РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 276 466** (13) **C1**

(51) МПК
H04L 12/28 (2006.01)
G06F 12/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004132548/09, 10.11.2004**

(24) Дата начала отсчета срока действия патента:
10.11.2004

(45) Опубликовано: **10.05.2006 Бюл. № 13**

(56) Список документов, цитированных в отчете о поиске: **RU 2182355 C1, 10.05.2002. CA 2489969 A1, 06.05.2004. US 6769034 B1, 27.07.2004. НИКОЛАЕВ Е.В. Частные сети для корпоративного бизнеса. В: "Документальная электросвязь", № 12, февраль 2004 г., с.12-13. ИГНАТОВ В.В. Универсальная среда сетевой защиты информации и ресурсов для безопасного функционирования корпоративных сетей на любых телекоммуникациях. Там же, с.24-26.**

Адрес для переписки:
124498, Москва, Зеленоград, пр-д 4806, 5, стр.20, ООО Фирма "Анкад"

(72) Автор(ы):
Романец Юрий Васильевич (RU),
Сырчин Владимир Кимович (RU),
Тимофеев Петр Александрович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью Фирма "Анкад" (RU)

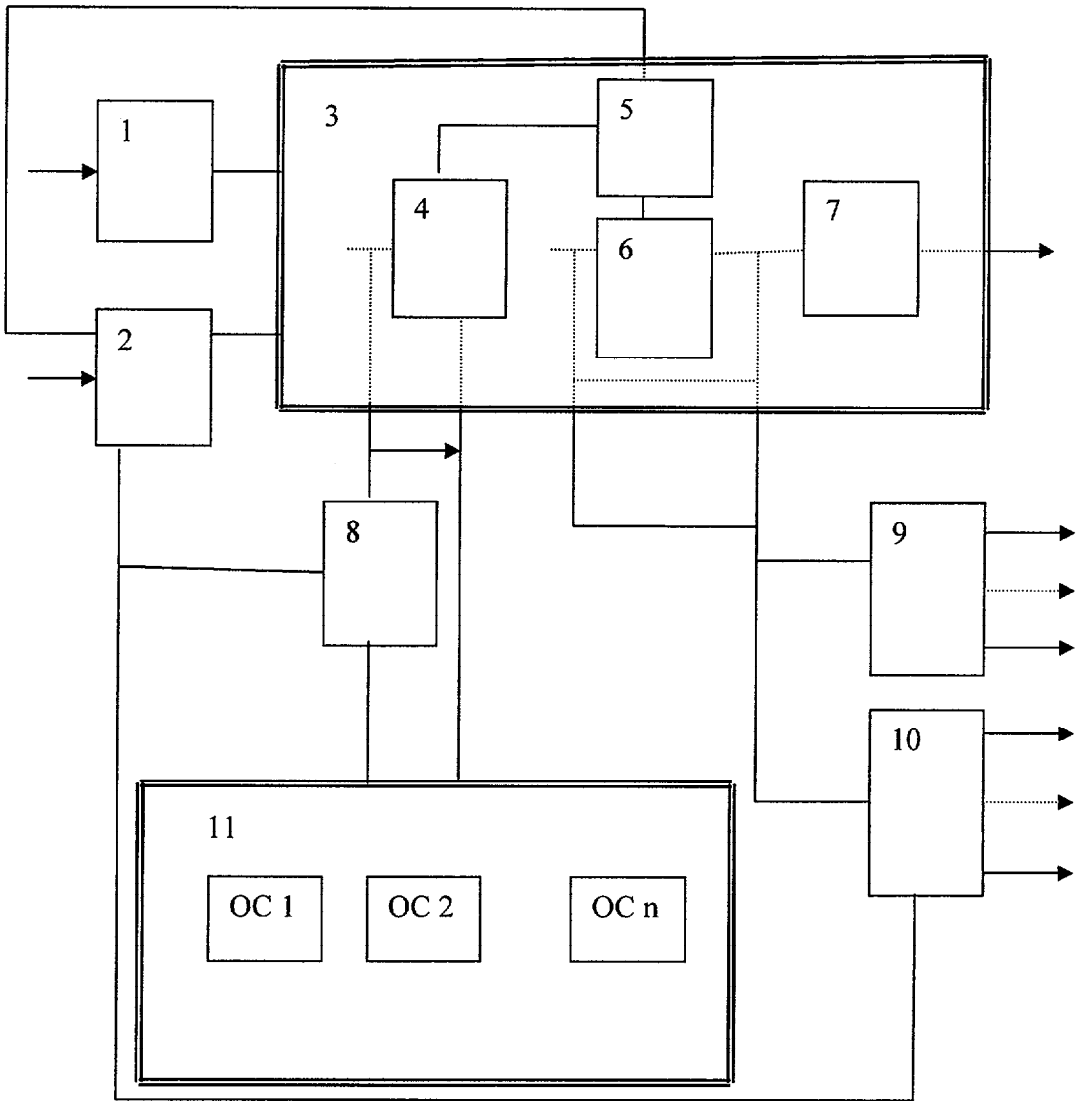
(54) СПОСОБ СОЗДАНИЯ ЗАЩИЩЕННЫХ ВИРТУАЛЬНЫХ СЕТЕЙ

(57) Реферат:

Изобретение относится к области вычислительной техники и может быть использовано для построения множества защищенных виртуальных сетей. Техническим результатом является расширение функциональных возможностей. Способ заключается в том, что шифруют исходный IP-пакет защищенной виртуальной сети, состоящей из отдельно стоящих компьютеров, или части компьютеров одной локальной сети, или компьютеров нескольких локальных сетей, создают выходной пакет с включением в него зашифрованного пакета (инкапсуляцию), при этом на каждом компьютере, который может использоваться в нескольких защищенных виртуальных сетях, для каждой создаваемой защищенной виртуальной сети выделяется отдельный блок долговременной памяти, в который записывается отдельная операционная система, настраиваемая на данную виртуальную сеть, а доступ к блоку долговременной памяти и загрузка операционной системы каждой защищенной виртуальной сети выполняется после предъявления пользователем полномочий, причем доступ к блокам памяти каждой защищенной виртуальной сети со стороны других виртуальных сетей блокируется средством ограничения доступа. 1 з.п. ф-лы, 11 ил.

