РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 728 506**(13) **C2**

(51) МПК
G06F 21/56 (2013.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/566 (2019.08); G06F 21/577 (2019.08); H04L 29/06775 (2019.08); H04L 63/1408 (2019.08)

(21)(22) Заявка: **2018123699, 29.06.2018**

(24) Дата начала отсчета срока действия патента:
29.06.2018

Дата регистрации:
29.07.2020

Приоритет(ы):
(22) Дата подачи заявки: **29.06.2018**

(43) Дата публикации заявки: **30.12.2019** Бюл. № 1

(45) Опубликовано: **29.07.2020** Бюл. № 22

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО "Лаборатория Касперского", Управление по интеллектуальной собственности, Надежда Васильевна Кащенко

(72) Автор(ы):
Овчарик Владислав Иванович (RU),
Быков Олег Григорьевич (RU),
Сидорова Наталья Станиславовна (RU)

(73) Патентообладатель(и):
Акционерное общество "Лаборатория Касперского" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 2014/0325209 A1, 30.10.2014. US 2014/0283054 A1, 18.09.2014. US 2009/0249445 A1, 01.10.2009. RU 2372650 C2, 10.11.2009. RU 2571381 C1, 20.12.2015.**

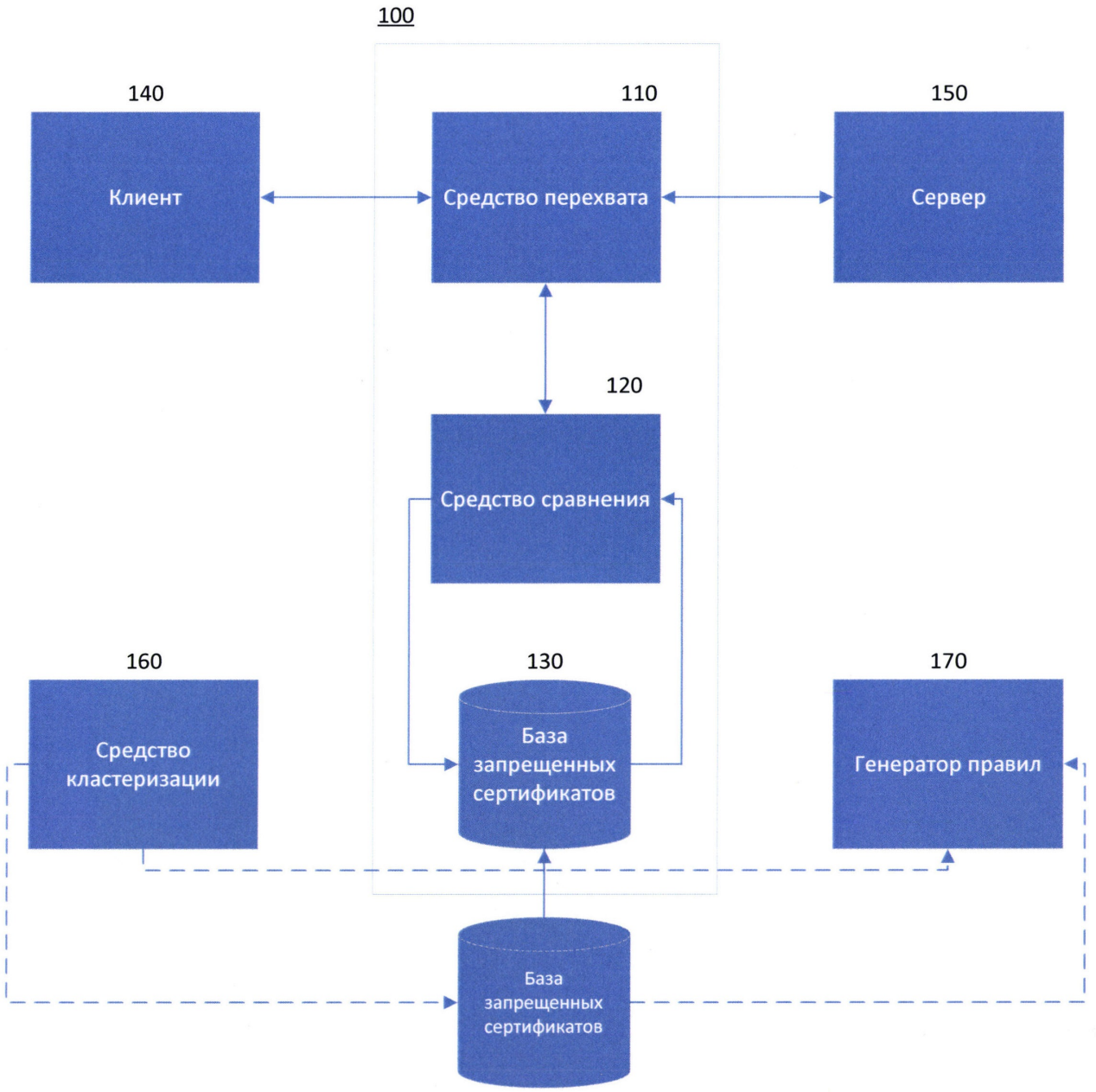
(54) Способ блокировки сетевых соединений

