РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **46 869** (13) **U1**

(51) МПК
G06F 12/14 (2000.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21), (22) Заявка: **2005102206/22, 31.01.2005**

(24) Дата начала отсчета срока действия патента:
31.01.2005

(45) Опубликовано: **27.07.2005**

Адрес для переписки:
121609, Москва, Осенний б-р, 11, (609 отделение связи), "Патентно-правовая фирма ВИС", пат.пов. Н.Д.Кольцовой, рег.№ 799

(72) Автор(ы):
Грушецкий А.В. (RU),
Березнев А.Г. (RU),
Панов С.Б. (RU),
Синяков А.В. (RU),
Готцев В.В. (RU),
Григорьев И.О. (RU),
Титов А.Г. (RU),
Оленин С.А. (RU),
Воротников К.И. (RU),
Симонов А.В. (RU)

(73) Патентообладатель(и):
Федеральное государственное унитарное предприятие "НИИ "Квант" (RU)

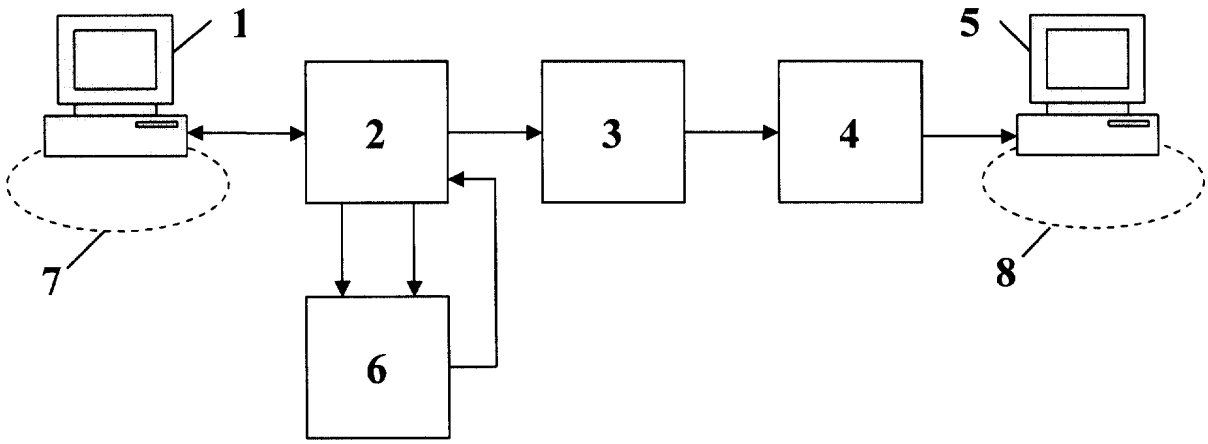
(54) СИСТЕМА ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ ИЗ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ В СЕТЬ НЕДОСТУПНУЮ ДЛЯ ОБЩЕГО ПОЛЬЗОВАНИЯ

Формула полезной модели

Система однонаправленной передачи данных из сети общего пользования в сеть недоступную для общего пользования, содержащая сетевой узел связи сети недоступной для общего пользования, к входу которого подключен выход приемника данных, вход которого через линию связи соединен с первым выходом передатчика данных, первый вход которого соединен с выходом сетевого узла связи сети общего пользования, отличающаяся тем, что на передающей стороне указанной системы введен узел квитирования, первый вход которого соединен со вторым выходом передатчика данных, а второй вход соединен с третьим выходом передатчика данных, второй вход которого соединен с выходом узла квитирования, при этом узел квитирования выполнен с возможностью формирования сигнала готовности приемника данных, задержанного относительно сигнала завершения передачи данных, формируемого по сигналу разрешения передачи данных, на величину, которая определена эмпирически из условия передачи без потерь данных из сети общего пользования в сеть недоступную для общего пользования, для конкретных сетей.

RU 46869 U1

RU 46869 U1



RU 46869 U1

RU 46869 U1

Изобретение относится к вычислительной технике и может быть использовано для защиты информационных ресурсов сетей недоступных для общего пользования, например, закрытых, корпоративных, служебных и т.д. сетей.

Известна система защиты информационных ресурсов при передаче данных связанных компьютерных сетей, которая содержит две сетевые материнские платы с сетевыми интерфейсными адаптерами для приема и передачи коммуникационных сообщений в частной и в общедоступной сети, и сетевыми адаптерами передачи для обмена информацией между материнскими платами. Каждая сетевая материнская плата имеет сетевые программные средства для предотвращения передачи информации об услугах маршрутизации между сетевыми интерфейсными адаптерами и адаптерами передачи каждой сетевой матричной платы. Одна материнская плата подсоединена к общедоступной сети, например, Интернет, а другая материнская плата подсоединена к частной сети, при этом каждая сетевая материнская плата содержит программные средства преобразования протокола, препятствующие прохождению информации протокола верхнего

уровня, информации об адресе назначения между указанным сетевым интерфейсным адаптером и указанным адаптером передачи каждой сетевой материнской платы. Связывающие команды, предоставляемые сетевым программным обеспечением на каждой материнской плате, используются для блокировки всех услуг маршрутизации, таких как протокола разрешения адресов (ARP), протокола информации маршрутизации (RIP) и протокола управления сообщениями Internet (ICMP) между сетевыми интерфейсными адаптерами и адаптерами передачи соответственно. Удаление заголовка IP дейтограмм и блокировка услуг маршрутизации запрещает передачу физических адресов устройств, связанных с частной сетью [1].

Недостаток известной системы защиты информационных ресурсов заключается в том, что она имеет как прямой, так и обратный каналы связи, защита от несанкционированного доступа осуществляется на уровне программных средств. При наличии в такой системе несанкционированного объекта (персоны или программы), обладающего «кодами санкционированного доступа», может происходить утечка информации из частной сети в сеть общего пользования.

Известна микрокомпьютерная система автоматической безопасной и прямой передачи данных из одной вычислительной системы в другую вычислительную систему, в которой данные передаются "от первого терминала в первую микрокомпьютерную систему, назначенную первому оконечному устройству, при этом данные обрабатываются и передаются с помощью этой микрокомпьютерной системы либо немедленно, либо через

некоторое время по линии передач данных напрямую во вторую микрокомпьютерную систему, предназначенную для другого терминала, в которой они обрабатываются и передаются либо немедленно, либо через некоторое время во второе оконечное устройство. В известной системе используется шлюзовой способ передач данных из одной микрокомпьютерной системы в другую микрокомпьютерную систему.

Данная микрокомпьютерная система является наиболее близкой к изобретению, так как является однонаправленной из-за применения шлюзовой системы передачи данных.