RU 2276466 C1

RU 2276466 C1



Фиг. 1

RU 2276466 C1

RU 2276466 C1

RUSSIAN FEDERATION

(19) **RU** (11) **2 276 466** (13) **C1**

(51) Int. Cl.
H04L 12/28 (2006.01)
G06F 12/08 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004132548/09, 10.11.2004**

(24) Effective date for property rights: **10.11.2004**

(45) Date of publication: **10.05.2006 Bull. 13**

Mail address:
124498, Moskva, Zelenograd, pr-d 4806, 5, str.20, OOO Firma "Ankad"

(72) Inventor(s):
Romanets Jurij Vasil'evich (RU),
Syrchin Vladimir Kimovich (RU),
Timofeev Petr Aleksandrovich (RU)

(73) Proprietor(s):
Obshchestvo s ogranichennoj otvetstvennost'ju Firma "Ankad" (RU)

(54) METHOD FOR CREATING PROTECTED VIRTUAL NETWORKS

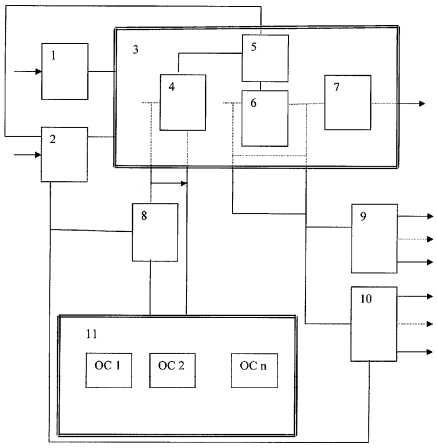
(57) Abstract:

FIELD: computer science, possible use for constructing multiple protected virtual networks.

SUBSTANCE: source IP packet of protected virtual network is encoded, network consisting of separately standing computers or portion of computers from local area network or computers of several local networks, output packet is formed including encoded packet (encapsulation), while at each computer, which can be utilized in several protected virtual networks, for each created protected virtual network separate long-term memory block is assigned, wherein separate operation system is recorded, adjusted for current virtual network, and access to long-term memory block and loading of operation system of each protected virtual network is performed after checking user rights, while access to memory blocks of each protected virtual network from other virtual networks is blocked by means of limiting access.

EFFECT: expanded functional capabilities.

2 cl, 11 dwg



Фиг. 1

RU 2276466 C1

RU 2276466 C1

Изобретение относится к области вычислительной техники и может быть использовано для построения множества сетей различного назначения на основе одного и того же парка компьютеров. Его использование позволит получить технический результат в виде создания множества виртуальных сетей, в которых используются одни и те же компьютеры: на одном и том же парке компьютеров - множество одновременно функционирующих виртуальных сетей.

Известен способ организации защищенных виртуальных сетей, подробно описанный в книге "Защита информации в корпоративных сетях и системах", авторы Соколов А.В., Шаньгин В.Ф., М.: ДМК Пресс, 2002, главы 11, 12.

Защита осуществляется с помощью программного модуля (программного обеспечения), выполняющего следующие действия:

- Шифрование исходного IP-пакета с помощью отдельно подключаемого программного модуля или аппаратного шифратора (в виде платы или внешнего устройства). Шифрование может выполняться по различным алгоритмам шифрования с применением симметричных или асимметричных ключей.

- Создание нового пакета с включением в него зашифрованного пакета (инкапсуляция) в соответствии с известными протоколами IpSec, SKIP или протоколом собственной разработки.

Данный модуль с шифраторами может устанавливаться на отдельный компьютер, на компьютер, находящийся в сети, на криптомаршрутизатор, на межсетевой экран. Поэтому виртуальная сеть может быть построена на базе:

- отдельно стоящих защищенных компьютеров;

- части компьютеров одной локальной сети;

- компьютеров нескольких локальных сетей с защищенными маршрутизаторами или межсетевыми экранами;

- комбинации перечисленных выше способов.

Известна реализация приведенного выше способа в технологии ViPNet (см. Игнатов В.В. Универсальная среда сетевой защиты информации и ресурсов для безопасного функционирования корпоративных сетей на любых телекоммуникациях. Аналитический и информационный журнал "Документальная электросвязь", №12, февраль 2004 г., с.24-26). Эта технология также основана на использовании программных модулей, реализующих описанные выше действия. Так называемый модуль ViPNet может быть установлен на каждом рабочем месте или на сервере (координаторе). При установке на рабочее место модуль защищает один ПК, при установке на координаторе защищается вся локальная сеть или ее сегмент. В модуле, устанавливаемом на координаторе, могут выполняться функции маршрутизации. При таком подходе виртуальная защищенная сеть может существовать внутри локальной, в виртуальную сеть может быть включен отдельный компьютер, множество локальных сетей и компьютеров. Модуль ViPNet осуществляет шифрование исходных пакетов, их преобразование (инкапсуляцию и другие действия). Шифрование осуществляется программным способом по различным алгоритмам шифрования с применением симметричных и асимметричных ключей.