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в обеспечении блокировки сетевых соединений на основании сравнения цифровых сертификатов в результате осуществления способа блокировки сетевых соединений в режиме реального времени. Способ блокировки сетевых соединений в режиме реального времени, в котором перехватывают сертификат в момент установки защищенного соединения; определяют похожесть перехваченного сертификата на запрещенные сертификаты, где похожим признается сертификат, который может быть отображен на множество запрещенных сертификатов, при этом отображение проверяется посредством применения правила, сформированного из общих признаков запрещенных сертификатов, полученных в результате кластеризации множества запрещенных сертификатов; блокируют устанавливаемое соединение, если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты. 2 н. и 4 з.п. ф-лы, 7 ил.

RU 2728506 C2

RU 2728506 C2



Фиг.1

RU 2728506 C2

RU 2728506 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 728 506**(13) **C2**

(51) Int. Cl.
G06F 21/56 (2013.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/566 (2019.08); G06F 21/577 (2019.08); H04L 29/06775 (2019.08); H04L 63/1408 (2019.08)

(21)(22) Application: **2018123699, 29.06.2018**

(24) Effective date for property rights:
29.06.2018

Registration date:
29.07.2020

Priority:
(22) Date of filing: **29.06.2018**

(43) Application published: **30.12.2019** Bull. № 1

(45) Date of publication: **29.07.2020** Bull. № 22

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO "Laboratoriya Kasperskogo", Upravlenie po intellektualnoj sobstvennosti, Nadezhda Vasilevna Kashchenko

(72) Inventor(s):
Ovcharik Vladislav Ivanovich (RU),
Bykov Oleg Grigorevich (RU),
Sidorova Natalya Stanislavovna (RU)

(73) Proprietor(s):
Aktsionernoe obshchestvo "Laboratoriya Kasperskogo" (RU)

RU 2728506 C2

(54) METHOD OF BLOCKING NETWORK CONNECTIONS

(57) Abstract:

