2. Андерсон Т. Введение в многомерный статистический анализ. – М., 1963.
3. Милинький А.В. Классификация сигналов в условия неопределённости. – М., 1975.
4. Фукунага К. Введение в статистическую теорию распознавания образов. – М., 1979.
5. Жук Е.Е., Харин Ю.С. Устойчивость в кластер-анализе многомерных наблюдений. – Мн., 1998.

АРХИВАЦИЯ И ШИФРОВАНИЕ ДАННЫХ

В.М. Куколев

Учреждение образования «Гомельский государственный технический университет имени П.О. Сухого», Республика Беларусь

Научный руководитель Кравченко О.А.

Целью данного проекта является создание программы, которая бы объединила в себе два процесса (архивация и шифрование).

Вся программа написана в среде DELPHI, т. к. эта среда даёт пользователю широкие возможности в управлении: удобный пользовательский интерфейс и работа с длинными именами файлов.

Среда DELPHI позволяет создавать основу всего интерфейса за более короткое время, нежели на Паскале.

Шифрование – процесс получения последовательности данных, которая может быть поставлена в соответствие другой (исходной) последовательности, но не явно, а посредством какой-либо функции, называемой ключом.

Существует множество различных способов осуществить преобразование информации. Самое эффективное, с точки зрения нераскрываемости, – это математическое преобразование, которое легко осуществить при помощи ЭВМ.

При создании программы по шифрованию можно использовать два метода: табличные подстановки и функциональные замены. Оба метода имеют как преимущества, так и недостатки. Так, например, метод табличных подстановок весьма эффективен при достаточно длинной таблице подстановок, по длине, сравнимой с длиной самой шифруемой информации. Применяя подстановки, мы можем использовать какую угодно зависимость, не подчиняющуюся законам математики, что затрудняет раскрываемость шифра. При использовании этого метода, сначала создаётся таблица подстановок. В ней для каждого байта информации ставится в соответствие другой байт, определяемые пользователем. Поскольку основная структурная единица ЭВМ (байт) может принимать значения от 0 до 255, то необходимо, чтобы и таблица подстановок содержала 256 подстановок, причём таких, чтобы преобразование было однозначным, иначе процесс дешифровки может быть затруднён, а чаще всего вообще невозможен. При сегодняшнем быстродействии ЭВМ информация, зашифрованная 256-ти элементной таблицей, может быть восстановлена в весьма сжатые сроки. Чтобы этого не произошло, можно применять таблицы нефиксированной и достаточно большой длины. Это позволит существенно снизить раскрываемость шифра и повысить безопасность.

Помимо таблицы можно использовать и функциональные замены, суть которых заключается в следующем: задаётся математическая функция, которая существует на всей области Ох, причём каждому Х соответствует только одно значение У, иначе преобразование будет неоднозначным. При работе программы шифрования она подставляет в функцию значение аргумента, которым является структурная единица шифруемой информации, далее программа вычисляет значение функции в этой точке и полученное значение можно назвать уже зашифрованным и в таком виде запи-

сать на диск. При данном подходе есть возможность раскрыть шифр, если удалось обнаружить функцию, которая используется в качестве преобразующей.

В данной программе использован метод, который позволяет практически полностью защитить шифруемые данные. Как уже отмечалось, самый лучший результат даёт табличная подстановка при очень длинной таблице, а именно ёе длина должна быть равна длине подлежащего шифрованию файла. Заполнение таблицы происходит непосредственно при осуществлении преобразования. Она заполняется близкими к случайным величинами. Функция, которая заполняет таблицу не является периодической, поскольку одним из входных её параметров является переменная счётчика считанных из исходного файла байт. Поэтому говорить про взлом шифра по отдельным фрагментам не целесообразно. Функция позволяет оперировать с ещё 17-ю входными параметрами: это 16-ти символьный пароль и 32-х битная величина типа «длинное целое», хранящая длину исходного файла. При преобразовании файла каждый его байт складывается с табличной подстановкой и с очередным символом пароля. Процесс сложения происходит по методу XOR (логическое или). Это позволит применить обратное преобразование для 100%-ной дешифровки файла.

В основе процедуры формирования таблицы лежит метод сложения гармонических функций синуса и косинуса, однако применена параметрическая модуляция этих функций, т. е. они изменяют свою фазу, частоту и амплитуду в зависимости от входных параметров.

Другим эффективным способом зашифровать информацию является т. н. сжатие этой информации (её архивирование).

