

процессор компьютера; возможна также установка на одном компьютере нескольких аппаратных шифраторов, что еще более повышает скорость обработки информации (это преимущество присуще шифраторам для шины PCI);

- использование парафазных шин в архитектуре шифрпроцессора исключает угрозу сня-

тия ключевой информации по возникающим в ходе криптографических преобразований колебаниям электромагнитного излучения в цепях “земля – питание” микросхемы.

Сравнительные характеристики персональных шифраторов приведены в таблице 1.

Таблица 1. Сравнительные характеристики персональных шифраторов

Персональный шифратор (ПШ)	Разработчик	Алгоритм шифрования	Назначение	Носитель ключевой информации	Примечание
Устройство защиты информации Шипка-1.5	ОКБ “САПР”	ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94	гарантированная защита информации и информационных технологий	микропроцессор	защищенная энергонезависимая память до 2 Мб
ПШ, встроенный в специальный сотовый телефон SMP-Атлас	ФГУП “НТЦ “Атлас” + концерн “Гудвин”	ГОСТ 28147-89	гарантированная защита информации, передаваемой по сетям GSM	русская интеллектуальная карта РИК (микросхема КБ5004ВЕ1)	персональный шифратор встроен в мобильный радиотелефон
ПШ, встроенный в Крипто Смарт Телефон	ЗАО “АНКОРТ”	симметричный, 256 бит	гарантированная защита информации, передаваемой по сетям GSM	шифропроцессор на основе TMS VC 5416	персональный шифратор встроен в мобильный радиотелефон
Персональный идентификатор ruToken RF	ЗАО “Актив”	ГОСТ 28147-89	хранение ключевой информации, контроль доступа к ресурсам ПК и в помещении	USB-брелок	полнофункциональный аналог смарт-карты + радиочастотная метка

ЗАВИСИМОСТЬ ПОЛЕЗНОЙ ПРОПУСКНОЙ СПОСОБНОСТИ ОТ РАЗМЕРА КАДРА ДЛЯ СЕТИ СТАНДАРТА ETHERNET

Лукьянов С.А., Ховансков С.А., Серогодский Д.И., Горягина Т.М., Котегов М.Г.
Южный федеральный университет,
Таганрогский технический институт
Таганрог, Россия

Технология Fast Ethernet 100 Мбит/с на витой паре поддерживает полезную и полную пропускную способность. Полезная пропускная способность – скорость передачи полезной информации, объем которой всегда несколько меньше полной передаваемой информации, так как каждый передаваемый кадр содержит служебную информацию, необходимую для его доставки

Максимальный размер кадра Ethernet составляет 1526 байт (12208 бит), минимальный – 72 байт (576 бит). При частоте передачи 10 МГц время передачи пакета минимальной длины составляет 57,6 мс. Каждый кадр начинается с преамбулы длиной 7 байт. Следом за преамбулой идет стартовый байт. Далее кадр содержит два 6-байтных поля адреса – получателя и отправителя.

Поле длины кадра определяет длину поля данных (от 0 до 1500 бит) и состоит из двух байтов. Однако, ввиду ограничений на минимальную длину кадра, поле данных не может быть короче 46 байт. Если же объем передаваемых данных меньше, то поле данных дополняется до минимального размера заполняющими битами. Заканчивается кадр всегда контрольной последовательностью.

Рассчитаем теоретическую полезную пропускную способность Fast Ethernet. Служебная информация в кадрах Ethernet постоянно 18 байт, а размер поля данных кадра меняется от 46 до 1500 байт. Размер кадра может меняться от $46 + 18 = 64$ байт до $1500 + 18 = 1518$ байт. Поэтому для кадра минимальной длины полезная информация составляет всего лишь $46 / 64 \approx 0,72$ от общей передаваемой информации, а для кадра максимальной длины $1500 / 1518 \approx 0,99$ от общей информации.

Зная частоту следования кадров f и размер полезной информации V_n в байтах, переносимой каждым кадром, можно рассчитать полезную пропускную способность сети:

$$P_n(\text{бит/с}) = V_n \cdot 8 \cdot f.$$

Для кадра минимальной длины (46 байт) теоретическая полезная пропускная способность

равна $P_{\text{ит1}} = 148\,810$ кадр/с = 54,76 Мбит/с, что составляет лишь немногим больше половины от общей максимальной пропускной способности сети.

