Лабораторное занятие № 2

Тема №2. Криптографические методы защиты информации.

Алгоритмы шифрования

Цель занятия: освоить основы криптографических методов защиты информации. Алгоритмы шифрования.

Учебные вопросы

3.1. Криптографические методы защиты информации.

3.2. Алгоритмы шифрования

3.1. Криптографические методы защиты информации.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы, рис.2.5.

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований
исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая зашифрованию, и ключ шифрования.

Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

В отличие от других методов криптографического преобразования информации, методы **стеганографии** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но

проведенные исследования показывают ее перспективность.

Рис. 2.5. Классификация методов криптографического преобразования информации

В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в КС открыла практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является простой метод скрытия файлов при работе в операционной системе MS DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш Control и Z). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по достижению метки EOF и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение,

речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса **кодирования** информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации

3.2. Алгоритмы шифрования

Основным видом криптографического преобразования информации в КС является шифрование. Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную информацию **(шифртекст)** или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название **зашифрование,** а процесс преобразования закрытой информации в открытую - **расшифрование.**

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. **Методом шифрования (шифром)** называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление ЭВМ и

КС инициировало процесс разработки новых шифров, учитывающих возможности использования ЭВМ как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр **(криптоанализ)** - это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

* стойкость шифра противостоять криптоанализу **(криптостойкость)** должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
* криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
* шифртекст не должен существенно превосходить по объему исходную информацию;
* ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
* время шифрования не должно быть большим;
* стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации - перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

В качестве примера удачного метода шифрования можно привести шифр DES (Data Encryption Standard), применяемый в США с 1978 года в качестве государственного стандарта. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнародовано ни одного случая обнаружения слабых мест в алгоритме шифрования.

В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора. Согласно заявлению специалистов Агентства национальной безопасности США 56-битный ключ для DES может быть найден менее чем за 453 дня с использованием суперЭВМ Cray T3D, которая имеет 1024 узла и стоит 30 млн. долл. Используя чип FPGA (Field Progammbly Gate Array - программируемая вентильная матрица) стоимостью 400 долл., можно восстановить 40-битный ключ DES за 5 часов. Потратив 10 000 долл. за 25 чипов FPGA, 40-битный ключ можно найти в среднем за 12 мин. Для вскрытия 56-битного ключа DES при опоре на серийную технологию и затратах в 300000 долл. требуется в среднем 19 дней, а если разработать специальный чип, то - 3 часа. При затратах в 300 млн. долл. 56-битные ключи могут быть найдены за 12 сек. Расчеты показывают, что в настоящее время для надежного закрытия информации длина ключа должна быть не менее 90 бит.

Все методы шифрования могут быть классифицированы по различным признакам. Один из вариантов классификации приведен на рис.2.6.