Использование идентификаторов источника и получателя сообщений в виде меток предлагается в статье Николаева Е.В. "Частные сети для корпоративного бизнеса", опубликованной в аналитическом и информационном журнале "Документальная электросвязь", №12, февраль 2004 г., с.12-13. В ней описывается технология многопротокольной коммутации меток. Благодаря специальным меткам, которые присваиваются каждому пакету, возрастают возможности управления графиком. Кроме адреса, метка может ассоциироваться с путем, виртуальной сетью, приоритетом обслуживания и др.

Известен способ создания виртуальных защищенных сетей, представленный в патенте RU 2182355, принятый за прототип. Для ограничения доступа к передаваемой информации и сокрытия адресов применяется шифрование трафика локальной вычислительной сети, входящей в состав виртуальной корпоративной сети, на третьем уровне модели OSI.

Шифруются IP-пакеты вместе с их адресами. Шифрование осуществляется на изолированном от публичной сети устройстве. Также в способе определяют идентификаторы источника и получателя сообщений в виде меток. Метки определяют собой заголовок фиксированной длины, идентифицирующий множество пакетов, передаваемых по одному и тому же пути или в соответствии с некоторым классом обслуживания. Множество пакетов, отправляемых в соответствии с определенными заданными критериями, называют классом маршрутной эквивалентности. Маршрутизаторы используют принцип коммутации меток. Они устанавливают привязку метки к классу маршрутной эквивалентности, а затем с помощью стандартного протокола распространяют информацию о привязке метки всем маршрутизаторам, для которых они будут использовать данную метку при отсылке пакетов. Виртуальная защищенная сеть в этом случае строится на основе защищенных маршрутизаторов. Маршрутизатор в данном варианте будет иметь, как минимум, два сетевых интерфейса (один для связи с ПК внутренней локальной сети, другой - для связи с маршрутизатором, выходящим в сеть Интернет), устройство шифрования, память для меток.

Можно выделить основные черты данного способа:

- программные компоненты защиты устанавливаются на маршрутизаторы;
- преобразование IP-пакетов включает в себя шифрование исходного пакета вместе с адресами, инкапсуляцию зашифрованного пакета в новый IP-пакет, добавление меток в выходные пакеты;
- преобразование пакетов ведется в соответствии с собственным форматом, приведенным в патенте.

К недостаткам описанного выше способа можно отнести то, что сразу все компьютеры локальной сети находятся в виртуальной сети. Также нет возможности удаленного подключения к виртуальной сети одного компьютера без дополнительного маршрутизатора.

Во всех перечисленных выше способах виртуальные сети работают по принципу, когда каждый компьютер может находиться только в одной виртуальной сети. Поэтому на базе физических локальных сетей можно построить одну виртуальную защищенную сеть или несколько, при условии, что в них включаются различные компьютеры. При таком подходе рабочее место не может использоваться в разных виртуальных сетях. Также в рассмотренных сетях не ограничивается возможность доступа на рабочее место (персональный компьютер виртуальной сети) посторонних лиц. Последние могут получить доступ к информации, хранящейся на жестком диске или циркулирующей в виртуальной сети, путем перехвата ключей или самой информации в результате модификации программного обеспечения, стоящего на рабочем месте.

Для выхода в сеть в предложенных способах предлагается открытый сетевой интерфейс, не шифрующий информацию. Обработка пакетов осуществляется в оперативной памяти ПК. Поэтому описанные выше способы создания виртуальных сетей не обеспечивают выполнения требований для работы с информацией, имеющей высокий гриф секретности.

Целью предлагаемого изобретения является возможность создания на базе одних и тех же локальных корпоративных сетей и сетей публичного пользования множества виртуальных защищенных сетей. При этом доступ к этим сетям может осуществляться одним или несколькими сотрудниками с разными полномочиями с одного и того же рабочего места. Реализация предложенного способа обеспечивает защиту информации даже в случае кражи компьютера.

Сеть строится из компьютеров, имеющих один (или несколько) выходов в локальную сеть. Для каждой создаваемой защищенной виртуальной сети в компьютере, который может использоваться одновременно в нескольких защищенных виртуальных сетях, выделяется отдельный блок долговременной памяти, в который записывается отдельная ОС, при этом доступ к блоку долговременной памяти и загрузка ОС каждой из защищенных виртуальных сетей выполняется после предъявления пользователем полномочий, то есть идентифицирующей и ключевой информации, и выполнения аутентификации, причем

доступ к блокам памяти каждой защищенной виртуальной сети со стороны других виртуальных сетей блокируется.

Доступ к блокам долговременной памяти каждой защищенной виртуальной сети со стороны других виртуальных сетей блокируется созданием отдельного ключа шифрования для каждого блока так, что при записи информации в блок она зашифровывается, а при чтении - расшифровывается.

Предложенный способ обладает новизной, практической значимостью и является изобретением, которое может быть использовано для построения множества защищенных виртуальных сетей различного назначения. Его использование позволяет получить технический результат в виде множества одновременно функционирующих виртуальных защищенных сетей, в которых используются одни и те же компьютеры и циркулирует информация различного уровня конфиденциальности и секретности.

Отличительными особенностями предложенного способа являются следующие.

Во-первых, при загрузке компьютер получает свой адрес и сетевые настройки из загружаемой ОС и таким образом получает доступ к одной виртуальной сети. При перезагрузке в другую ОС компьютер получает другие настройки и попадает в другую виртуальную сеть. Таким образом, один и тот же компьютер может использоваться для работы в различных виртуальных сетях, переходя из одной виртуальной сети в другую путем перезагрузки.