Архивация – представление последовательности данных определённой длины другой последовательностью, но уже меньшей длины, т. е. её более короткая запись.

Известно, что существуют физические ограничения в объёме внешних носителей магнитной информации. Это связано с тем, что мы не можем поместить на единицу площади магнитной поверхности бесконечное число диполей. Поэтому приходится использовать математические преобразования для более короткой записи исходной информации.

С развитием ЭВМ придумали много методов сжатия. Основные из них – это использование алгоритма Хаффмана, основанного на формировании «дерева повторений», а также использование словарей часто встречающихся байт или целых информационных цепочек.

Оба метода предполагают предварительное прочтение файла и формирования на основе содержимого подготовительной информации. Идея метода Хаффмана заключается в том, что частота появления различных байт в файле неодинакова. На основе статистической кривой делается вывод о наиболее часто и редко встречающихся байт в файле. Часто встречаемые байты можно записать всего лишь несколькими битами, а редко встречаемые записываются более длинной последовательностью. Во многих случаях это себя оправдывает. Оптимальный результат сжатия произойдёт тогда, когда частота всех встречающихся байт будет кратной степеням двойки.

В общем случае содержимое файла представляет собой случайную комбинацию байт. Из теории вероятности известно, что вероятность появления случайного события при бесконечном потоке событий примерно одинакова, а в идеальном случае, когда число событий стремится к бесконечности, она является величиной постоянной.

Совершенно очевидно, что размер современных дисковых массивов является величиной, сравнимой с бесконечностью по сравнению с количеством принимаемых

одним байтом значений, поэтому использование алгоритма Хаффмана не оправдано с точки зрения сжатия информации, хотя и может быть применено как её шифрование.

Все современные методы сжатия используют словарные подстановки, причём словарь формируется динамически по мере прочтения файла. Это несколько снижает коэффициент сжатия, однако позволяет существенно повысить скорость обработки. Кроме того, добавляется возможность моментальной передачи сжатого потока данных.

В данной программе был использован метод поиска подпоследовательности повторяющихся байт и запись её более короткой конструкцией. Для того, чтобы программа, осуществляющая распаковку, могла отмечать момент начала сжатых данных при архивации использовался указатель на начало конструкции. Как только программа встретила данный указатель в сжатом тексте, она начинает алгоритм формирования исходной последовательности, поскольку непосредственно за указателем следуют два байта: длина подпоследовательности и байт-заполнитель.

Применяя данную программу, можно с уверенностью сказать о том, что сжатые и зашифрованные файлы можно смело передавать на дискетах или по электронной почте, не опасаясь, что их кто-то сможет расшифровать в разумные сроки. Самый веский аргумент такой, что битовое совпадение файла оригинала и зашифрованного составил 0,005 %.

ОЦЕНКА ФИНАНСОВОГО СОСТОЯНИЯ ПРЕДПРИЯТИЯ ПРИ ПОМОЩИ ТАБЛИЧНОГО РЕДАКТОРА MS EXCEL

Н.Н. Масалитина

Учреждение образования «Гомельский государственный технический университет имени П.О. Сухого», Республика Беларусь

Научный руководитель Водополова Н.В.

В условиях рыночной экономики верная оценка финансового состояния предприятия делового партнера, конкурента или своего собственного предприятия зачастую является главной составляющей успеха. Поэтому подобного рода анализу уделяется большое внимание в системе экономических наук, предлагающих множество методик оценки. Однако все они включают в себя достаточно значительный перечень показателей, а значит, требуют громоздких расчетов. Особенно если учесть, что оценка обычно производится за несколько периодов, по нескольким объектам. Использование современных вычислительных машин и информационных технологий значительно повышает эффективность такого анализа, его оперативность, позволяет производить анализ в реальном масштабе времени. При этом упрощается ввод исходных данных, их варьирование, выбор анализируемого периода. Целью разработки программы «ФинАудит» было создание инструмента анализа, позволяющего легко и быстро производить оценку финансового положения предприятия.

Анализ производится по четырем основным направлениям: ликвидность, прибыльность, платежеспособность и финансовая независимость. При этом рассчитываются следующие показатели: коэффициенты общей промежуточной и абсолютной ликвидности, коэффициенты обеспеченности запасов и затрат источниками средств (без учета и с учетом временно свободных источников средств), коэффициенты рентабельности капитала и рентабельности продаж и коэффициент финансовой независимости.