Недостаток этой системы заключается в том, что при использовании ее для передачи данных из сети общего пользования в сеть, недоступную для общего

пользования, наличие в последней несанкционированного объекта (персоны или программы), обладающего «кодом санкционированного доступа», что вполне вероятно, может происходить утечка информации сигнала типа «ДА» или «НЕТ» в сеть общего пользования путем модуляции средней скорости передачи данных в сеть, недоступную для общего пользования, так как независимо от буферной памяти «шлюза» формируются сигналы квитирования информации по времени заполнения памяти, связанной с сетью общего пользования, и времени выгрузки памяти в сети, недоступной для общего пользования. При наличии первого несанкционированного объекта в сети общего пользования, обладающего возможностью передачи информации в сеть, недоступную для общего пользования, и измерения скорости передачи данных, и при наличии

второго несанкционированного объекта в сети недоступной для общего пользования, обладающего возможностью получения информации из сети общего пользования путем освобождения буферной памяти шлюза, первый несанкционированный объект сети общего пользования может переслать второму несанкционированному объекту сети, недоступной для общего пользования, вопрос, предполагающий ответ типа «ДА» или «НЕТ», и организовать поток прямой передачи ничего незначащей информации для второго из указанных несанкционированных объектов. При ответе второго несанкционированного объекта сети недоступной для общего пользования, типа «ДА» на поставленный вопрос он будет в нормальном режиме отгружать буферную память шлюза, а при ответе типа «НЕТ» он будет искусственно тормозить отгрузку, что в целом изменит среднюю скорость передачи данных, которая будет зафиксирована первым несанкционированным объектом сети общего доступа, что снижает информационную защищенность ресурсов в известной системе при использовании ее для передачи данных из сети общего пользования в сеть недоступную для общего пользования.

Технический результат данного изобретения заключается в повышении надежности защиты инфорации в сетях, недоступных для общего пользования, при передаче в эти сети данных из сетей общего пользования путем исключения возможности передачи информационных сигналов типа «ДА» или «НЕТ».

Указанный технический результат достигается тем, что в систему однонаправленной передачи данных из сети общего пользования в сеть недоступную для общего пользования, содержащую сетевой узел связи сети недоступной для общего пользования, к входу которого подключен выход приемника данных, вход которого через линию связи соединен с первым выходом передатчика данных, первый вход которого соединен с выходом сетевого узла связи сети общего пользования, на передающей стороне указанной системы введен узел квитирования, первый вход которого соединен со вторым выходом передатчика данных, а второй вход соединен с третьим выходом передатчика данных, второй вход которого соединен с выходом узла квитирования, при этом узел квитирования выполнен с возможностью формирования сигнала готовности приемника данных, задержанного относительно сигнала разрешения передачи данных на величину, которая определена эмпирически из условия передачи данных без потерь из сети общего пользования в сеть недоступную для общего пользования, для конкретных сетей.

На фиг.1 представлена структурная схема системы однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования.

На фиг.2 - структурная схема интерфейсной платы передатчика данных. На фиг.3 - структурная схема интерфейсной платы приемника данных. На фиг 4 -

функциональная схема управления передатчика данных. На фиг.5 - функциональная схема управления приемника данных.

На фиг.6 - временные диаграммы, поясняющие работу схемы управления передатчика данных.

На фиг.7 - временные диаграммы, поясняющие работу схемы управления приемника данных.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, содержит сетевой узел 1 (фиг.1) связи сети общего пользования, выход которого соединен с входом передатчика 2 данных. Первый выход передатчика 2 данных через линию 3 связи соединен с входом приемника 4 данных, выходом подключенного к входу сетевого узла 5 связи сети недоступной для общего пользования.

В систему однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, веден узел 6 квитирования, который формирует сигнал готовности приемника данных, задержанный относительно сигнала разрешения передачи данных на величину, которая определена эмпирически из условия передачи данных без потерь из сети общего пользования в сеть недоступную для общего пользования, первый вход которого соединен со вторым выходом передатчика 2 данных, а второй вход узла квитирования соединен с третьим выходом передатчика 2 данных, второй вход которого соединен с выходом узла 6 квитирования.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования может быть

построена на базе двух персональных электронно-вычислительных машин (ПЭВМ) типа IBM-PC, для передачи файлов, находящихся на жестких дисках данных ПЭВМ.

ПЭВМ сети 7 общего пользования передает данные, а ПЭВМ сети 8 недоступной для общего пользования принимает данные. Передатчик 2 данных и приемник 4 данных построены на базе интерфейсных плат, через которые осуществляется сопряжение ПЭВМ сети общего пользования и ПЭВМ сети недоступной для общего пользования.

Интерфейсная плата передатчика 2 данных содержит контроллер PCI 9 (фиг.2), схему 10 управления, формирователь 11 выходных данных. Вход контроллера PCI 9 шиной 12 соединен с ПЭВМ сети общего пользования, а первой выходной шиной 13 подключен к входу схемы 10 управления. Выходная шина 14 контроллера PCI 9 образует второй выход передатчика 2 данных, который соединен с первым входом узла 6 квитирования, выход которого шиной 15 соединен со вторым входом контроллера PCI 9. Схема управления 10 шиной 16 соединена с входом формирователя 11 данных, а шиной 17 - со вторым входом узла 6 квитирования. Шина 18 образует выход данных передатчика 2 данных.

Интерфейсная плата приемника 4 данных (фиг.3) содержит формирователь 19 данных, схему управления 20 и контроллер PCI 21. Вход формирователя 19 данных шиной 22 соединен с линией связи 3, а выходной шиной 23 с входом схемы управления 20, которая выходной шиной 24 подключена к контроллеру PCI 21, выходные данные которого по шине 25

поступают на сетевой узел 5 связи сети 8, недоступной для общего пользования.

Схема 10 управления передатчика 2 данных состоит из 32-х разрядного регистра 26 (фиг.4), счетчика 27 байт, мультиплексора 28 выходных данных. Входы 29, 30, 31, регистра 26 и входы 30, 31 счетчика 27 байт связаны с выходной шиной 13 контроллера PCI 9 интерфейсной платы 2 передатчика данных. На вход 29 регистра 26

поступает 32-х разрядное слово, на вход 30 регистра 26, счетчика 27 байт и узла 6 квитирования поступает сигнал разрешения передачи данных. На вход 31 регистра 26, счетчика 27 байт и узла 6 квитирования поступает сигнал синхронизации (тактовый сигнал) шины PCI 12. Выходы 33, 34, 35 и 36 регистра 26 подключены к одноименным входам мультиплексора 28, вход 37 которого соединен с первым выходом 37 счетчика 27 байт. Выходная шина 38 мультиплексора 28 и второй выход 39 счетчика 27 байт образуют шину 16 схемы управления 10 формирователя 11 данных. Третий 17 выход счетчика 27 байт соединен со вторым входом узла 6 квитирования, который в данном случае выполнен на базе перепрограммируемого делителя частоты. По входу 32 узла 6 квитирования задается коэффициент деления частоты.

Схема 20 управления приемника 4 данных состоит из трех восьмиразрядных регистров 40, 41, 42 (фиг.5), счетчика 43 байт и выходного 32-х разрядного регистра 44, соединенных между собой последовательно. Входы 45, 46, 47 регистров 40, 41, 42 и счетчика 43 байт соединены с выходной шиной 23 формирователя 19 данных. Выходы 48, 49, 50

восьмиразрядных регистров 40, 41, 42 соединены с входами 48, 49, 50 32-х разрядного регистра 44, вход 50 которого подключен к выходу счетчика 43 байт. Выход 51 регистра 44 и выход 52 счетчика 43 байт образует выходную шину 24 схемы управления 20 интерфейсной платы приемника 4 данных.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, работает следующим образом.