Во-вторых, ОС изолированы друг от друга, то есть каждая ОС имеет свое пространство в долговременной памяти (на жестком диске или других устройствах) для своих файлов и данных. Разделение доступа к различным частям диска осуществляется либо аппаратными средствами, либо программными средствами, установленными в данном экземпляре ОС. Шифрование данных, передаваемых по сети между различными компьютерами, осуществляется также либо аппаратными средствами, либо программными средствами, установленными в данном экземпляре ОС.

В-третьих, каждому пользователю компьютера предоставляются права доступа к одной или нескольким ОС. При загрузке ОС обязательно выполняется строгая аутентификация пользователя. Таким образом, имея доступ к определенной ОС, пользователь получает доступ к одной из виртуальных сетей. Разграничение прав доступа пользователей к различным ОС реализуется программно или обеспечивается использованием аппаратных средств. Такое разграничение защищает доступ к информации различных защищенных виртуальных сетей.

Допустим, имеются несколько локальных сетей, в составе которых находятся 30 компьютеров. В настоящее время защищенные виртуальные сети строятся таким образом, что компьютер находится в одной сети. В принципе при наличии двух интерфейсов он может находиться в двух виртуальных сетях, но тогда трудно разделить доступ к информации этих двух сетей. То есть в этих двух сетях гриф информации не должен существенно различаться. Дополнительно также потребуются сетевые платы и другое коммуникационное оборудование.

В предлагаемом способе можно установить на каждый компьютер, например, по три ОС, и тогда мы можем использовать и увидеть в виртуальных сетях не 30, а 90 компьютеров, то есть в три раза увеличить парк для построения виртуальных сетей без дополнительного коммуникационного оборудования.

Например, установив на ноутбук несколько ОС, пользователь может с разных рабочих мест в разных офисах и городах входить в различные виртуальные сети со своего переносного компьютера. В домашних условиях при установке трех ОС один и тот же компьютер может использоваться для выхода в Интернет (одна ОС), для игр детей (другая ОС), для серьезной работы взрослых (третья ОС).

Графические изображения

На фигуре 1 представлена блочная структура персонального компьютера (ПК) с выделением блоков, необходимых для выполнения действий, описываемых в способе, где:

1 - Блок первоначальной загрузки;

2 - Устройство или система ограничения/разграничения доступа;

3 - Системная плата;

4 - Программа шифрования логических дисков в составе загруженной ОС;

5 - Аппаратный шифратор (например, выполненный в виде платы);

6 - Драйверы для сетевых устройств виртуальной сети (VPN-драйверы) в составе загруженной ОС;

7 - Встроенный в системную плату сетевой интерфейс;

8 - Устройство ограничения/разграничения доступа к разделам одного или нескольких накопителей на жестком диске;

9 - Один или несколько отдельных от системной платы сетевых интерфейсов;

10 - Один или несколько отдельных от системной платы криптографических сетевых интерфейсов;

11 - Один или несколько накопителей на жестком диске.

На фигуре 2 изображены два варианта конфигурации виртуального компьютера (ВК) для работы в виртуальной сети с открытой информацией. При этом используется операционная система ОС1 (см. фиг.1), блок 7 сетевых адаптеров, встроенных в системную плату или выполненных в виде отдельных устройств (блок 9).

На фигурах 3 и 4 приведены два варианта конфигурации ВК для работы в виртуальной сети с конфиденциальной информацией. В отличие от конфигурации ВК фиг.2, на фиг.3 блоком 1 производится программная аутентификация, блоком 4 - программное ограничение доступа к памяти путем шифрования, а блоком 6 - программное шифрование пакетов. На фиг.4 предлагается аутентификацию и проверку полномочий проводить аппаратно блоком 2.

На фигурах 5 и 6 приведены варианты конфигурации ВК для работы в сети с секретной информацией. В обоих вариантах предлагается аутентификацию и проверку полномочий проводить аппаратно блоком 2, шифрование пакетов проводить аппаратно блоком 5 (см. фиг.5) или 10 (см. фиг.6). На фиг.6 шифрование блоков памяти осуществляется программно.

На фигуре 7 представлена конфигурация ВК для работы в сети с совершенно секретной информацией. В отличие от предыдущих вариантов, блокировку доступа к блокам памяти предлагается выполнять аппаратно блоком 8 с шифрованием информации.

На фигуре 8 представлен вариант корпоративной сети, состоящей из четырех локальных вычислительных сетей (ЛВС), соединенных между собой через открытую сеть (Интернет). ЛВС1 состоит из незащищенных персональных компьютеров (ПК) и защищенных персональных компьютеров (ПКЗ) и выходит в корпоративную сеть через незащищенный маршрутизатор (М). ЛВС2 состоит только из защищенных компьютеров. ЛВС3, наоборот, состоит из незащищенных ПК и выходит в открытую сеть через защищенные маршрутизаторы (МЗ). Также имеются два отдельных защищенных персональных компьютера (ОПКЗ).

На фигуре 9 изображена блочная структура компьютера для работы в трех виртуальных сетях: одной открытой и двух защищенных.

На фигуре 10 изображена блочная структура компьютера для работы в двух виртуальных сетях - открытой и защищенной.

На фигуре 11 изображена блочная структура компьютера для работы с открытой, секретной и совсекретной информацией в трех виртуальных сетях.

Рассмотрим более подробно предложенные в способе действия.

На каждом компьютере для каждой защищенной виртуальной сети выделяются блоки долговременной памяти (жесткие диски, разделы жесткого диска, компакт-диски, флеш-память, дискеты и т.п.) блок 11 (см. фиг.1). В эти блоки устанавливаются операционные системы по одной на каждую виртуальную сеть. То есть число ОС соответствует числу виртуальных сетей, к которым компьютер имеет доступ.

