При использовании ***непосредственных методов*** обработке подвергаются сами исходные изображения (пикселы). ***Спектральные методы*** основаны на применении дискретных унитарных преобразований Фурье, Адамара и др. При этом обрабатывается не исходное изображение, а соответствующие коэффициенты преобразования.

Алгоритм сжатия JPEG состоит из следующих этапов:

– преобразование изображения в оптимальное цветовое пространство;

– субдискретизация компонентов цветности посредством их усреднения;

– применение дискретных косинусных преобразований (разновидность преобразований Фурье) для уменьшения избыточности данных изображения;

– квантование коэффициентов преобразования с применением весовых функций, оптимизированных с учетом физиологических особенностей зрения;

– кодирование данных изображения (результирующих коэффициентов) для удаления избыточности информации с применением алгоритма Хаффмана.

Возможность использования файловых форматов, построенных по схеме сжатия JPEG, для скрытия информации обусловлена их широким распространением при хранении и передаче графических изображений, в частности в сети Internet.

В JPEG-файлах могут использоваться следующие методы скрытия информации:

– дописывание данных скрываемой информации в конец файла;

– скрытие информации в косвенных данных файла;

– скрытие информации с использованием таблиц квантования;

– скрытие информации между блоками данных файла.

Методы скрытия информации в JPEG-файлах обладают достаточно высокой степенью защищенности от стегоанализа, так как возможность варьирова-

ния качества сжатого изображения в широком диапазоне не позволяет легко установить, являются ли возникающие в результате сжатия погрешности следствием скрытия данных или следствием использования высоких коэффициентов квантования.

4.2.2.6. Компьютерная стеганография в PRN-файлах

Файлы печати цветных графических изображений на принтерах, поддерживающих точечный вывод, содержат описание битовой карты отпечатка.

Процедура печати предполагает получение битовых карт отпечатков, кодирование их на языке управления принтером (PRN-файлы) и пересылку на принтер для непосредственного получения отпечатка. В этом случае в качестве контейнера стегосистемы может быть использована битовая карта отпечатка [5].

Структурная схема стегосистемы для скрытия информации в битовых картах приведена на рис. 4.2.

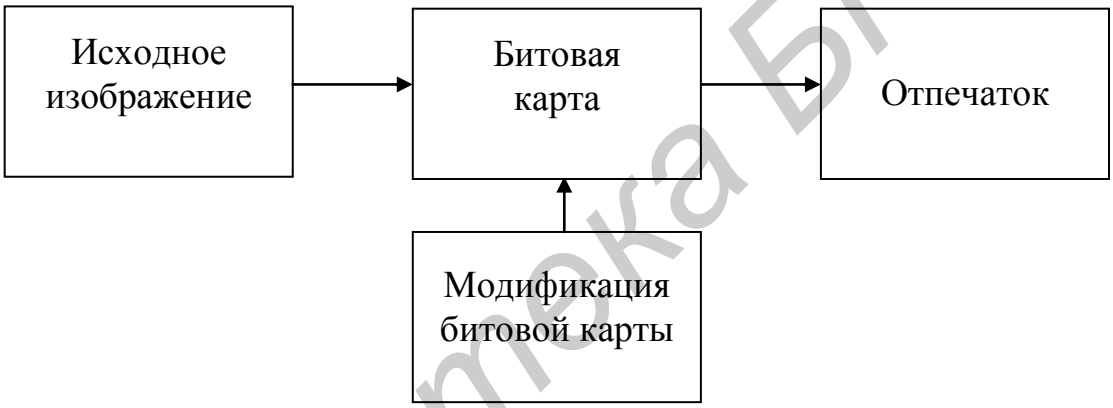

Рис. 4.2. Структурная схема стегосистемы для скрытия информации в битовых картах

До получения отпечатка битовая карта модифицируется таким образом, чтобы не позволить выявить наличие встроенного сообщения визуальным контролем самой карты и соответствующего ей отпечатка. Для скрытия информации в этом случае применяется один из методов компьютерной стеганографии, основанный на избыточности данных. В битовых картах избыточность данных создается за счет большой вариантности взаимного расположения цветных пятен внутри одного и того же единичного фрагмента отпечатка изображения. Количество битовых карт равно количеству первичных красителей принтера. Каждая битовая карта, соответствующая одному первичному красителю принтера, может быть представлена прямоугольной матрицей с нулевыми и единичными компонентами, у которой 1 соответствует наличию красителя в соответствующей позиции, а 0 – его отсутствию. Совокупность битовых матриц с соответствующими значениями 0 и 1 соответствует конкретному отпечатку. Градации цвета на отпечатке воспроизводятся с помощью подмножеств (единич-

ных фрагментов) битовой карты – растровых точек с различной плотностью красочных пятен. Для сохранения правильного градационного воспроизведения при печати и, следовательно, для скрытия факта встраивания конфиденциальной информации, модификация битовых карт отпечатков не должна приводить к изменению плотности красочных пятен (дотов) внутри растровых точек. Вариантность взаимного расположения дотов внутри растровых точек и является ресурсом, который используется для организации стегосистемы в PRN-файлах.