Данные для передачи из сети 7 общего пользования поступают в сетевой узел 1 связи, далее через передатчик 2 данных, линию связи 3 - на вход приемника 4 данных и затем через сетевой узел 5 в сеть 8, недоступную для общего пользования.

Передача данных в интерфейсной плате передатчика 2 данных осуществляется следующим образом (см. фиг.4 и фиг.6).

Данные для передачи по шине 12 поступают на контроллер PCI 9, затем по шине 13 на схему управления 10, где принятое слово данных (32 разряда) выдается порциями по 8 разрядов и через шину 16 поступает на вход формирователем 11 данных, который формирует выходные данные.

По шине 13 с выхода контроллера PCI 9 на вход 29 регистра 26 поступают данные i-слова (32 разряда) и по сигналу разрешения передачи 30 и переднему фронту сигнала синхронизации 31 в регистр 26. Байты i-слова A(i), B(i), C(i), D(i) с выходов 33, 34, 35, 36 поступают на входы 33, 34, 35, 36 мультиплексора 28 и по коду адреса байта (2 разряда) с выхода 37 счетчика байт 27 поступает на выход 38, далее вместе с сигналом сопровождения

байта с выхода 39 счетчика 27 поступает по шине 16 на вход формирователя 11 данных. Узел 6 квитирования формирует сигнал готовности приемника 15, поступающий на вход готовности передатчика 2 данных.

Пока сигнал готовности приемника 15 равен нулю, новое слово на передачу поступать не будет, то есть формируется задержка передачи данных. После прохождения сигнала рарешения передачи 30 (момент времени t0 - фиг.6) сигнал готовности приемника 15 сбрасывается в ноль, а узел 6 квитирования начинает формирование задержки сигнала готовности приемника с момента прихода на вход 17 сигнала завершения передачи данных с учетом коэффициента деления на входе 32. Длительность паузы T_delay0 от момента t0 до момента t1 определяется временем передачи 4-х байт, является величиной постоянной и зависит от частотных характеристик приемо-передающего тракта.

Длительность паузы от момента t1 до момента t2 можно изменять на величину T_delay1=Tclk * N_delay, где Tclk - период тактового сигнала, поступающего на вход 31 узла квитирования 6, N_delay - коэффициент-деления такового сигнала, поступающего на вход 32 узла квитирования 6. Минимальная величина паузы будет при N_ delay=0 (пунктирная линия на выходе 15, фиг.6). Величина N_ delay может быть определена эмпирически при проведении тестовых испытаний системы однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования. Общая задержка сигнала готовности 15 приемника относительно сигнала разрешения передачи данных 30 равна T_delay=T_delay0+ T_delay 1.

Работа схемы управления приемника 4 данных осуществляется следующим образом (см. фиг.5 и фиг.7).

Входные данные 45 (8 разрядов) по шине 23 с выхода формирователя 19 данных поступают на вход 45 регистров 40 и 44 вместе с сигналом сопровождения байт, поступающим на вход 46 восьмиразрядных регистров 40, 41, 42 и счетчика 43 байт, и сигналом тактирования, поступающего на вход 47 регистров 40,41,42 и счетчика 43 байт.По этим сигналам данные последовательно записываются в регистры 40, 42, 43. Для приема i-слова необходимо принять байты A(i), B(i), C(i), D(i) (фиг.7), которые подаются на входы 45, 48, 49, 50 регистра 44. Подсчет байт ведет счетчик 43 по модулю 4. Сигнал переноса (сигнал готовности по приему данных) с выхода 52 разрешает запись данных в регистр 44. Данные с выхода 51 поступают в контроллер PCI 21 вместе с сигналом готовности слова с выхода 52 счетчика 43.

Процесс передачи данных от ПЭВМ-передатчика сети общего пользования до ПЭВМ-приемника сети, недоступной для общего пользования происходит под управлением программы для передатчика (TRM) и программы для приемника (RCV).

Программа TRM для каждого передаваемого файла данных f формирует блок данных в формате заголовок-данные вида:

Block(f)=[H(f),D(f)] (1)

где

Block(f) - блок данных для файла f,

F - файл данных, длина которого равна N(f) байт,

H(f) - заголовок блока, который имеет фиксированной длинны N(H)-224 байт,

D(f) - данные блока для файла f, переменной длинны N(D). При пердаче любого файла в заголовке блока H(f) передается имя файла, его атрибуты и длина в байтах. Особенностью работы программы TRM в условиях полностью односторонней связи является отсутствие возможности аппаратной синхронизации между передатчиком и приемником. Это в свою очередь может приводить к потере данных в ПЭВМ-приемнике.

В данном изобретении для передачи файлов без потерь посредством узла 6 квитирования вводится задержка T_delay между словами в передаваемом блоке данных.

Величина задержки зависит от соотношения производительностей ПЭВМ-приемника и ПЭВМ-передатчика при подготовке, приему-передаче и размещении файлов.

Если ПЭВМ-приемник имеет производительность, не достаточную для приема данных без потерь, то в ПЭВМ-передатчике и необходимо вводить задержку отправки очередных данных, которая должна исключить любые потери данных при передаче.

Прием данных происходит под управлением программы RCV. Данные на приемной стороне принимаются в два этапа. На первом этапе происходит прием заголовка блока данных H(f). Как только заголовок блока будет целиком принят, программа RCV откроет новый файл с именем передаваемого файла и, определив его длину, станет на втором этапе принимать данные файла D(f) и записывать их на жесткий диск.

В конце приема файлу присваиваются атрибуты, переданные в заголовке. После этого программа RCV повторит цикл приема для следующего файла.

Из-за наличия задержки T_delay при передаче данных приемник работает так, что успевает записать текущий блок данных D(f) на жесткий диск до начала поступления следующего блока данных. Чтобы обеспечить прием данных без потерь, необходимо определить минимально допустимый интервал задержки T_delay при передаче данных.

Определить min{T_delay} можно после проведения серии экспериментов, в ходе выполнения которых будет найден рабочий коэффициент деления N_delay, который позволит сформировать необходимую задержку T_delay.

Обозначим S1, S2,..., Sn - тестовые состояния на ПЭВМ-приемнике, которые определяет пользователь. Указанные состояния можно считать приближением к некоторым рабочим состояниям. Состояние Si (i=1,...,n) характеризуется совокупностью работающих приложений (программ) и интенсивностью взаимодействия последних с жестким диском при чтении и записи файлов. Для каждого Si под управлением программ TRC и RCV проведена серия тестов Ti(k), (k=1,...,p).