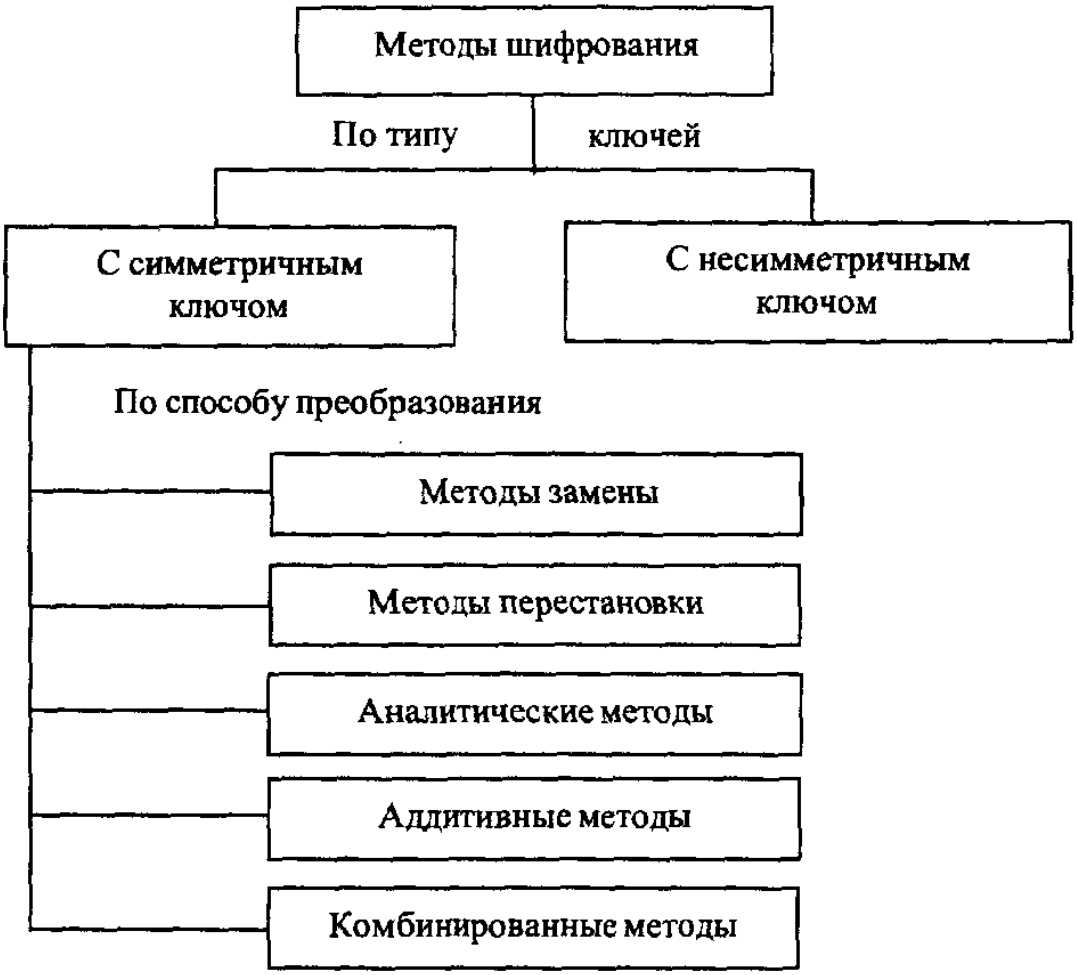

Рис.2.6.Классификация методов шифрования

3.3. Методы шифрования с симметричным ключом

Метод замены

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу. Самым простым является *метод прямой замены.* Символам 5м исходного алфавита A_0, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы s_{1i} шифрующего алфавита A_1. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста To, длиной - K символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа L_{oh}, путем замены каждого символа $s_{0i} \in T_0$ $(i=\overline{1,K})$, представленного в исходном алфавите A_0 размера [1xR], на число $h_{0i}(s_{0i})$ соответствующее порядковому номеру символа s_{0i} в алфавите A_0.

Шаг 2. Формирование числового кортежа L_{1h} путем замены каждого числа кортежа L_{oh} на соответствующее число h_{1i} кортежа L_{1h} вычисляемое по формуле:

$$H_{1i} = (k_1 * h_{oi}(s_{0i}) + k_2) (\mathrm{mod}\ R),$$

где k_1 - десятичный коэффициент; k_2 - коэффициент сдвига. Выбранные коэффициенты k_1, k_2 должны обеспечивать однозначное соответствие чисел h_{0i}, и h_{1i}, а при получении $h_{1i}= 0$ выполнить замену $h_{1i}= R$.

Шаг 3. Получение шифртекста T_1 путем замены каждого числа $h_{1i}(s_{1i})$ кортежа L_{1h} соответствующим символом $s_{1i} \in T_1$ $(i=\overline{1,K})$ алфавита шифрования A_1 размера [1 × R].

Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

*УПРАЖНЕНИЕ 1.**Метод шифрование путём замены с использованием алгоритма моноалфавитной замены***

Исходными данными для шифрования являются:

T_O = <МЕТОД_ШИФРОВАНИЯ>;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ>;

A_1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЛЪШБУЮ>;

R=32; k_1=3; k_2=15; b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1.L_{0h} = <12,6,18,14,5,32,24,9,20,16,14,3,1,13,9,31>.

Шаг 2. L_{1h} =<19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>.

Шаг3.T_1 = <СОЯГБДИМЧУГЦКПМХ>.

Шаг4.T_2 = <СОЯГ БДИМ ЧУГЦ КПМХ>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T_1 длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

$$k_1 h_{0i} + k_2 = nR + h_{1i},$$

При известных целых величинах k_1, k_2, h_{1i} и R величина h_{0i} вычисляется методом перебора n.

Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 2.1).

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки s_{0i} таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки s_{1i}, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке s_{1i}.

Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки перехваченных сообщений может установить соответствие между символами обоих алфавитов.

Таблица 2.1.

Таблица замены

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

s_{0i}	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	25	26	27	28	29	30	31	32
s_{1i}	Н	Ш	Ю	Щ	Т	Ж	Х	Д
h_{1i}	26	29	32	3	6	9	12	15

Существенно более стойкими являются методы полиалфавитной замены. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста. Формально полиалфавитную замену можно представить следующим образом. При N - алфавитной замене символ s_{01} из исходного алфавита A_0 заменяется символом s_{11} из алфавита A_1, s_{01} заменяется символом s_{22} из алфавита A_2 и так далее. После замены s_{0N} символом s_{NN} из A_N символ $s_{0(N+1)}$ замещается символом $s_{1(N+1)}$ из алфавита A_1 и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера Тв, которая представляет собой квадратную матрицу [RxR], где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32x32] (рис. 2.7).

$$T_B = \begin{vmatrix} \text{АБВГД} \ldots\ldots\ldots\ldots \text{ЪЭЮЯ\_} \\ \text{БВГДЕ} \ldots\ldots\ldots\ldots \text{ЭЮЯ\_А} \\ \text{ВГДЕЖ} \ldots\ldots\ldots\ldots \text{ЮЯАБ} \\ \\ \text{АБВГ} \ldots\ldots\ldots\ldots \text{ЫЪЭЮЯ} \end{vmatrix}$$

