РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 607 997**(13) **C1**

(51) МПК
G06F 15/163 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2015132590, 05.08.2015**

(24) Дата начала отсчета срока действия патента:
05.08.2015

Дата регистрации:
11.01.2017

Приоритет(ы):
(22) Дата подачи заявки: **05.08.2015**

(45) Опубликовано: **11.01.2017** Бюл. № **2**

Адрес для переписки:
119334, Москва, 5-й Донской пр-д, 15, стр. 4, Патентный отдел ООО АРК "Информ Экспресс", Фокиной Н. Л.

(72) Автор(ы):
Стародымов Георгий Александрович (RU),
Чикалев Игорь Александрович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью "Научно-Техническая Компания "Эспадон" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2214623 C2, 20.10.2003. US 2004/0013086 A1, 22.01.2004. US 2011/0035469 A1, 10.02.2011. US 2007/0153696 A1, 05.07.2007. US 2012/0317611 A1, 13.12.2012.**

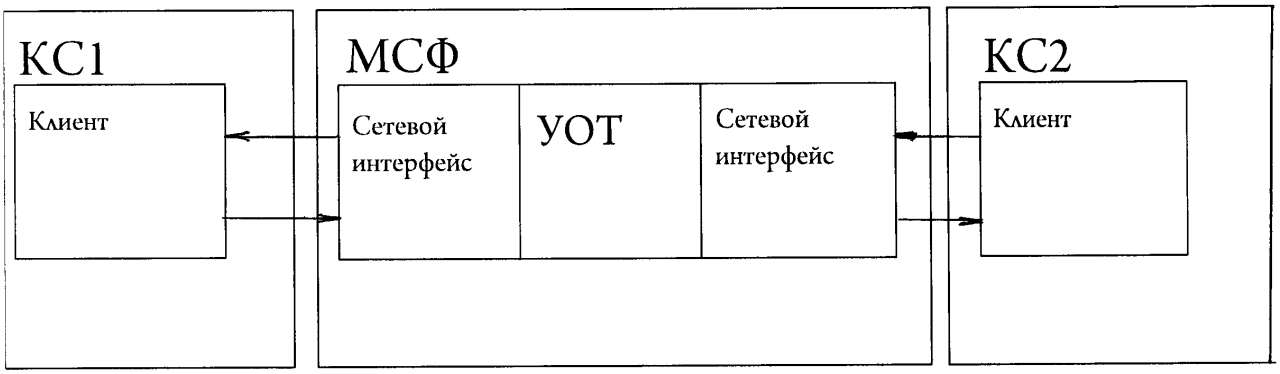
(54) СИСТЕМА ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

(57) Реферат:

Изобретение относится к вычислительной технике и сфере обеспечения информационной безопасности. Техническим результатом является защита узлов сети на основе анализа заголовка и информационной части сообщения. Система защиты компьютерных сетей от несанкционированного доступа представляет собой межсетевой фильтр, включаемый между двумя компьютерными сетями таким образом, что весь обмен информацией между указанными сетями ограничивается с помощью правил фильтрации, при этом межсетевой фильтр содержит по меньшей мере два сетевых интерфейса для обмена данными между клиентами первой компьютерной сети и второй компьютерной сети из двух вышеуказанных компьютерных сетей, при этом она дополнительно содержит узел обработки трафика, включающий устройство управления, обеспечивающее ввод правил фильтрации трафика и хранение информации о правилах фильтрации, устройство анализа трафика, обеспечивающее проверку соответствия поступающей информации правилам фильтрации, а также коммутирующее устройство, через которое указанные сетевые интерфейсы соединены между собой и которое обеспечивает прохождение разрешенной правилами фильтрации информации между сетевыми интерфейсами и блокировку неразрешенной правилами фильтрации информации, при этом правила фильтрации запрещают транзитную передачу любых пакетов между указанными сетевыми интерфейсами кроме тех, которые имеют разрешенные признаки и параметры адресации в своих заголовках, форму информационной части пакета, соответствующую шаблону, хранящемуся в памяти межсетевого фильтра, а также параметры запроса или ответа, соответствующие множеству разрешенных значений, хранящихся в памяти межсетевого фильтра. 1 з.п. ф-лы, 1 ил.