При выполнении тестов Ti(k) с ПЭВМ-передатчика передается один тестовый файл file_testl объема 1Мб. На винчестер ПЭВМ-приемника записывается эталонный файл file_compl и после этого устанавливаем тестовое состояние S1. В узле 6 квитирования первоначально устанавливается на входе 32 двоичный код коэффициента деления N_delay=O (т.е. устанавливаем минимальную задержку сигнала готовности 15 приемника). Выполняем первый тест T 1(1) (т.е. передаем тестовый файл file_testl объема 1Мб). После приема и записи файла file_testl на винчестер его данные сравниваются с эталонным файлом file_comp1. Если файлы совпадают (т.е. тест прошел успешно), то на следующем шаге будем выполнять тест T1(2), в противном случае, увеличиваем N_delay на единицу и вновь выполняем тест T 1(1). Серия тестов Tl(k) (k=1,..., p) будет продолжаться до тех пор, пока не будет определен рабочий коэффициент деления N_delay(S1) для состояния S1, при котором вся серия тестов T1(k) (k=1,..., p) пройдет успешно. Сохраняем N_delay(S1). После этого на ПЭВМ-приемнике устанавливаем тестовое состояние S2, а на ПЭВМ-передатчике в узле квитирования 6 устанавливаем на входе 32 двоичный код коэффициента деления N_delay=0. Проводим серию тестов T2(k) аналогично для состояния S1 пока не получим рабочий коэффициент деления N_delay(S2) для состояния S2. Проводим тесты для остальных состояний S3.S4,..., Sn. По окончании всей серии тестов Ti(k) для всех тестовых состояний Si будет найдена совокупность параметров N_delay(Si), из которых выбираем рабочий коэффициент деления N_delay_ws по формуле:

$$N\_delay\_ws=\max\{N\_delay(Si)\},\ i=1,...,n \quad (2)$$

Полученное рабочее значение коэффициент деления N_delay_ws фиксируется в узле 6 квитирования, для исключения возможности изменения ее в данной системе (где проводились данные тестовые испытания), чтобы обеспечить передачу данных из сети общего пользования в сеть недоступную для общего пользования без потерь.

Источники информации, принятые во внимание:

1. Патент RU №2163727 C2, G 06 F 1/00, опубл. 27.02.2001
2. Патент RU №2170494 C2, H 04 L 12/56, опубл. 10.07.2001

(57) Реферат

Изобретение относится к вычислительной технике и может быть использовано для защиты информационных ресурсов сетей недоступных для общего пользования, например, закрытых, корпоративных, служебных и т.д. сетей.

Технический результат данного изобретения заключается в повышении надежности защиты информации в сетях, недоступных для общего пользования, при передаче в эти сети данных из сетей общего пользования путем исключения возможности передачи информационных сигналов типа «ДА» или «НЕТ».

В систему однонаправленной передачи данных из сети общего пользования в сеть недоступную для общего пользования, содержащую сетевой узел связи сети недоступной для общего пользования, к входу которого подключен выход приемника данных, вход которого через линию связи соединен с первым выходом передатчика данных, првый вход которого соединен с выходом сетевого узла связи сети общего пользования, на передающей стороне указанной системы введен узел квитирования.

МПК 7 H 04 L 13/00

G 06 F 12/22

СИСТЕМА ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ ИЗ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ В СЕТЬ НЕДОСТУПНУЮ ДЛЯ ОБЩЕГО ПОЛЬЗОВАНИЯ

Реферат

Изобретение относится к вычислительной технике и может быть использовано для защиты информационных ресурсов сетей недоступных для общего пользования, например, закрытых, корпоративных, служебных и т.д. сетей.

Технический результат данного изобретения заключается в повышении надежности защиты информации в сетях, недоступных для общего пользования, при передаче в эти сети данных из сетей общего пользования путем исключения возможности передачи информационных сигналов типа «ДА» или «НЕТ».

В систему однонаправленной передачи данных из сети общего пользования в сеть недоступную для общего пользования, содержащую сетевой узел связи сети недоступной для общего пользования, к входу которого подключен выход приемника данных, вход которого через линию связи соединен с первым выходом передатчика данных, первый вход которого соединен с выходом сетевого узла связи сети общего пользования, на передающей стороне указанной системы введен узел квитирования,

2005102206

МПК 7

H 04 L 13/00
G 06 F 12/22

СИСТЕМА ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ ИЗ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ В СЕТЬ НЕДОСТУПНУЮ ДЛЯ ОБЩЕГО ПОЛЬЗОВАНИЯ

Изобретение относится к вычислительной технике и может быть использовано для защиты информационных ресурсов сетей недоступных для общего пользования, например, закрытых, корпоративных, служебных и т.д. сетей.

Известна система защиты информационных ресурсов при передаче данных связанных компьютерных сетей, которая содержит две сетевые материнские платы с сетевыми интерфейсными адаптерами для приема и передачи коммуникационных сообщений в частной и в общедоступной сети, и сетевыми адаптерами передачи для обмена информацией между материнскими платами. Каждая сетевая материнская плата имеет сетевые программные средства для предотвращения передачи информации об услугах маршрутизации между сетевыми интерфейсными адаптерами и адаптерами передачи каждой сетевой матричной платы. Одна материнская плата подсоединена к общедоступной сети, например, Интернет, а другая материнская плата подсоединена к частной сети, при этом каждая сетевая материнская плата содержит программные средства преобразования протокола, препятствующие прохождению информации протокола верхнего

уровня, информации об адресе назначения между указанным сетевым интерфейсным адаптером и указанным адаптером передачи каждой сетевой материнской платы. Связывающие команды, предоставляемые сетевым программным обеспечением на каждой материнской плате, используются для блокировки всех услуг маршрутизации, таких как протокола разрешения адресов (ARP), протокола информации маршрутизации (RIP) и протокола управления сообщениями Internet (ICMP) между сетевыми интерфейсными адаптерами и адаптерами передачи соответственно. Удаление заголовка IP дейтограмм и блокировка услуг маршрутизации запрещает передачу физических адресов устройств, связанных с частной сетью [1].

Недостаток известной системы защиты информационных ресурсов заключается в том, что она имеет как прямой, так и обратный каналы связи, защита от несанкционированного доступа осуществляется на уровне программных средств. При наличии в такой системе несанкционированного объекта (персоны или программы), обладающего «кодами санкционированного доступа», может происходить утечка информации из частной сети в сеть общего пользования.

Известна микрокомпьютерная система автоматической безопасной и прямой передачи данных из одной вычислительной системы в другую вычислительную систему, в которой данные передаются от первого терминала в первую микрокомпьютерную систему, назначенную первому оконечному устройству, при этом данные обрабатываются и передаются с помощью этой микрокомпьютерной системы либо немедленно, либо через

некоторое время по линии передач данных напрямую во вторую микрокомпьютерную систему, предназначенную для другого терминала, в которой они обрабатываются и передаются либо немедленно, либо через некоторое время во второе оконечное устройство. В известной системе используется шлюзовой способ передач данных из одной микрокомпьютерной системы в другую микрокомпьютерную систему.

Данная микрокомпьютерная система является наиболее близкой к изобретению, так как является однонаправленной из-за применения шлюзовой системы передачи данных.