Рис. 2.7. Матрица Вижинера

Шифрование осуществляется с помощью ключа, состоящего из М неповторяющихся символов. Из полной матрицы Вижинера выделяется матрица шифрования $T_ш$, размерностью [(M+1)R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк (рис. 2.8).

$$T_ш = \begin{vmatrix} АБВГДЕЖЗИКЛМНОЛРСТУФХЦЧШЩЪЬЫЬЭЮЯ\_ \\ ЗИКЛМНОПРСТУФХЦЧШЩЪЬЫЪЭЮЯ\_АБВГДЕЖ \\ ОПРСТУФХЦЧШЩЪЬЫЬЭЮЯ\_АБВГДЕЖЗИКЛМН \\ НОПРСТУФХЦЧШЩЪЬЫЬЭЮЯ\_АБВГДЕЖЗИКЛМ \\ ДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЬЫЬЭЮЯ\_АБВГ \end{vmatrix}$$

Рис.2.8. Матрица шифрования для ключа <ЗОНД>

Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов.

Шаг 1. Выбор ключа К длиной М символов.

Шаг 2. Построение матрицы шифрования $T_ш=(b_{ij})$ размерностью [(M+1)R] для выбранного ключа К.

Шаг 3. Под каждым символом 8ог исходного текста длиной I символов размещается символ ключа k_m . Ключ повторяется необходимое число раз.

Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из $T_ш$ по следующему правилу:

1) определяется символ k_m ключа К, соответствующий замещаемому символу s_{or};
2) находится строка i в $T_ш$, для которой выполняется условие $k_m=b_{i1}$;
3) определяется столбец j, для которого выполняется условие:

   $s_{0r}= b_{1j}$,
4) символ s_{0r} замещается символом b_{ij}.

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2. Последовательно выбираются символы s_{1r} из шифртекста и соответствующие символы ключа k_m. В матрице $T_ш$ определяется строка i, для которой выполняется условие $k_m = b_{i1}$. В строке i определяется элемент $b_{ij} = s_{1r}$. В расшифрованный текст на позицию r помещается символ b_{1j}.

Шаг 3. Расшифрованный текст записывается без разделения на блоки. Убираются служебные символы.

УПРАЖНЕНИЕ 2. Метод шифрование путём замены с помощью матрицы Вижинера

Требуется с помощью ключа К = <ЗОНД> зашифровать исходный текст

Т = <БЕЗОБЛАЧНОЕ_НЕБО>. Механизмы зашифрования и расшифрования представлены на рис.2.9.

Криптостойкость методов полиалфавитной замены значительно выше методов простой замены, так как одни и те же символы исходной последовательности могут заменяться разными символами. Однако стойкость шифра к статистическим методам криптоанализа зависит от длины ключа.

Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО
Ключ	ЗОНДЗОНДЗОНДЗОНД
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО

Рис.2.9. Пример шифрования с помощью матрицы Вижинера

Для повышения криптостойкости может использоваться модифицированная матрица шифрования. Она представляет собой матрицу размерности [11R], где R - число символов алфавита. В первой строке располагаются символы в алфавитном порядке. Остальные 10 строк нумеруются от 0 до 9. В этих строках символы располагаются случайным образом.

В качестве ключей используются, например, непериодические бесконечные числа π, e и другие. Очередной n-й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n-й цифрой бесконечного числа.

УПРАЖНЕНИЕ 3.Индивидуальное задание

Используя различные методы, выполнить индивидуальное шифрование выражений проведённых в таблице 2.1.

*Задание 3.1.****Метод шифрование путём замены с использованием алгоритма моноалфавитной замены.***

Задание 3.2.Метод шифрование путём замены с помощью матрицы Вижинера.

Таблица 2.1.

Исходные данные для индивидуального шифрования

Номер варианта	Исходный текст для индивидуального шифрования
1	Текстовый и графический режимы работы монитора
2	Большая интегральная схема модуля памяти
3	Матричный струйный лазерный специальный принтеры
4	Механическая оптическая радиоуправляемая мышь
5	Параллельный последовательный порты системного блока
6	Аппараты компьютерной сети модем факс-модем
7	НГМД НЖМД СИ-ДИ диски дискеты дисководы
8	Снять характеристики микропроцессорной техники
9	Базовое прикладное программное обеспечение ПЭВМ
10	Лингвистическое программное обеспечение САПР
11	Программа схемотехнического проектирования платы
12	Моделирование переходных процессов платы
13	Программа конструкторского проектирования микропроцессора
14	Редактор условных графических элементов схем
15	Разработка УГО обозначения электронной схемы
16	Позиционное обозначение компонентов схемы
17	Схема структурная системного блока
18	Архитектура персонального компьютера
19	Модуль Базовая система ввода-вывода
20	Контроллер клавиатуры персонального компьютера
21	Видеоконтроллер монитора персонального компьютера
22	Пакет программ П-КАД фирмы ПЕРСОНАЛ-КАД

23	Графический редактор электрических схем КАПТУРЕ
24	Вспомогательная программа моделирования ПИСПАЙС