Для кадра максимального размера (1500 байт) полезная пропускная способность сети равна $P_{\text{ит2}} = 8127$ кадр/с = 97,52 Мбит/с.

Таким образом, в сети Fast Ethernet полезная пропускная способность может меняться в зависимости от размера передаваемых кадров от 54,76 до 97,52 Мбит/с.

АНАЛОГО-ЦИФРОВЫЕ ПРЕОБРАЗОВАТЕЛИ НА ОСНОВЕ ИЗБЫТОЧНЫХ СИСТЕМ СЧИСЛЕНИЯ

Серогодский Д.И., Трунов И.Л., Горягина Т.М.,
Котегов М.Г., Лукьянов С.А.
*Южный федеральный университет,
Таганрогский технический институт
Таганрог, Россия*

Избыточность избыточной системы счисления проявляется в возможности представления чисел множеством кодовых комбинаций. Данное обстоятельство позволяет при наличии отклонений весов разрядов в АЦП и ЦАП на основе избыточной системы счисления получать неразрывную характеристику кодирования, что невозможно для двоичного кода.

Возможность появления разрывов передаточной характеристика – один из наиболее существенных недостатков двоичных неизбыточных преобразователей информации. Возникают указанные разрывы из-за несоответствия реальных

весов разрядов преобразователя информации требуемым значениям.

Числовой ряд Фибоначчи имеет вид 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ... в которой каждое число равно сумме двух предыдущих. Если i -е число Фибоначчи в последовательности обозначить через F_i , тогда закон построения числовой последовательности можно задать с помощью следующей рекуррентной формулы:

$$F_i = F_{i-1} + F_{i-2}.$$

«Коды Фибоначчи» и «коды золотой пропорции» и вытекающая из них компьютерная арифметика обладают «естественной» избыточностью, которая может быть использована для целей контроля разнообразных преобразований информации в компьютерах. Например, можно представить некоторую гипотетическую компьютерную сеть, в которой вся информация кодируется в виде натуральных чисел, представленных в коде золотой пропорции. У этого кода отсутствует избыточность. Эта избыточность проявляется себя в свойстве «множественности» представлений одного и того же числа. Например, число 19 в коде Фибоначчи имеет и другие кодовые представления: $19 = 1001101 = 1010001 = 1010010 = 0111101$. Входной сигнал величиной от 5 до 7 единиц может быть представлен как с участием, так и без участия 5-го разряда преобразователя информации.

Указанная многозначность представления информации позволяет сохранить непрерывность передаточной характеристики преобразователя информации и при наличии определённых отклонений весов разрядов.

Филологические науки

ПОИСК И ОБРАБОТКА ИНФОРМАЦИИ НА БАЗЕ МУЛЬТИЛИНГВИСТИЧЕСКИХ ТЕЗАУРУСОВ

Зеленков П.В., Ковалев И.В., Карасева М.В.,
Рогов С.С.

*Сибирский государственный аэрокосмический
университет
Красноярск, Россия*

В настоящее время разработано множество моделей и алгоритмов для представления информации в информационных системах. Частным случаем подобных систем являются информационно-управляющие системы, корпоративные информационные системы и системы поддержки принятия решения. Однако большинство моделей распределенных систем строятся на основе одноязычного представления информации или учитывают многоязычность неявно.

Одним из перспективных направлений является применение предметных словарей или тезаурусов. Необходимо отметить, что в современных системах подобные словари-тезаурусы очень редко встречаются представленными в мультILINGВИСТИЧЕСКОЙ частотной реализации.

Авторами статьи в рамках предлагаемых моделей применяются тезаурусы, выполненные на основе мультILINGВИСТИЧЕСКОЙ технологии для проведения поисковой процедуры в информационных системах.

Авторский подход направлен на решение проблемы многоязычного представления информации в информационно-управляющих системах. В современных условиях даже небольшие корпоративные информационные системы работают в мультILINGВИСТИЧЕСКОМ режиме.

В работе программный модуль выполняет основную работу по поиску, ранжированию и определению уровня релевантности документов путем использования метапоисковых мультILINGВИСТИЧЕСКИХ алгоритмов обработки информации. Для этого необходимо определить параметры процесса поиска. К ним относятся функции выбора предметной области и настройки языковых множеств, в рамках которых необходимо производить поиск.

Кроме того, необходимо отдельно показать возможность работы со строкой поиска информации, как в Internet, так и корпоративной сети. Согласно предлагаемому авторами подходу