Недостаток этой системы заключается в том, что при использовании ее для передачи данных из сети общего пользования в сеть, недоступную для общего пользования, наличие в последней несанкционированного объекта (персоны или программы), обладающего «кодом санкционированного доступа», что вполне вероятно, может происходить утечка информации сигнала типа «ДА» или «НЕТ» в сеть общего пользования путем модуляции средней скорости передачи данных в сеть, недоступную для общего пользования, так как независимо от буферной памяти «шлюза» формируются сигналы квитирования информации по времени заполнения памяти, связанной с сетью общего пользования, и времени выгрузки памяти в сети, недоступной для общего пользования. При наличии первого несанкционированного объекта в сети общего пользования, обладающего возможностью передачи информации в сеть, недоступную для общего пользования, и измерения скорости передачи данных, и при наличии

второго несанкционированного объекта в сети недоступной для общего пользования, обладающего возможностью получения информации из сети общего пользования путем освобождения буферной памяти шлюза, первый несанкционированный объект сети общего пользования может переслать второму несанкционированному объекту сети, недоступной для общего пользования, вопрос, предполагающий ответ типа «ДА» или «НЕТ», и организовать поток прямой передачи ничего незначащей информации для второго из указанных несанкционированных объектов. При ответе второго несанкционированного объекта сети недоступной для общего пользования, типа «ДА» на поставленный вопрос он будет в нормальном режиме отгружать буферную память шлюза, а при ответе типа «НЕТ» он будет искусственно тормозить отгрузку, что в целом изменит среднюю скорость передачи данных, которая будет зафиксирована первым несанкционированным объектом сети общего доступа, что снижает информационную защищенность ресурсов в известной системе при использовании ее для передачи данных из сети общего пользования в сеть недоступную для общего пользования.

Технический результат данного изобретения заключается в повышении надежности защиты информации в сетях, недоступных для общего пользования, при передаче в эти сети данных из сетей общего пользования путем исключения возможности передачи информационных сигналов типа «ДА» или «НЕТ».

Указанный технический результат достигается тем, что в систему однонаправленной передачи данных из сети общего пользования в сеть недоступную для общего пользования, содержащую сетевой узел связи сети недоступной для общего пользования, к входу которого подключен выход приемника данных, вход которого через линию связи соединен с первым выходом передатчика данных, первый вход которого соединен с выходом сетевого узла связи сети общего пользования, на передающей стороне указанной системы введен узел квитирования, первый вход которого соединен со вторым выходом передатчика данных, а второй вход соединен с третьим выходом передатчика данных, второй вход которого соединен с выходом узла квитирования, при этом узел квитирования выполнен с возможностью формирования сигнала готовности приемника данных, задержанного относительно сигнала разрешения передачи данных на величину, которая определена эмпирически из условия передачи данных без потерь из сети общего пользования в сеть недоступную для общего пользования, для конкретных сетей.

На фиг.1 представлена структурная схема системы однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования.

На фиг.2 – структурная схема интерфейсной платы передатчика данных.

На фиг.3 – структурная схема интерфейсной платы приемника данных.

На фиг 4 – функциональная схема управления передатчика данных.

На фиг.5 – функциональная схема управления приемника данных.

На фиг.6 - временные диаграммы, поясняющие работу схемы управления передатчика данных.

На фиг.7 – временные диаграммы, поясняющие работу схемы управления приемника данных.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, содержит сетевой узел 1 (фиг.1) связи сети общего пользования, выход которого соединен с входом передатчика 2 данных. Первый выход передатчика 2 данных через линию 3 связи соединен с входом приемника 4 данных, выходом подключенного к входу сетевого узла 5 связи сети недоступной для общего пользования.

В систему однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, веден узел 6 квитирования, который формирует сигнал готовности приемника данных, задержанный относительно сигнала разрешения передачи данных на величину, которая определена эмпирически из условия передачи данных без потерь из сети общего пользования в сеть недоступную для общего пользования, первый вход которого соединен со вторым выходом передатчика 2 данных, а второй вход узла квитирования соединен с третьим выходом передатчика 2 данных, второй вход которого соединен с выходом узла 6 квитирования.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования может быть

построена на базе двух персональных электронно-вычислительных машин (ПЭВМ) типа IBM-PC, для передачи файлов, находящихся на жестких дисках данных ПЭВМ.

ПЭВМ сети 7 общего пользования передаёт данные, а ПЭВМ сети 8 недоступной для общего пользования принимает данные. Передатчик 2 данных и приемник 4 данных построены на базе интерфейсных плат, через которые осуществляется сопряжение ПЭВМ сети общего пользования и ПЭВМ сети недоступной для общего пользования.

Интерфейсная плата передатчика 2 данных содержит контроллер PCI 9 (фиг.2), схему 10 управления, формирователь 11 выходных данных. Вход контроллера PCI 9 шиной 12 соединен с ПЭВМ сети общего пользования, а первой выходной шиной 13 подключен к входу схемы 10 управления. Выходная шина 14 контроллера PCI 9 образует второй выход передатчика 2 данных, который соединен с первым входом узла 6 квитирования, выход которого шиной 15 соединен со вторым входом контроллера PCI 9. Схема управления 10 шиной 16 соединена с входом формирователя 11 данных, а шиной 17 – со вторым входом узла 6 квитирования. Шина 18 образует выход данных передатчика 2 данных.

Интерфейсная плата приемника 4 данных (фиг.3) содержит формирователь 19 данных, схему управления 20 и контроллер PCI 21. Вход формирователя 19 данных шиной 22 соединен с линией связи 3, а выходной шиной 23 с входом схемы управления 20, которая выходной шиной 24 подключена к контроллеру PCI 21, выходные данные которого по шине 25

поступают на сетевой узел 5 связи сети 8, недоступной для общего пользования.

Схема 10 управления передатчика 2 данных состоит из 32-х разрядного регистра 26 (фиг.4), счетчика 27 байт, мультиплексора 28 выходных данных. Входы 29, 30, 31, регистра 26 и входы 30, 31 счетчика 27 байт связаны с выходной шиной 13 контроллера PCI 9 интерфейсной платы 2 передатчика данных. На вход 29 регистра 26 поступает 32-х разрядное слово, на вход 30 регистра 26, счетчика 27 байт и узла 6 квитирования поступает сигнал разрешения передачи данных. На вход 31 регистра 26, счетчика 27 байт и узла 6 квитирования поступает сигнал синхронизации (тактовый сигнал) шины PCI 12. Выходы 33, 34, 35 и 36 регистра 26 подключены к одноименным входам мультиплексора 28, вход 37 которого соединен с первым выходом 37 счетчика 27 байт. Выходная шина 38 мультиплексора 28 и второй выход 39 счетчика 27 байт образуют шину 16 схемы управления 10 формирователя 11 данных. Третий 17 выход счетчика 27 байт соединен со вторым входом узла 6 квитирования, который в данном случае выполнен на базе перепрограммируемого делителя частоты. По входу 32 узла 6 квитирования задается коэффициент деления частоты.

Схема 20 управления приемника 4 данных состоит из трех восьмиразрядных регистров 40, 41, 42 (фиг.5), счетчика 43 байт и выходного 32-х разрядного регистра 44, соединенных между собой последовательно. Входы 45, 46, 47 регистров 40, 41, 42 и счетчика 43 байт соединены с выходной шиной 23 формирователя 19 данных. Выходы 48, 49, 50

восьмиразрядных регистров 40, 41, 42 соединены с входами 48, 49, 50 32-х разрядного регистра 44, вход 50 которого подключен к выходу счетчика 43 байт. Выход 51 регистра 44 и выход 52 счетчика 43 байт образует выходную шину 24 схемы управления 20 интерфейсной платы приемника 4 данных.

Система однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования, работает следующим образом.

Данные для передачи из сети 7 общего пользования поступают в сетевой узел 1 связи, далее через передатчик 2 данных, линию связи 3 - на вход приемника 4 данных и затем через сетевой узел 5 в сеть 8, недоступную для общего пользования.