При загрузке компьютер получает свой адрес и сетевые настройки из загружаемой ОС и таким образом получает доступ к одной виртуальной сети. При перезагрузке в другую ОС

компьютер получает другие настройки и попадает в другую виртуальную сеть. Таким образом, один и тот же компьютер может использоваться для работы в различных виртуальных сетях, переходя из одной виртуальной сети в другую путем перезагрузки.

Для исключения модификации незагруженных ОС в процессе работы одной из них используется блок 8 (см фиг.1) ограничения (блокировки) доступа. Ограничение доступа обеспечивается:

- программным образом (системой разграничения доступа, используемой в составе загруженной ОС);
- аппаратным образом путем блокировки доступа к блокам памяти различных ОС в соответствии с полномочиями, предъявленными каждым пользователем;
- использованием аппаратного (блок 8) или программного (блок 4) прозрачного шифрования информации (при записи информация шифруется, а при чтении - расшифровывается на ключах шифрования, загруженных из блока 2 ограничения доступа (см. фиг.1) или напрямую в блоки 8 и 4).

Блок 4 используется для прозрачного шифрования информации при записи на логические диски (прозрачно шифруемые логические диски-файлы будем называть виртуальными дисками). Он включается в виде драйвера в загруженную ОС. Блок 4 шифрует информацию самостоятельно программным образом или использует аппаратное шифрование блоком 5.

Для выполнения аутентификации пользователя и проверки его полномочий используются блоки 1 или 2 (см. фиг.1). Блок 1 представляет собой программу, прописанную в BIOS компьютера, которая запрашивает полномочия пользователя и при положительном результате аутентификации расшифровывает для него управляющую информацию ОС и загружает эту ОС. Блок 2 аппаратно выполняет следующие действия:

- Проводит строгую криптографическую аутентификацию пользователя.
- Осуществляет разграничение доступа к информации. У каждого пользователя свой набор полномочий, который хранится в зашифрованном виде внутри блока 2 (см. фиг.1) и передается в блок 8 или 4.
- Проводит проверку целостности загружаемой ОС. Если целостность нарушена, ОС не загружается. Об этом факте делается отметка в журнале администратора безопасности.
- Осуществляет загрузку ключей шифрования в блоки 5, 8 и 10.

Преобразование пакетов осуществляет блок 6, который выполняет следующие действия:

- Шифрование исходного IP-пакета программно (самостоятельно или с помощью отдельно подключаемого программного модуля) или аппаратно с помощью блока 5 (см. фиг.1.) Шифрование может выполняться по различным алгоритмам шифрования с применением симметричных или асимметричных ключей.
- Создание нового пакета (инкапсуляция) с включением в него зашифрованного пакета в соответствии с известными протоколами IPSec, SKIP или протоколом собственной разработки.

Вместо блоков 5 и 6 или совместно с блоком 6 может использоваться блок 10 криптографического сетевого интерфейса, который выполняет либо оба описанных выше действия, либо только первое (тогда второе действие выполняет блок 6).

Рассмотрим различные варианты конфигурации ПК, используемые при работе в защищенной виртуальной сети с определенной категорией информации, построенные на основе блочной структуры ПК, приведенной на фиг.1. Назовем эти конфигурации ПК виртуальным компьютером (ВК). В частном случае каждая конфигурация может быть единственной на компьютере, и тогда компьютер будет работать только в одной виртуальной или открытой сети. Две конфигурации ВК для открытой сети предприятия с выходом в Интернет приведены на фиг.2. Виртуальная защищенная сеть с конфиденциальной информацией может быть построена на основе конфигурации ВК фиг.3, 4. Для работы в защищенной виртуальной сети с секретной информацией предлагаются варианты реализации ВК, изображенные на фиг 5, 6. И, наконец, для работы с совершенно

секретной информацией предлагается строить виртуальную сеть на основе ВК, представленного на фиг.7.

Предлагаемые структуры носят рекомендательный характер. Пользователь вправе собрать свою конфигурацию ВК на основе предлагаемых средств (см. фиг.1).

Рассмотрим варианты работы сети, приведенной на фиг.8. Имеются три ЛВС с конфиденциальной информацией:

- ЛВС1 - сеть администрации компании. Персональный компьютер ПК31 принадлежит руководителю предприятия. На нем он работает в открытой сети Интернет, в защищенной виртуальной сети бухгалтерии ЗЛВС3 (ПК31, ПК32 из ЛВС1 и вся сеть ЛВС3), в виртуальной защищенной сети разработчиков ЗЛВС2 (ПК31, ПК32 из ЛВС1 и ПК3 ЛВС2).

- ЛВС2 - сеть разработчиков, в которой функционирует защищенная виртуальная сеть и открытая виртуальная сеть. Разработчики общаются друг с другом через виртуальную защищенную сеть, выходят в Интернет через открытую сеть. Разработчики имеют выход в Интернет со своих ПК.

- ЛВС3 - сеть бухгалтерии. Выход в Интернет из этой сети запрещен.

Для работы в трех виртуальных сетях на ПК31 и ПК32 устанавливаются три ОС (см. фиг.9). Первая ОС используется для выхода в Интернет, обмена почтой. Вторая ОС настроена на доступ в сеть разработчиков, а третья - на доступ в сеть бухгалтерии. Для перехода из одной виртуальной сети в другую достаточно перезагрузить компьютер.

ПК3 разработчиков могут быть укомплектованы более слабыми средствами защиты, как показано на фиг.10. На них устанавливаются две ОС.