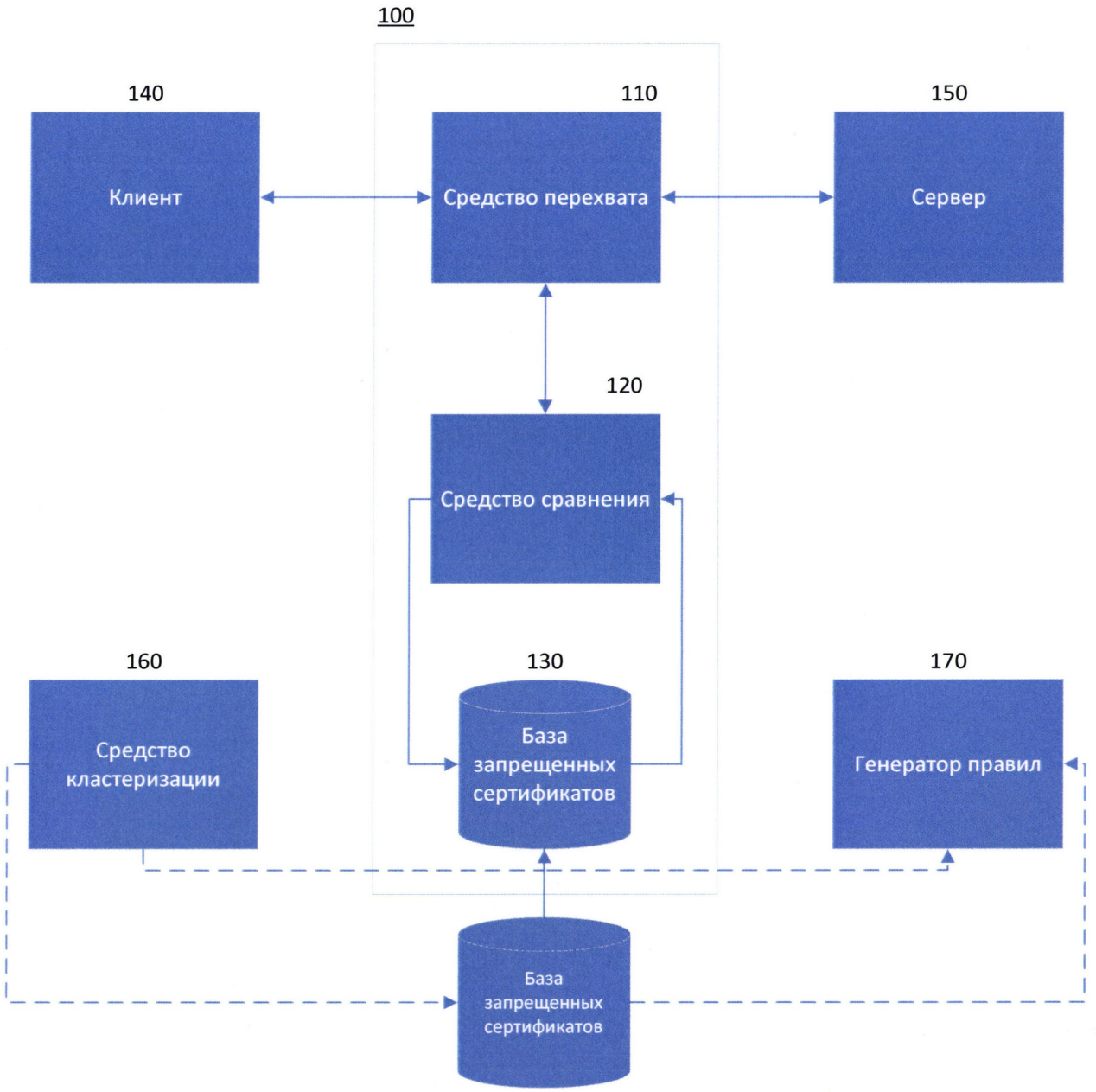
FIELD: computer equipment.

SUBSTANCE: method of blocking network connections in real time, in which a certificate is intercepted when a secure connection is established; determining similarity of intercepted certificate to forbidden certificates, where similar is recognized a certificate, which can be displayed on a plurality of prohibited certificates, wherein the display is checked by applying the rule, generated from common features of prohibited certificates obtained as a result of clustering of a plurality of prohibited certificates; blocking the installed connection, if intercepted certificate as a result of determination of similarity is recognized as similar to forbidden certificates.

EFFECT: technical result consists in providing blocking of network connections based on comparison of digital certificates as a result of real-time blocking of network connections.

6 cl, 7 dwg

RU 2728506 C2



Фиг.1

RU 2728506 C2

Способ блокировки сетевых соединений

Область техники

Изобретение относится к способам контроля и фильтрации сетевого трафика в соответствии с заданными правилами.

Уровень техники

Установка безопасных сетевых соединений с использованием криптографических протоколов позволяет избежать раскрытия передаваемых данных третьей стороне. Но как любые технологии, технологии, реализующие механизмы безопасного обмена не лишены недостатков. И в зависимости от способа исполнения могут иметь уязвимости технического или организационного характера. Например, при использовании протокола SSL совместно с протоколом HTTP злоумышленники реализуют атаку посредника, используя слабое место технологии, - операцию перенаправления на HTTPS через код ответа HTTP 302. Для осуществления атаки на точку перехода от незащищенного к защищенному каналу связи

(ГОСТ 53109-2008 Система обеспечения информационной безопасности сети общего пользования)

были созданы специальные инструменты, например, программа «SSLStrip». С использованием данного инструмента процесс атаки выглядит следующим образом:

- перехватывают трафик между клиентом и веб-сервером;
- обнаруживают адрес HTTPS URL и подменяют его адресом HTTP URL;
- предоставляют сертификаты веб-серверу и под видом клиента;
- принимают с веб-сервера траффик по защищенному каналу и перенаправляют его клиенту.