Передача данных в интерфейсной плате передатчика 2 данных осуществляется следующим образом (см. фиг.4 и фиг.6).

Данные для передачи по шине 12 поступают на контроллер PCI 9, затем по шине 13 на схему управления 10, где принятое слово данных (32 разряда) выдается порциями по 8 разрядов и через шину 16 поступает на вход формирователем 11 данных, который формирует выходные данные.

По шине 13 с выхода контроллера PCI 9 на вход 29 регистра 26 поступают данные *i*-слова (32 разряда) и по сигналу разрешения передачи 30 и переднему фронту сигнала синхронизации 31 в регистр 26. Байты i-слова A(i), B(i), C(i), D(i) с выходов 33, 34, 35, 36 поступают на входы 33, 34, 35, 36 мультиплексора 28 и по коду адреса байта (2 разряда) с выхода 37 счетчика байт 27 поступает на выход 38, далее вместе с сигналом сопровождения

байта с выхода 39 счетчика 27 поступает по шине 16 на вход формирователя 11 данных. Узел 6 квитирования формирует сигнал готовности приемника 15, поступающий на вход готовности передатчика 2 данных.

Пока сигнал готовности приемника 15 равен нулю, новое слово на передачу поступать не будет, то есть формируется задержка передачи данных. После прохождения сигнала разрешения передачи 30 (момент времени t0 – фиг.6) сигнал готовности приемника 15 сбрасывается в ноль, а узел 6 квитирования начинает формирование задержки сигнала готовности приемника с момента прихода на вход 17 сигнала завершения передачи данных с учетом коэффициента деления на входе 32. Длительность паузы T_delay0 от момента t0 до момента t1 определяется временем передачи 4-х байт, является величиной постоянной и зависит от частотных характеристик приёмо-передающего тракта.

Длительность паузы от момента t1 до момента t2 можно изменять на величину T_delay1 = Tclk * N_delay, где Tclk – период тактового сигнала, поступающего на вход 31 узла квитирования 6, N_delay – коэффициент деления такового сигнала, поступающего на вход 32 узла квитирования 6. Минимальная величина паузы будет при N_ delay=0 (пунктирная линия на выходе 15, фиг.6). Величина N_ delay может быть определена эмпирически при проведении тестовых испытаний системы однонаправленной передачи данных из сети общего пользования в сеть, недоступную для общего пользования. Общая задержка сигнала готовности 15 приемника

относительно сигнала разрешения передачи данных 30 равна T_delay=T_delay0 + T_delay1.

Работа схемы управления приемника 4 данных осуществляется следующим образом (см. фиг.5 и фиг.7).

Входные данные 45 (8 разрядов) по шине 23 с выхода формирователя 19 данных поступают на вход 45 регистров 40 и 44 вместе с сигналом сопровождения байт, поступающим на вход 46 восьмиразрядных регистров 40, 41, 42 и счетчика 43 байт, и сигналом тактирования, поступающего на вход 47 регистров 40,41,42 и счетчика 43 байт. По этим сигналам данные последовательно записываются в регистры 40, 42, 43. Для приема i-слова необходимо принять байты A(i), B(i), C(i), D(i) (фиг.7), которые подаются на входы 45, 48, 49, 50 регистра 44. Подсчет байт ведет счетчик 43 по модулю 4. Сигнал переноса (сигнал готовности по приему данных) с выхода 52 разрешает запись данных в регистр 44. Данные с выхода 51 поступают в контроллер PCI 21 вместе с сигналом готовности слова с выхода 52 счетчика 43.

Процесс передачи данных от ПЭВМ-передатчика сети общего пользования до ПЭВМ-приемника сети, недоступной для общего пользования происходит под управлением программы для передатчика (TRM) и программы для приемника (RCV).

Программа TRM для каждого передаваемого файла данных f формирует блок данных в формате заголовок-данные вида:

$$Block(f) = [H(f),D(f)] \quad (1)$$

где

Block(f) – блок данных для файла f,

f – файл данных, длина которого равна N(f) байт,

H(f) – заголовок блока, который имеет фиксированной длинны N(H)=224 байт,

D(f) – данные блока для файла f, переменной длинны N(D).

При передаче любого файла в заголовке блока H(f) передается имя файла, его атрибуты и длина в байтах. Особенностью работы программы TRM в условиях полностью односторонней связи является отсутствие возможности аппаратной синхронизации между передатчиком и приемником. Это в свою очередь может приводить к потере данных в ПЭВМ-приемнике.

В данном изобретении для передачи файлов без потерь посредством узла 6 квитирования вводится задержка T_delay между словами в передаваемом блоке данных.

Величина задержки зависит от соотношения производительностей ПЭВМ-приемника и ПЭВМ-передатчика при подготовке, приёму-передаче и размещении файлов.

Если ПЭВМ-приемник имеет производительность, не достаточную для приема данных без потерь, то в ПЭВМ-передатчике и необходимо вводить задержку отправки очередных данных, которая должна исключить любые потери данных при передаче.

Прием данных происходит под управлением программы RCV. Данные на приемной стороне принимаются в два этапа. На первом этапе происходит прием заголовка блока данных H(f). Как только заголовок блока будет целиком принят, программа RCV откроет новый файл с именем передаваемого файла и, определив его длину, станет на втором этапе принимать данные файла D(f) и записывать их на жесткий диск.

В конце приема файлу присваиваются атрибуты, переданные в заголовке. После этого программа RCV повторит цикл приема для следующего файла.

Из-за наличия задержки T_delay при передаче данных приемник работает так, что успевает записать текущий блок данных D(f) на жесткий диск до начала поступления следующего блока данных. Чтобы обеспечить прием данных без потерь, необходимо определить минимально допустимый интервал задержки T_delay при передаче данных.

Определить min{T_delay} можно после проведения серии экспериментов, в ходе выполнения которых будет найден рабочий коэффициент деления N_delay, который позволит сформировать необходимую задержку T_delay.

Обозначим S1, S2, ... , Sn – тестовые состояния на ПЭВМ-приемнике, которые определяет пользователь. Указанные состояния можно считать приближением к некоторым рабочим состояниям. Состояние Si (i = 1,...n) характеризуется совокупностью работающих приложений (программ) и интенсивностью взаимодействия последних с жестким диском при чтении и записи файлов. Для каждого Si под управлением программ TRC и RCV проведена серия тестов Ti(k), (k = 1, ..., p).