Среди всех возможных узоров, отвечающих некоторой плотности заполнения растровой точки красочными пятнами, для целей стеганографии можно пользоваться регуляризованными, не создающими муара растрами, т. е. такими, доты которых распределены достаточно равномерно по площади растровой точки.

Следует отметить, что размеры растровой точки жестко не определены и могут варьироваться в разумных пределах. Например, при разрешении 300 dpi (**d**ot **p**er **i**nch) можно использовать квадратную матрицу размерами 6x6, 7×7, 8×8 и 9×9. Форма растровой точки (прямоугольная, круглая, овальная и т. д.) также может варьироваться при встраивании информации.

Получить отпечатки со скрытой информацией можно только с помощью специального программного обеспечения, так как при печати драйвер принтера, используя фирменную технологию растрирования, «размоет» те символы скрытой информации, которые по своим размерам сравнимы с размерами растровой точки. Для извлечения скрытой информации необходимо использовать программу и алфавитные таблицы.

В заключение можно отметить, что методы компьютерной стеганографии, использующие особенности форматов файлов-контейнеров, невозможно выявить путем субъективного анализа (просмотром, прослушиванием), но достаточно легко обнаружить, используя различные программные средства стегоанализа. В то же время методы, основанные на использовании психофизических особенностей человека, невозможно выявить простым программным анализом на предмет соответствия формату и достаточно сложно, а в некоторых случаях и невозможно, обнаружить путем субъективного анализа.

4.3. Порядок выполнения работы

1. Изучить теоретическую часть работы.
2. Провести самопроверку теоретических знаний, ответив на поставленные вопросы.
3. Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения отдельных цветов файла-контейнера.
4. Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения комбинации цветов файла-контейнера.

5. Исследовать влияние количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения различных цветов в многокомпонентной цветовой картине файла-контейнера.

6. На основании результатов, полученных в пп. 3–5, добиться наилучшего качества многоцветной картины файла-контейнера при скрытии в нем информации.

7. Оформить отчет и защитить работу.

4.4. Описание программы для ЭВМ

Программа позволяет осуществлять проверку теоретических знаний студентов и проводить исследования влияния количества заменяемых младших бит составляющих цвета на качество изображения файла-контейнера при скрытии в нем информации методом замены младших бит, с использованием профессиональной программы компьютерной стеганографии. Имя программы STEGAN.

4.5. Содержание отчета

1. Цель лабораторной работы.

2. Результаты исследований влияния количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения отдельных цветов файла-контейнера с указанием конкретных значений бит и видов используемых файлов-контейнеров.

3. Результаты исследований влияния количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения комбинации цветов файла-контейнера с указанием конкретных значений бит и видов используемых файлов-контейнеров.

4. Результаты исследований влияния количества заменяемых младших бит для различных составляющих RGB по отдельности и в их комбинации на качество воспроизведения различных цветов в многокомпонентной цветовой картине файла-контейнера с указанием конкретных значений бит и вида используемой многокомпонентной цветовой картине.

5. Результаты исследований по п. 6 порядка выполнения работы с указанием конкретных значений бит и вида используемой многоцветной картины.

6. Выводы по работе.

Литература

1. Петраков, А. В. Защита абонентского телетрафика / А. В. Петраков, В. С. Лагутин. – М. : Радио и связь, 2001. – 504 с.

2. Генне, О. В. Основные положения стеганографии / О. В. Генне // Конфидент. – 2000. – №3.

3. Кустов, В. Н. Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федчук // Конфидент. – 2000. – №3.

4. Быков, С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии / С. Ф. Быков // Конфидент. – 2000. – №3.

5. Архипов, О. П. Стеганография в PRN-файлах / О. П. Архипов, П. О. Архипов, З. П. Зыкова // Конфидент. – 2002. – №2.

Св. план 2015, поз. 6

Учебное издание

МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

В двух частях

Часть 1

Алефиренко Виктор Михайлович

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПОСОБИЕ

Редактор *Е. И. Герман*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Д. Степусь*

Подписано в печать 01.09.2015. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 4,07 . Уч.-изд. л. 4,1. Тираж 100 экз. Заказ 1.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6