В результате атаки злоумышленник получает доступ к данным, которые клиент отправляет на веб-сервер, и веб-сервер передает клиенту.

Для защиты от этой и других подобных атак используют проверки задержки по времени, анализ сетевого трафика, анализ сертификатов. Также некоторыми компаниями используются политика доверенных сертификатов, когда допускается соединение только с ресурсами, которые находятся в белых списках и только с использованием доверенных сертификатов. Так публикация US 8966659 описывает способ обнаружения мошеннических сертификатов при установке соединения с удаленным ресурсом, посредством сравнения полученного сертификата с сертификатами, полученными от того же ресурса ранее, другая публикация US 9282092 описывает способ определения доверия при осуществлении взаимодействия клиента с онлайн-ресурсом посредством проверки цепочки сертификатов и оценки их репутации.

Использование политики доверенных сертификатов делает систему защиты не гибкой, во-первых, сертификат от того же издателя может быть изменен, и соединение станет невозможным (так как сравнение осуществляется по отпечатку, а каждый сертификат уникален), во-вторых разрешительная политика существенно ограничивает доступность сетевых ресурсов, очерчивая их только кругом доверенных. Также потенциально доверенный сертификат может быть неизвестен на текущий момент механизму защиты, так как база доверенных сертификатов не была вовремя обновлена.

Отдельно стоит отметить, что использование защищенных соединений используется в том числе и в противоправных целях, для сокрытия передаваемой информации, содержащей сведения противоправного характера. Для борьбы с подобной деятельностью блокируется уникальный сетевой адрес ресурса в компьютерной сети, который является посредником в передаче такой информации или ее источником. Но, как показывает практика, это не эффективный способ, так как адреса на которых располагаются ресурсы, могут меняться. Настоящее изобретение лишено недостатков,

описанных в уровне техники.

Раскрытие изобретения

Настоящее изобретение предназначено для блокировки сетевых соединений на основании результатов сравнения информации из перехваченных сертификатов с информацией из запрещенных сертификатов.

Технический результат настоящего изобретения заключается в обеспечении блокировки сетевых соединений на основании сравнения цифровых сертификатов в результате осуществления способа блокировки сетевых соединений в режиме реального времени, в котором перехватывают сертификат в момент установки защищенного соединения и определяют похожесть перехваченного сертификата на запрещенные сертификаты, при этом похожим признается сертификат, который может быть отображен на множество запрещенных сертификатов, при этом отображение проверяется посредством применения правила, сформированного из общих признаков запрещенных сертификатов, полученных в результате кластеризации множества запрещенных сертификатов. Если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты блокируют устанавливаемое соединение.

В частном случае из перехваченного сертификата дополнительно извлекают признаки и в этом случае правило может выражается регулярным выражением. При осуществлении способа определение похожести перехваченного сертификата на запрещенные сертификаты осуществляется посредством применения правила, где похожим признается, который удовлетворяет правилу.

Технический результат настоящего изобретения достигается также при осуществлении другого способа блокировки сетевых соединений в режиме реального времени, в котором перехватывают сертификат в момент установки защищенного соединения и определяют похожесть перехваченного сертификата на запрещенные сертификаты, но в данном случае похожим признается сертификат, который может быть отображен на множество запрещенных сертификатов, при этом отображение проверяется посредством применения метрик расстояния. Если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты блокируют устанавливаемое соединение.

Запрещенные сертификаты могут быть представлены кластером, содержащим векторы признаков запрещенных сертификатов. В частном случае из перехваченного сертификата извлекают признаки, которые преобразуются в N-мерный вектор. При преобразовании признаков сертификата в N-мерный вектор определение похожести осуществляется посредством определения расстояния между N-мерным вектором перехваченного сертификата и кластером, где перехваченный сертификат признается похожим если:

- расстояние, между N-мерным вектором сертификата и центром по кластера в N-мерном пространстве, меньше радиуса этого кластеров; или
- мера близости между N-мерным вектором элемента и центром кластера, в N-мерном пространстве, меньше порогового значения.

Краткое описание чертежей

Сопровождающие чертежи включены для обеспечения дополнительного понимания изобретения и составляют часть описания, показывают варианты осуществления изобретения и совместно с описанием необходимы для объяснения признаков изобретения.

Фиг. 1 - изображает систему блокировки сетевых соединений.

Фиг. 2 - изображает пример N-мерного пространства, векторы, кластер с его основными характеристиками.