Для работы с открытой, секретной и совсекретной информацией рекомендуется к использованию конфигурация, изображенная на фиг.11.

На отдельные жесткие диски или на один с шифрованными разделами устанавливаются три ОС. Первая ОС (ОС1) работает со своими разделами и настроена на использование открытого интерфейса 9. Вторая и третья ОС (ОС2 и ОС3) работают через криптографический интерфейс 10. При этом открытый интерфейс 9 блокируется устройством 2 и не функционирует при работе ОС2 и ОС3.

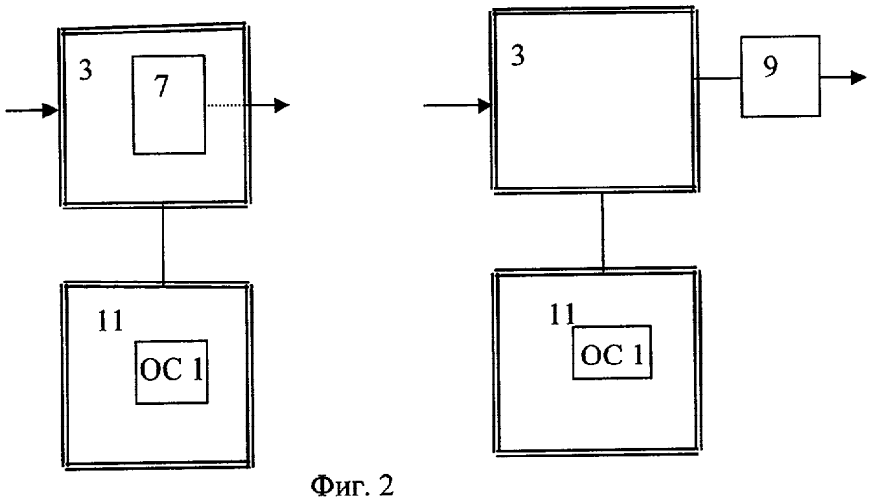
Рассмотренные примеры показывают различные возможноси практической реализации предложенного способа для построения защищенных виртуальных сетей, где с одного и того же компьютера можно выходить в различные виртуальные сети. Например, руководитель компании имея один компьютер ПК31 (см. фиг.8) у себя на столе может с него работать в Интернете и заходить в две защищенные виртуальные сети: сеть бухгалтерии и сеть разработчиков. При этом разработчики не смогут входить в сеть бухгалтерии, но могут выходить в Интернет. При работе в Интернет используется ОС1 и блокируется доступ к памяти ОС2 (рис.10). Этим предотвращается доступ к информации виртуальной сети разработчиков из Интернета. В защищенной виртуальной сети разработчиков используются ключи шифрования графика, отличные от сети бухгалтерии. Информация в каждой виртуальной сети при передаче шифруется на своих ключах, поэтому ее перехват из Интернета или другой сети, функционирующей на этом же оборудовании, становится бессмысленным.

Формула изобретения

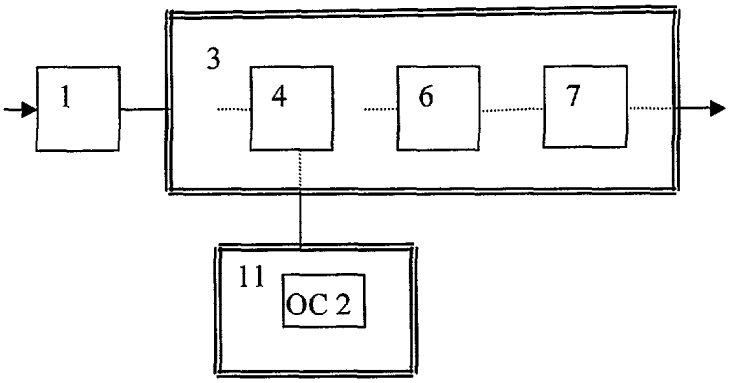
1. Способ создания защищенных виртуальных сетей, включающий шифрование исходного IP-пакета защищенной виртуальной сети, состоящей из отдельно стоящих компьютеров, или части компьютеров одной локальной сети, или компьютеров нескольких локальных сетей с сетевыми экранами и/или защищенными маршрутизаторами, с помощью размещенных на компьютерах программных модулей шифрования и инкапсуляции или аппаратных шифраторов, создание выходного пакета с включением в него зашифрованного пакета (инкапсуляцию) в соответствии с протоколами IpSec, SKIP или протоколом собственной разработки с включением идентификаторов источника и получателя сообщений, отличающийся тем, что на каждом компьютере, который может использоваться одновременно в нескольких защищенных виртуальных сетях, для каждой

создаваемой защищенной виртуальной сети выделяется отдельный блок долговременной памяти, в который записывается отдельная операционная система, настраиваемая на данную виртуальную сеть, при этом переход из одной виртуальной сети в другую осуществляется путем перезагрузки компьютера, а доступ к блоку долговременной памяти и загрузка операционной системы каждой защищенной виртуальной сети выполняется после предъявления пользователем полномочий, то есть идентифицирующей и ключевой информации, и выполнения аутентификации, причем доступ к блокам памяти каждой защищенной виртуальной сети со стороны других виртуальных сетей блокируется средством ограничения доступа.