RU 2607997 C1

RU 2607997 C1



Фиг.1

RU 2607997 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 607 997**(13) **C1**

(51) Int. Cl.
G06F 15/163 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2015132590, 05.08.2015**

(24) Effective date for property rights:
05.08.2015

Registration date:
11.01.2017

Priority:
(22) Date of filing: **05.08.2015**

(45) Date of publication: **11.01.2017** Bull. № **2**

Mail address:
119334, Moskva, 5-j Donskoj pr-d, 15, str. 4, Patentnyj otdel OOO ARK "Inform Ekspress", Fokinoj N. L.

(72) Inventor(s):
Starodymov Georgij Aleksandrovich (RU),
Chikalev Igor Aleksandrovich (RU)

(73) Proprietor(s):
Obshchestvo s ogranichennoj otvetstvennostyu "Nauchno-Tekhnicheskaya Kompaniya "Espadon" (RU)

RU 2607997 C1

(54) SYSTEM FOR PROTECTING COMPUTER NETWORKS FROM UNAUTHORISED ACCESS

(57) Abstract:

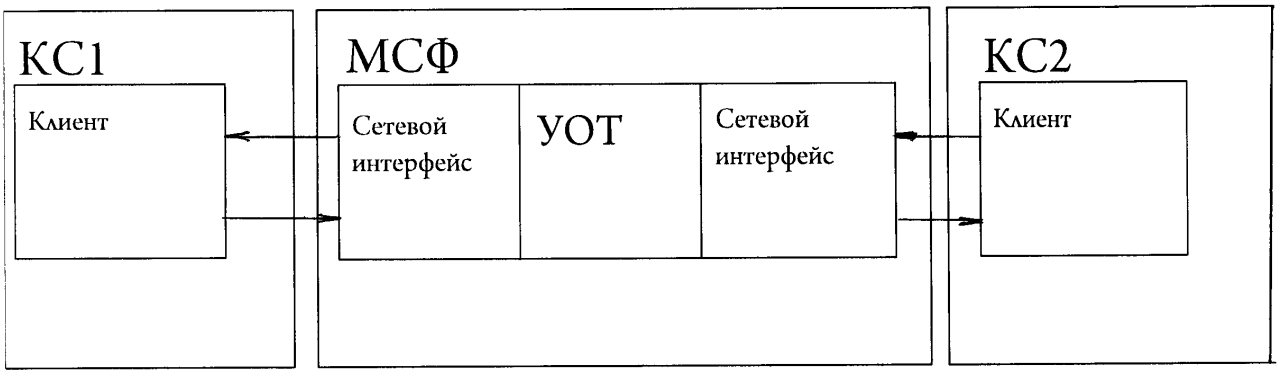
FIELD: computer engineering.

SUBSTANCE: invention relates to computer engineering and provide information security. System for protecting computer networks against unauthorized access is an internetwork filter, which is included between two computer networks so that all communication between said networks is limited by filtering rules, wherein internetwork filter comprises at least two network interfaces for communication between clients of a first computer network and a second computer network of two said computer networks, wherein it further comprises a traffic processing unit, including a control device, providing input of traffic filtering rules and storing information on filtering rules, a traffic analysis device to check conformity of incoming information with filtering rules, as well as a switching device, through which said network interfaces are interconnected and which provides flow of information allowed by filtering rules between network interfaces and blocking information prohibited by filtering rules, wherein filtering rules prohibit backhauling of any packets between said network interfaces except those having allowed features and parameters of addressing in headers, form of information part of packet corresponding to a template stored in memory of internetwork filter, as well as request or response parameters, corresponding to a plurality of permitted values stored in memory of internetwork filter.

EFFECT: technical result is protection of network nodes based on analysis of header and information part of a message.

1 cl, 1 dwg

RU 2607997 C1



Фиг.1

RU 2607997 C1

Изобретение относится к вычислительной технике и сфере обеспечения информационной безопасности и может быть использовано для управления взаимодействием двух автоматизированных систем.

Известны средства защиты периметра локальной (корпоративной) вычислительной сети, именуемые как межсетевой экран, сетевой экран, файервол, брандмауэр - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Известна система защиты сетей, содержащая две сетевые материнские платы, каждая из которых имеет сетевой интерфейсный адаптер для обмена данными с указанными сетями (RU 96118130 A).

