$h_5(x)$	57	101111	$x^5+x^3+x^2+x+1$
$h_6(x)$	73	111011	$x^5+x^4+x^3+x+1$

Выбор множеств пар М-кодов, кодовые слова которых обладают только определенными значениями ВКФ, основывается на следующем утверждении [1]. При всех $k \neq 0 \bmod 4$ существуют пары М-кодов с ВКФ, принимающими трехуровневые значения:

(-1), t(k), t(k)-2, (2)

где $t(k)=1+2^{\lceil (k+2)/2 \rceil}$, $\lceil \alpha \rceil$ — обозначает наибольшее целое число меньшее или равное α.

Пары примитивных многочленов, порождающие пары М-кодов с ВКФ, принимающими значения (2) образуют пары предпочтительных М-кодов. Для рассматриваемой системы связи важны не пары, а множества кодов с хорошими взаимно-корреляционными свойствами, в которых любая входящая в нее пара предпочтительна. Для приведенного выше примера М-кода значности 31 можно построить 8 различных множеств, в каждом из которых по 3 пары предпочтительных М-кодов. Распределение полиномов h(x) в множествах предпочтительных пар М-кодов выглядит так:

$M_3^1=\{h_1(x), h_2(x), h_6(x)\}$;
$M_3^2=\{h_1(x), h_2(x), h_3(x)\}$;
$M_3^3=\{h_1(x), h_3(x), h_5(x)\}$;
$M_3^4=\{h_1(x), h_5(x), h_6(x)\}$;
$M_3^5=\{h_2(x), h_4(x), h_6(x)\}$;
$M_3^6=\{h_2(x), h_3(x), h_4(x)\}$;
$M_3^7=\{h_3(x), h_4(x), h_5(x)\}$;
$M_3^8=\{h_4(x), h_5(x), h_6(x)\}$;

Заметим, что каждый предпочтительный многочлен h(x) входит в четыре из восьми множеств. Абсолютное максимальное значение коэффициента корреляции между всеми кодовыми словами каждого множества пар предпочтительных М-кодов M_3^i (j=1...8) равно (2)

$t(5)=1+2^{\lceil (5+2)/2 \rceil}=9$.

Относительное максимальное значение выбросов ВКФ не превышает величины 9/31 = 0,29. Выбранное для передачи множество M_3^i содержит $3\cdot(2^5-1)=93$ кодовых слов длиной 31. Если в системе предусматривается смена используемых множеств предпочтительных пар М-кодов, то количество применяемых слов для кодирования сообщений достигает величины

$M=8M_3^i = 8\cdot 93=744$.

Как видно, даже для малой длины кода можно построить сравнительно большое множество кодовых слов, удовлетворяющее основным требованиям скрытой системы: обеспечение заданной $P_{ош}$ декодирования для всех кодовых слов кода мощностью М.

Если переходить к большим значностям кода (n>100), когда число пар предпочтительных полиномов симплексного кода (его модификацией) увеличивается вместе с увеличением совокупности множеств M_r^j, эффективность защиты от подслушивания будет также расти. При низких отношениях Q и больших М для обнаружения слабых сигналов подслушивающей стороне потребуются значительные временные затраты во многих случаях несоизмеримые с реальным временем передачи информации по основному каналу.

Литература

1.Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. ТИИЭР. 1980. Т. 68. № 5.

СОХРАНЕНИЕ КОРПОРАТИВНЫХ ДАННЫХ С ПОМОЩЬЮ СИСТЕМЫ АВТОМАТИЧЕСКОГО РЕЗЕРВНОГО КОПИРОВАНИЯ

Д.С. ПРИЩЕПА

Работа любой организации немыслима без создания надежной и удобной информационной системы, в которой должны находиться все корпоративные данные. При этом остро встает вопрос сохранности этих данных, так как их потеря может привести к остановке работы всего предприятия. Одним из самых надежных путей решения данной проблемы является резервное копирование.

Современные корпоративные СУБД представляют подобные сервисы [1, 2], однако доступ к такому инструментарию имеет лишь администратор СУБД, что приводит к усложнению процесса. Возможно также использование файлового копирования, предоставляемого сервисами ОС, но в таком случае требуется предоставить пользователю сведения об архитектуре распределенной БД, что является грубым нарушением политики безопасности. В данной работе реализован внешний по отношению к СУБД сервис, основанный на механизмах аутентификации, используемых для доступа к корпоративным данным. За основу взята технология DataSnap компании Borland Software Corp [3].

Разработанная система состоит из трех частей: сервер расписания, сервер копирования и клиентское приложение. Первый является дополнительным сервисом бизнес-уровня корпоративной сети и представляет собой DCOM-сервер, реализованный в виде службы NT. Сервер расписания выполняет следующие функции: посредничество между СУБД и пользователем (в том числе аутентификация), поддержка расписания (добавление, редактирование и удаление заданий), обработка таймера и запуск сервера копирования по появлению события задания. Сервер копирования является COM-сервером и

выполняет копирование и восстановление данных. Клиентское приложение предоставляет интерфейс пользователя.

Данная система позволяет осуществлять копирование и восстановление данных с помощью заданий, которые могут выполняться автоматически по расписанию. Возможны следующие режимы запуска: однократно, ежедневно, еженедельно, ежемесячно и ежегодно. При этом действует политика безопасности СУБД, так как сервера расписания и копирования подключаются к БД, используя учетную запись пользователя. Имеется возможность поддержания одновременно нескольких баз данных.

Литература

Луни К. Oracle 8. Настольная книга администратора. М. 1999.
Бобровски С. Oracle 8. Архитектура. М. 1998.
Елманова Н., Трепалин С., Тенцер А. Delphi 6 и технология COM. СПб. 2002.