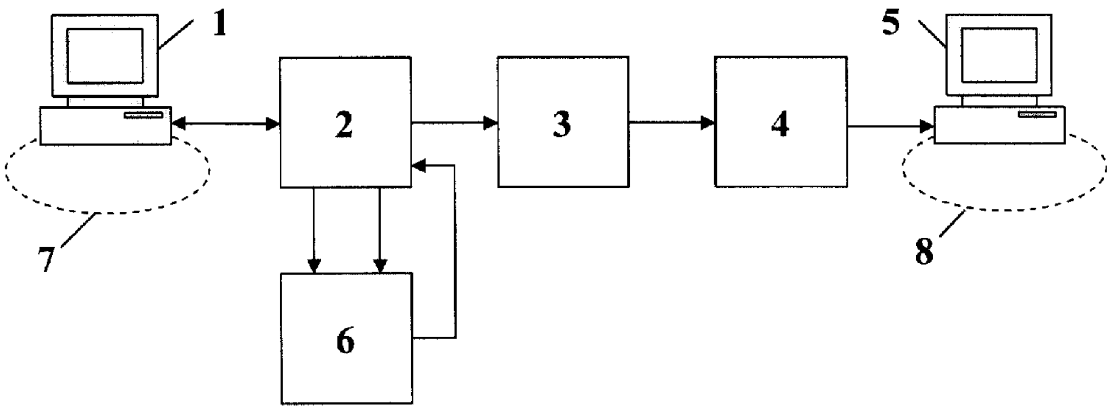
При выполнении тестов Ti(k) с ПЭВМ-передатчика передается один тестовый файл file_test1 объема 1Мб. На винчестер ПЭВМ-приемника записывается эталонный файл file_comp1 и после этого устанавливаем тестовое состояние S1. В узле 6 квитирования первоначально устанавливается на входе 32 двоичный код коэффициента деления N_delay = 0 (т.е. устанавливаем минимальную задержку сигнала готовности 15 приемника). Выполняем первый тест T1(1) (т.е. передаем тестовый файл file_test1 объема 1Мб). После приема и записи файла file_test1 на винчестер его данные сравниваются с эталонным файлом file_comp1. Если файлы совпадают (т.е. тест прошел успешно), то на следующем шаге будем выполнять тест T1(2), в противном случае, увеличиваем N_delay на единицу и вновь выполняем тест T1(1). Серия тестов T1(k) (k = 1, … , p) будет продолжаться до тех пор, пока не будет определен рабочий коэффициент деления N_delay(S1) для состояния S1, при котором вся серия тестов T1(k) (k = 1, … , p) пройдет успешно. Сохраняем N_delay(S1). После этого на ПЭВМ-приемнике устанавливаем тестовое состояние S2, а на ПЭВМ-передатчике в узле квитирования 6 устанавливаем на входе 32 двоичный код коэффициента деления N_delay = 0. Проводим серию тестов T2(k) аналогично для состояния S1 пока не получим рабочий коэффициент деления N_delay(S2) для состояния S2. Проводим тесты для остальных состояний S3,S4, …, Sn. По окончании всей серии тестов Ti(k) для всех тестовых состояний Si будет найдена совокупность параметров N_delay(Si), из которых выбираем рабочий коэффициент деления N_delay_ws по формуле:

$$N\_delay\_ws = \max \{ N\_delay(Si) \},\ i = 1,\ldots,n \qquad (2)$$

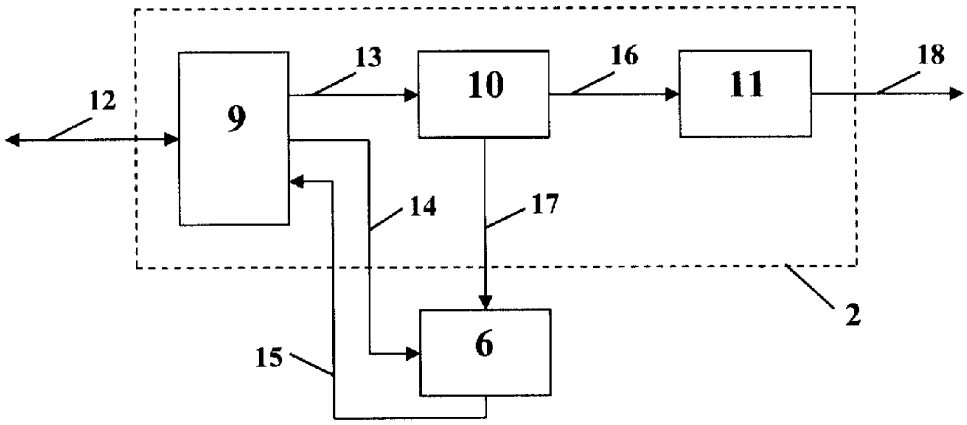
Полученное рабочее значение коэффициент деления N_delay_ws фиксируется в узле 6 квитирования, для исключения возможности изменения её в данной системе (где проводились данные тестовые испытания), чтобы обеспечить передачу данных из сети общего пользования в сеть недоступную для общего пользования без потерь.

Источники информации, принятые во внимание:

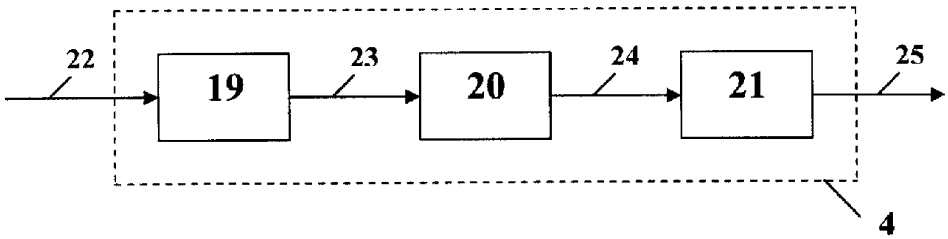
1. Патент RU № 2163727 C2, G 06 F 1/00, опубл. 27.02.2001
2. Патент RU № 2170494 C2, H 04 L 12/56, опубл.10.07.2001