В качестве ближайшего аналога может быть рассмотрена система защиты компьютерных сетей от несанкционированного доступа, в которой межсетевой экран содержит по меньшей мере два сетевых интерфейса для пакетной коммутации данных между сегментами вычислительной сети, выполняемой в соответствии с программой фильтрации пакетов (RU 2214623 C2).

К недостаткам известных систем можно отнести то, что они не защищают узлы сети от проникновения через разные уязвимости, не защищают от загрузки пользователями вредоносных программ, в том числе вирусов, а также не обеспечивают полную защиту от внутренних угроз, в первую очередь - утечки данных.

Задачей изобретения является создание системы защиты, основанной на анализе заголовка и информационной части сообщения. Заявленная система защиты, обладая сетевыми интерфейсами, рассматривается как адресуемый сетевой узел, то есть не использует при своем функционировании при обращении со стороны первой компьютерной сети (КС1) сетевой адрес ни одного из клиентов второй компьютерной сети (КС2).

При обращении клиента сети КС2 в сеть КС1 адрес клиента сети КС1 указывается.

Поставленная задача решается тем, что система защиты компьютерных сетей от несанкционированного доступа, представляющая собой межсетевой фильтр, включаемый между двумя компьютерными сетями таким образом, что весь обмен информацией между указанными компьютерными сетями ограничивается с помощью правил фильтрации, при этом межсетевой фильтр содержит по меньшей мере два сетевых интерфейса для обмена данными между клиентами первой компьютерной сети и второй компьютерной сети из двух вышеуказанных компьютерных сетей, отличается тем, что она дополнительно содержит узел обработки трафика, включающий устройство управления, обеспечивающее ввод правил фильтрации трафика и хранение информации о правилах фильтрации, устройство анализа трафика, обеспечивающее проверку соответствия поступающей информации правилам фильтрации, а также коммутирующее устройство, через которое указанные сетевые интерфейсы соединены между собой и которое обеспечивает прохождение разрешенной правилами фильтрации информации между сетевыми интерфейсами и блокировку неразрешенной правилами фильтрации информации.

Указанные правила фильтрации могут запрещать транзитную передачу любых пакетов между указанными сетевыми интерфейсами кроме тех, которые имеют разрешенные признаки и параметры адресации в своих заголовках, форму информационной части пакета, соответствующую шаблону, хранящемуся в памяти межсетевого фильтра, а также параметры запроса или ответа, соответствующие множеству разрешенных значений, хранящихся в памяти межсетевого фильтра, а интерфейс устройства управления узла обработки трафика защищен от

несанкционированного доступа программно-аппаратными средствами.

Межсетевой фильтр (МСФ) представляет собой специализированное сетевое устройство, которое включается между двумя компьютерными сетями таким образом, что весь обмен информацией между ними ограничивается с помощью специальных правил фильтрации.

Согласно изобретению для управления процессами фильтрации трафика МСФ содержит специальный узел обработки трафика (УОТ), устройство управления которого информационно изолировано от сетевых интерфейсов, а взаимодействие с ним осуществляется через отдельный интерфейс управления.

Все изменения программы фильтрации трафика, а также управление соединениями могут быть выполнены исключительно через интерфейс устройства управления УОТ, что полностью устраняет возможность несанкционированного доступа с МСФ со стороны сетей КС1 и КС2.

Для формирования любого обращения к клиенту КС2 клиент КС1 должен обратиться по сетевому адресу МСФ с запросом, форма которого определена протоколом обмена. При поступлении запроса УОТ определяет, от какого клиента он поступил. Если приславший запрос клиент уполномочен иметь доступ к сети КС2, проверяется форма запроса и значения параметров. Если полномочия клиента, форма запроса, значения параметров не соответствуют допустимым, зафиксированным в файле конфигурации МСФ, запрос отклоняется, событие фиксируется в памяти МСФ.

При соответствии полномочий клиента КС1, формы запроса, значений параметров допустимым, УОТ на основе запроса клиента КС1 формирует запрос в формате, присущем КС2, и отправляет его на сетевой интерфейс второй сети.

Запрос поступает в КС2, подключенную ко второму интерфейсу МСФ, далее к запрашиваемому клиенту, который откликается на запрос.