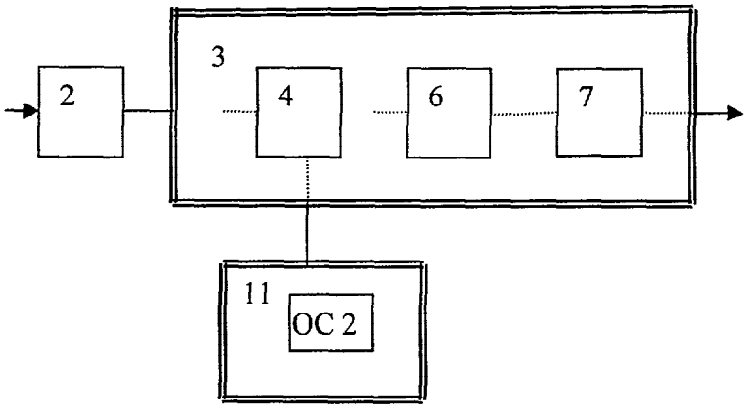
2. Способ по п.1, отличающийся тем, что дополнительная блокировка доступа к блокам долговременной памяти каждой защищенной виртуальной сети со стороны других виртуальных сетей осуществляется созданием отдельного ключа шифрования для каждого блока так, что при записи информации в блок она прозрачно зашифровывается, а при чтении - расшифровывается.