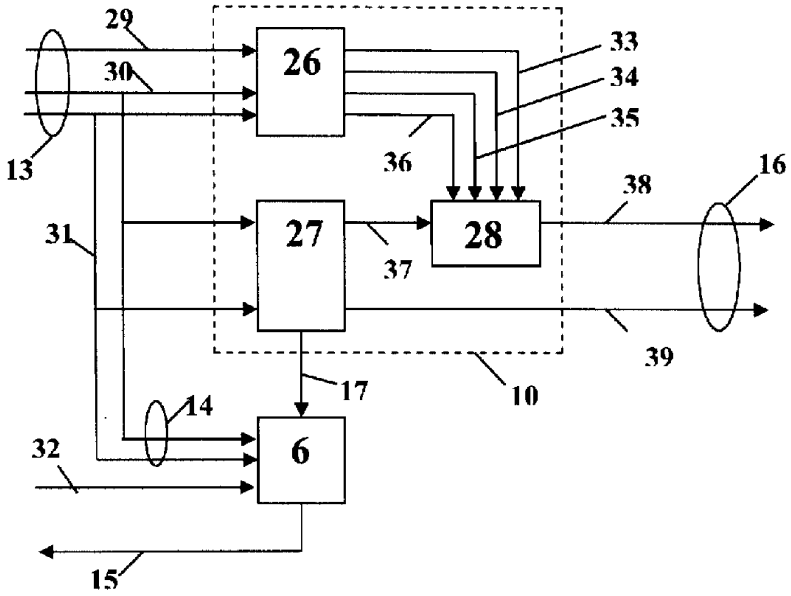
Фиг. 1



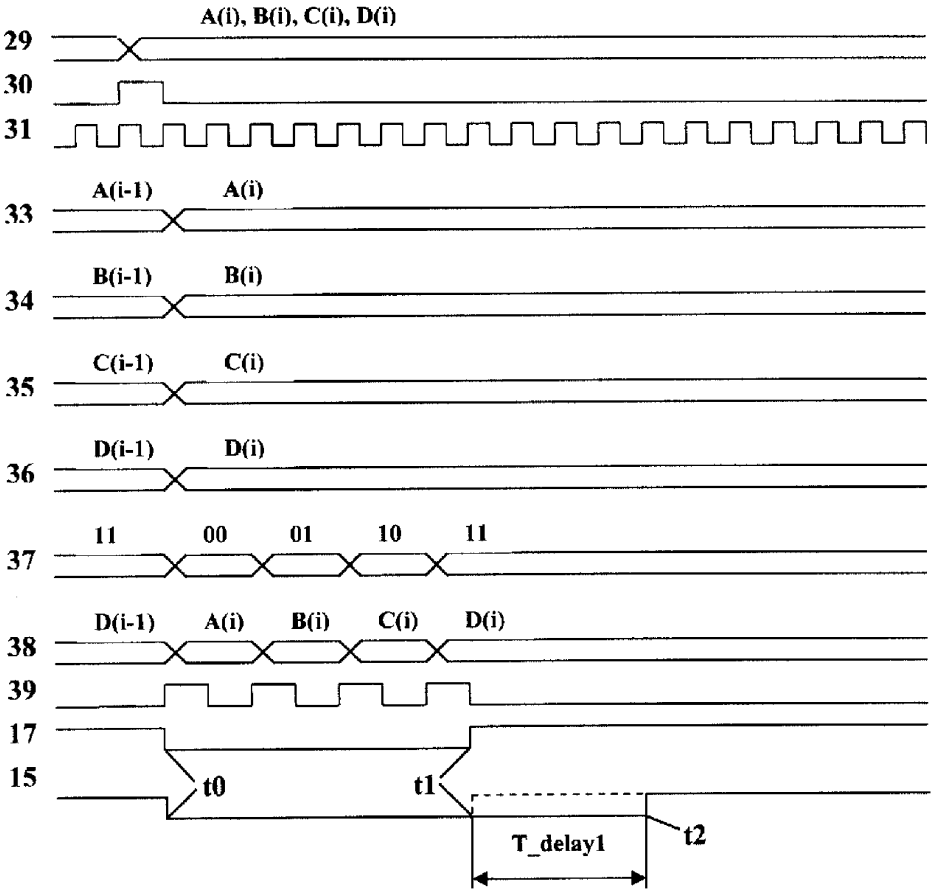
Фиг. 2



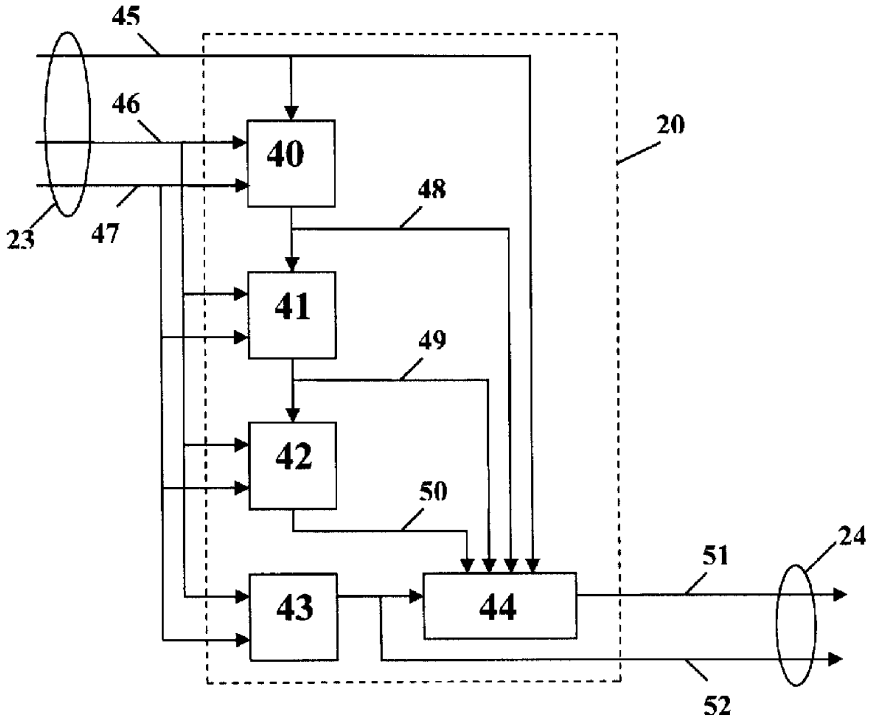
Фиг. 3


29
30
13
26
33
34
35
36
16
38
31
27
37
28
39
17
10
14
32
6
15

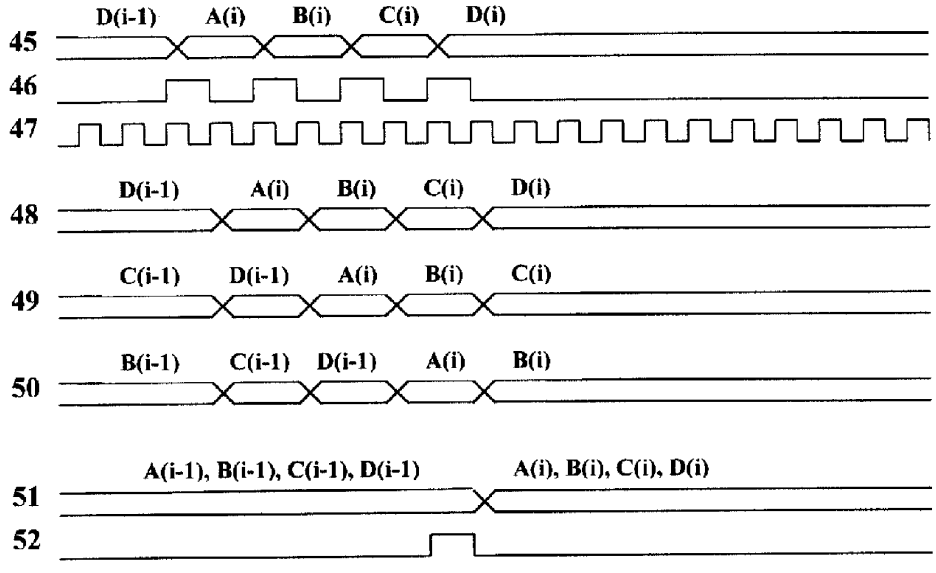
Фиг. 4


A(i), B(i), C(i), D(i)
29
30
31
A(i-1)
A(i)
33
B(i-1)
B(i)
34
C(i-1)
C(i)
35
D(i-1)
D(i)
36
11
00
01
10
11
37
D(i-1)
A(i)
B(i)
C(i)
D(i)
38
39
17
15
t0
t1
T_delay1
t2

Фиг. 6


45
46
20
40
48
23
47
41
49
42
50
24
51
43
44
52

Фиг. 5


D(i-1) A(i) B(i) C(i) D(i)
45
46
47
D(i-1) A(i) B(i) C(i) D(i)
48
C(i-1) D(i-1) A(i) B(i) C(i)
49
B(i-1) C(i-1) D(i-1) A(i) B(i)
50
A(i-1), B(i-1), C(i-1), D(i-1)
A(i), B(i), C(i), D(i)
51
52

Фиг. 7