Фиг. 3 - изображает систему категоризации сертификатов.

Фиг. 4 - изображает способ блокировки сетевых соединений.

Фиг. 5а - изображает способ блокировки сетевых соединений с формированием списка запрещенных сертификатов.

Фиг. 5б - изображает способ блокировки сетевых соединений на основании категории сетевого ресурса.

Фиг. 6 - изображает пример компьютерной системы общего назначения.

Осуществление изобретения

На Фиг. 1 изображена система блокировки сетевых соединений 100. Система 100 включает по меньшей мере средство перехвата 110, средство сравнения 120, базу запрещенных сертификатов 130. Система 100 может быть реализована, как распределенно, так и централизованно. В первом случае средство перехвата 110 и клиент 140 (которым, например, является веб-браузер) могут располагаться на одном устройстве (планшете, мобильном телефоне, персональном компьютере), средство сравнения 120 и база запрещенных сертификатов 130 могут находиться на другом устройстве локальной или корпоративной сети, в составе которой находится устройство с клиентом. В случае с централизованной реализаций система 100 полностью располагается либо на устройстве с клиентом, либо на другом устройстве (например, прокси-сервере), через которое от сервера 150 к устройству с клиентом 140 передается сетевой трафик. Средство перехвата 110 системы 100 перехватывает трафик, идущий от сервера 150 (например, веб-сервера) к клиенту (например, веб-браузеру) и извлекает сертификат, направленный от сервера клиенту 140. Перехват может осуществляться по схеме MITM (от англ. Man in the middle) и с распаковкой HTTPS трафика, если сертификат передается в защищеном тоннеле. Перехваченный сертификат от средства перехвата передается средству сравнения 120.

Средство сравнения 120 используется для того, чтобы определить, похож ли перехваченный сертификат на запрещенные сертификаты, для этого средство сравнения 120 системы 100 использует правила (в т.ч. регулярные выражения), векторы и кластеры (подробнее далее). Отдельно необходимо отметить, что определение похожести говорит о том, что определяется именно похожесть сертификатов, а не их тождественность, что существенно отличает наше изобретение от других решений, которые сравнивают полученные сертификаты с известными для определения тождественности (идентичности), например, путем сравнения отпечатков сертификатов (англ. fingerprint). Перехваченный сертификат признается похожим, если он может быть отображен (англ. mapping) на множество запрещенных сертификатов. Так как определяют похожесть перехватываемых сертификатов на запрещенные сертификаты, то используются нечеткие (англ. fuzzy) способы для определения отображения, например, регулярные выражения и метрики близости, поэтому даже если перехваченный сертификат идентичен сертификату из множества запрещенных в результате сравнения средство сравнения их признает только похожими.

Запрещенные сертификаты и/или признаки запрещенных сертификатов, кластеры, правила хранятся в базе запрещенных сертификатов 130. Сертификаты могут храниться как индивидуально (не связано), так и в списке, где список, упорядоченный по какому-либо признаку (например, владельцу сертификата, центру сертификации), - это набор сертификатов. Частным случаем списков являются кластеры, которые хранят не сами сертификаты, а их отображения - N-мерные векторы. Таким образом, база запрещенных

сертификатов может хранить: непосредственно запрещенные сертификаты; запрещенные сертификаты в списках; отображения запрещенных сертификатов, например, в виде правил, связывающих общие признаки или в виде N-мерных векторов; отображения запрещенных сертификатов в кластерах. В том случае, если база 130 хранит отображение запрещенных сертификатов в N-мерных векторах и/или кластерах, подразумевается, что база хранит модель N-мерного пространства запрещенных сертификатов.

N-мерный вектор сертификата - упорядоченный набор из n действительных чисел, где числа есть координаты вектора. Количество координат вектора называется размерностью вектора. Координаты определяют положение соответствующего сертификата или группы сертификатов от одного вида ресурсов (например, сети TOR) в N-мерном пространстве (на Фиг. 2 приведен пример двумерного пространства). Вектор получают преобразованием сведений о содержимом сертификата или группы сертификатов. Вектор отображает некоторую информацию о содержимом сертификата или группы сертификатов. В частном случае каждая координата отображает одну из характеристик сертификата, например, одна координата характеризует центр сертификации, другая владельца сертификата. Также числа могут отображать лексикографический порядок строковых параметров сертификатов или расстояние Левенштейна между строковыми параметрами разных элементов сертификата. Например, на Фиг. 2 изображены примеры векторов, в частности двумерные векторы с координатами (1666, 1889) и (1686, 1789)