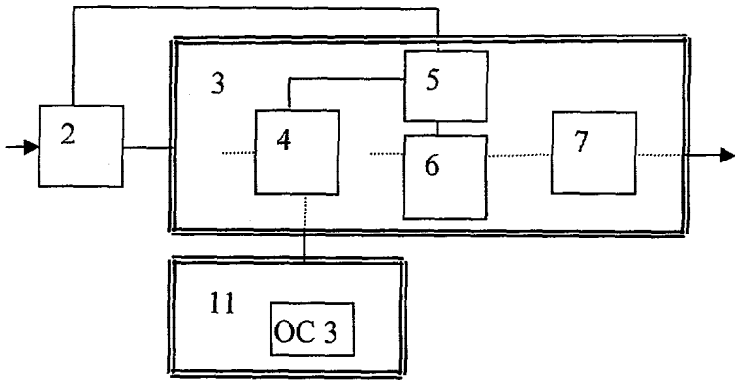
Фиг. 2



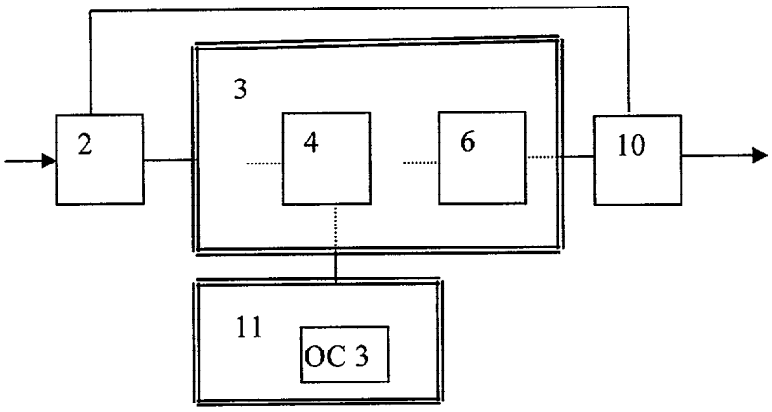
Фиг. 3



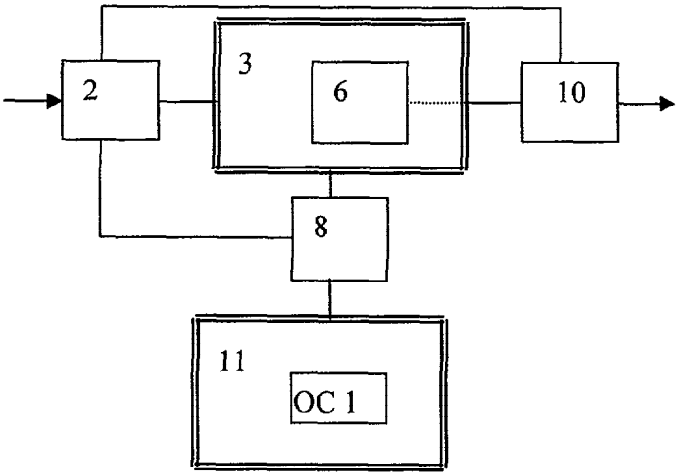
Фиг. 4



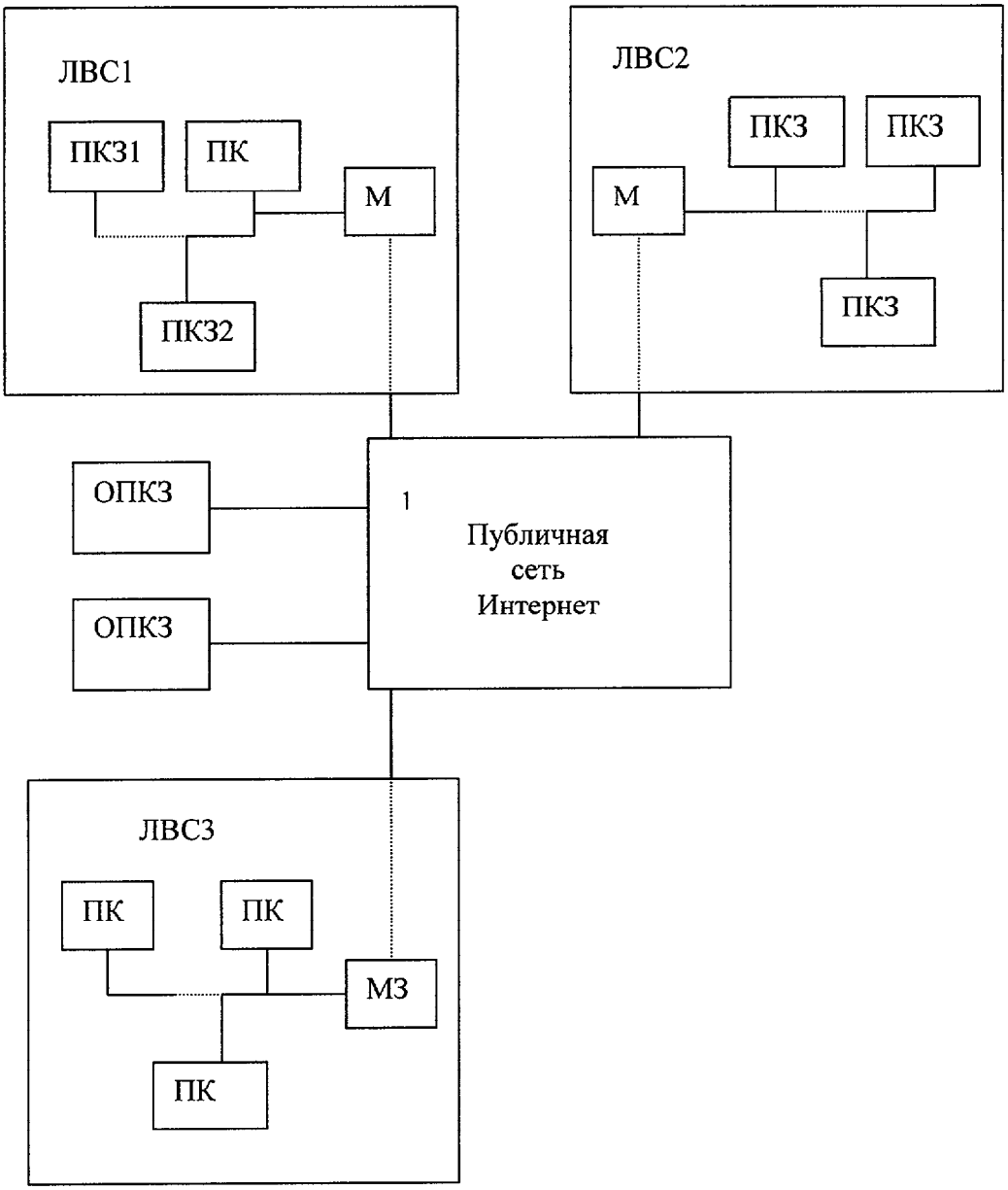
Фиг. 5



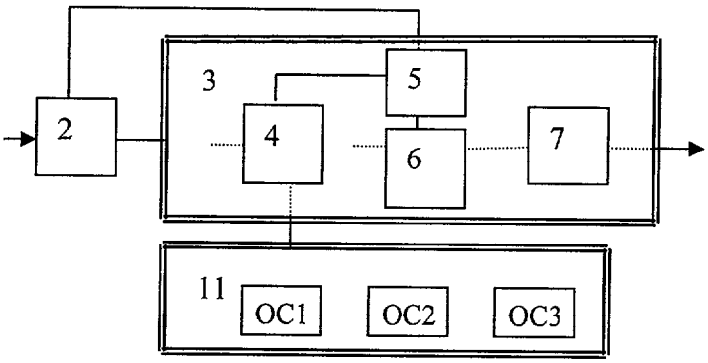
Фиг. 6



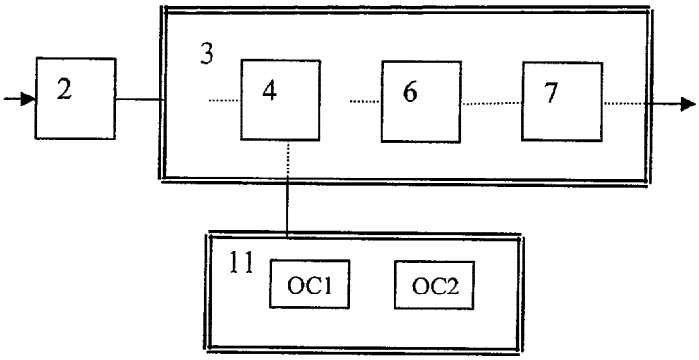
Фиг. 7


ЛВС1
ПКЗ1
ПК
М
ПКЗ2
ЛВС2
ПКЗ
ПКЗ
М
ПКЗ
ОПКЗ
ОПКЗ
1
Публичная
сеть
Интернет
ЛВС3
ПК
ПК
МЗ
ПК

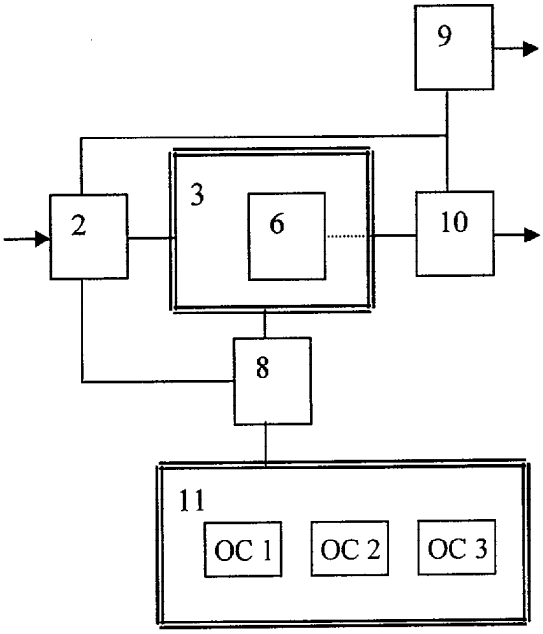
Фиг. 8


2
3
4
5
6
7
11
ОС1
ОС2
ОС3

Фиг. 9



Фиг. 10



Фиг. 11