Устройство УОТ принимает ответ, обрабатывает его, формирует в соответствии с установленными протоколами, ответ с адресом клиента, приславшего запрос, и направляет его на сетевой интерфейс КС1.

Схема информационного взаимодействия МСФ и КС показана на фиг. 1.

При функционировании МСФ реализуется принцип «разрешено только то, что разрешено в явном виде», относящийся к адресам клиентов, их полномочиям, формам и параметрам запросов, формам и параметрам ответов.

Применение МСФ полностью исключает несанкционированный доступ к защищенной КС2 со стороны клиентов, не имеющих соответствующих полномочий, а также проникновения через уязвимости ПО, обеспечивает полную защиту от внутренних угроз, в том числе утечки данных, защищает от загрузки клиентами КС1 вредоносных программ, в том числе вирусов, при отсутствии у клиентов информации о протоколах обмена, формах и параметрах запросов.

Средства программирования параметров фильтрации трафика обеспечивают возможность настройки МСФ для решения различных задач.

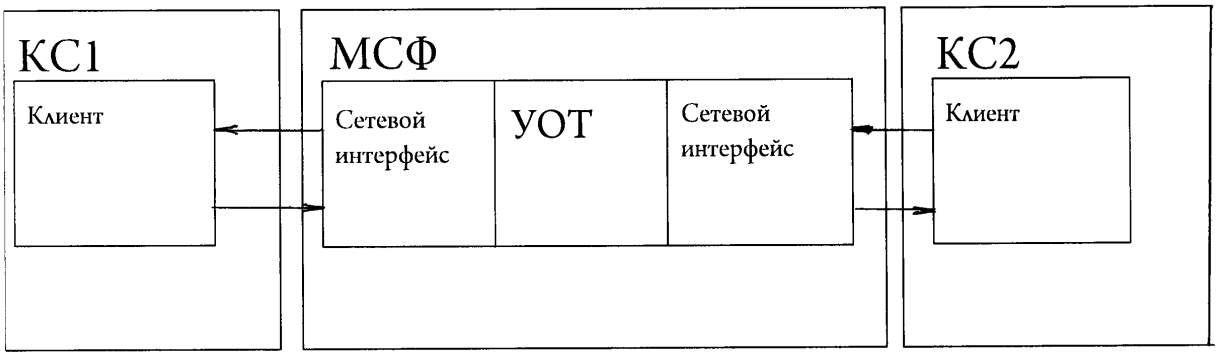
(57) Формула изобретения

1. Система защиты компьютерных сетей от несанкционированного доступа, представляющая собой межсетевой фильтр, включаемый между двумя компьютерными сетями таким образом, что весь обмен информацией между указанными сетями ограничивается с помощью правил фильтрации, при этом межсетевой фильтр содержит по меньшей мере два сетевых интерфейса для обмена данными между клиентами первой компьютерной сети и второй компьютерной сети из двух вышеуказанных компьютерных

сетей, отличающаяся тем, что она дополнительно содержит узел обработки трафика, включающий устройство управления, обеспечивающее ввод правил фильтрации трафика и хранение информации о правилах фильтрации, устройство анализа трафика, обеспечивающее проверку соответствия поступающей информации правилам фильтрации, а также коммутирующее устройство, через которое указанные сетевые интерфейсы соединены между собой и которое обеспечивает прохождение разрешенной правилами фильтрации информации между сетевыми интерфейсами и блокировку неразрешенной правилами фильтрации информации, при этом правила фильтрации запрещают транзитную передачу любых пакетов между указанными сетевыми интерфейсами кроме тех, которые имеют разрешенные признаки и параметры адресации в своих заголовках, форму информационной части пакета, соответствующую шаблону, хранящемуся в памяти межсетевого фильтра, а также параметры запроса или ответа, соответствующие множеству разрешенных значений, хранящихся в памяти межсетевого фильтра.

2. Система по п. 1, отличающаяся тем, что интерфейс устройства управления узла обработки трафика защищен от несанкционированного доступа программно-аппаратными средствами.

1


КС1
Клиент
МСФ
Сетевой интерфейс
УОТ
Сетевой интерфейс
КС2
Клиент

Фиг.1