Кластер - совокупность N-мерных векторов сертификатов. Перехваченный сертификат относится к некоторому кластеру, если расстояние от N-мерного вектора перехваченного сертификата до центра данного кластера меньше радиуса кластера в направлении N-мерного вектора. На Фиг. 2 в двумерном пространстве показан пример кластера. В частном случае сертификат относится к некоторому кластеру, если значение расстояния (на Фиг. 2 «d'») от N мерного вектора сертификата до ближайшего N-мерного вектора сертификата данного кластера меньше предельно допустимого (порогового значения расстояния fd'J), или если значение расстояния (на Фиг. 2 «d») от N-мерного вектора сертификата до центра данного кластера меньше радиуса этого кластера. Например, расстояние от вектора (1666, 1889) до центра кластера меньше радиуса кластера, следовательно, сертификат или группа сертификатов, содержание которых отражает вектор, принадлежат данному кластеру и напротив - расстояние от вектора (1686, 1789) до центра кластера больше и радиуса кластера, и расстояния до ближайшего N-мерного вектора больше порогового значения, следовательно, сертификат или группа сертификатов, содержание которых отражает N-мерный вектор, не принадлежат данному кластеру. Варианты расстояний для оценки близости:

- линейное расстояние;
- евклидово расстояние;
- квадрат евклидова расстояния;
- обобщенное степенное расстояние Минковского;
- расстояние Чебышева;
- Манхэттенское расстояние.

Мера близости (степень сходства, коэффициент сходства) -безразмерный показатель для определения похожести сертификатов. Типы расстояний и меры близости являются метриками расстояния. Для определения меры близости используются меры:

- Охай;
- Жаккара;
- Сокала-Снита;

- Кульчинского;
- симметричная Дайса.

Центр кластера (центроид) - это среднее геометрическое место N-мерных векторов в N-мерном пространстве. Для кластеров, состоящих из одного вектора, данный вектор будет являться центром кластера.

Радиус кластера (на Фиг. 2 «Я») - максимальное расстояние N-мерных векторов, входящих в кластер, от центра кластера.

Дополнительно в системе блокировки сетевых соединений 100 могут использоваться средство кластеризации 160 и генератор правил 170, которые обрабатывают запрещенные сертификаты, а именно:

- объединяют их в списки/кластеры;
- создают правила на основании общих признаков для сертификатов, объединенных в списки/кластеры.

Для кластеризации сертификатов используют различные известные алгоритмы и подходы, в том числе иерархические (агломеративные и дивизивные) и неиерархические. Кластеризация используется также для группировки сертификатов по общим признакам. Так после кластеризации сертификаты, векторы которых попали в один кластер, группируют в один список и формируют правило генератором правил на основании общих для сертификатов признаков (на основании которых они попали в один кластер). Правило может быть выражено в виде регулярного выражения, когда общие признаки выражены строками.

Обработка запрещенных сертификатов средством кластеризации 160 и генератором правил 170 может осуществляться удаленно, а в локальную базу запрещенных сертификатов загружаются только полученные правила. В другом частном случае средство сравнения 120 локально преобразует перехваченный сертификат в N-мерный вектор признаков, а кластеры, с которыми сравнивается полученный вектор, сохранены в удаленной базе 130.

Запрещенные сертификаты для обработки в систему 100 могут загружаться: пользователем устройства с клиентом; администратором корпоративной сети; администратором сетевого ресурса, осуществляющего контроль, диспетчеризацию и маршрутизацию трафика (например, провайдером). В общем случае отнесение сертификатов к запрещенным администраторами или пользователем не зависит от вредоносности сетевых ресурсов с которым сертификат связан. Будет тот или иной сертификат отнесен к запрещенным определяется политиками компании, предпочтениями конечных пользователей, настройками родительского контроля, требованиями местного законодательства и органов исполнительной власти, статусом самого сертификата (отозванные сертификаты, само подписанные сертификаты и т.д.)

Для поддержания работы системы блокировки сетевых соединений 100 дополнительно может использоваться система категоризации сертификатов 300, изображенная на Фиг. 3. Категоризация используется, например: в системах родительского контроля, когда нужно оградить несовершеннолетних от нежелательного контента; в системах корпоративного администрирования, когда необходимо наемным сотрудникам заблокировать доступ к развлекательным ресурсам. Способы категоризации могут быть различными, в результате осуществления которых, в частности, могут выделять такие категории ресурсов как:

- для взрослых (англ. adult content);
- программное обеспечение, аудио, видео (англ. software, audio, video);
- алкоголь, табак, наркотические и психотропные вещества (англ. alcohol, tobacco,

narcotics);

- насилие (англ. violence);
- оружие, взрывчатые вещества, пиротехника (англ. weapons);
- нецензурная лексика (англ. profanity);
- азартные игры, лотереи, тотализаторы (англ. gambling, lotteries, sweepstakes);
- средства интернет-коммуникации (англ. internet communication media);
- электронная коммерция (англ. electronic commerce);
- поиск работы (англ. recruitment);
- переадресация http-запросов (англ. http query redirection);
- компьютерные игры (англ. computer games);
- религии, религиозные объединения (англ. religions, religious associations);
- новостные ресурсы (англ. news media).

Система категоризации сертификатов 300, изображенная на Фиг. 3 предназначена для установления соответствия между сертификатами и категориями ресурсов, поэтому система 300 содержит базу категорий 310, которая включает адреса сетевых ресурсов и категории этих ресурсов. База, в частном случае, сформирована ранее и используется как есть. Система 300 содержит также базу сертификатов 320, где каждому сетевому ресурсу соответствует сертификат, который использует ресурс при установке соединения с клиентом. База сертификатов 320 системы 300 наполняется, например, системой блокировки 100. В другом случае могут использоваться базы сертификатов Microsoft, также эти способы могут использоваться совместно с другими возможными способами в различных комбинациях. База сертификатов 320 и база категорий 310 системы 300 связаны со средством категоризации 330, которое предназначено для установления соответствия между категорией сетевого ресурса и сертификатом, на основании пересечения по адресу сетевого ресурса. В результате установления соответствия средство категоризации 330 наполняет базу сертификатов по категориям. На основании полученной базы сертификатов 320 по категориям средство кластеризации 330 и генератор правил 170 наполняют базу запрещенных сертификатов 130. В базу запрещенных сертификатов 130 попадают те сертификаты или их отображения (векторы, правила, кластеры), которые относятся к категории сетевых ресурсов, доступ к которым для устройства с клиентом запрещен политиками, законом, актом органа исполнительной власти и т.д. База запрещенных сертификатов 130 будет использована в дальнейшем системой блокировки сетевых соединений 100. Средство кластеризации 160 и генератор правил 170 в другом частном случае могут использоваться для наполнения базы доверенных сертификатов 350. В базу доверенных сертификатов 350 попадают те сертификаты или их отображения (векторы, правила, кластеры) которые относятся к категории сетевых ресурсов доступ, к которым для устройства с клиентом разрешен политиками, законом, актом органа исполнительной власти и т.д. Использование системы категоризации сертификатов 300 с системой блокировки сетевых соединений 100 позволяет существенно повысить эффективность (снижение ошибок второго рода) функционирования систем администрирования компьютерных сетей и родительского контроля. Повышение эффективности достигается за счет того, что в случае смены запрещенным ресурсом сетевого адреса или сетевого сертификата, соединение с данным ресурсом будет все равно заблокировано на основании похожести перехваченного сертификата на сертификат из базы запрещенных сертификатов.

Система блокировки сетевых соединений 100 используется для осуществления способа блокировки сетевых соединений, изображенного наФиг. 4. На этапе 410, при установлении защищенного соединения между сервером 140 и клиентом 150 средством

перехвата 110 перехватывают сертификат от сервера 150. Далее на этапе 420 определяют похож ли перехваченный сертификат на запрещенные сертификаты. В зависимости от способа определения похожести и способа хранения запрещенных сертификатов в базе запрещенных сертификатов 130, перехваченный сертификат преобразуют. В частном случае из сертификата получаются признаки для построения N-мерного вектора и сравнения его с кластерами в базе запрещенных сертификатов 130, такими признаками могут быть:

- даты и время начала и окончания срока действия сертификата,
- владелец сертификата ключа подписи,
- открытый ключ,
- наименование и реквизиты центра сертификации,
- наименование криптографического алгоритма,
- информация об ограничении использования подписи,
- указание на страну выпуска сертификата,
- частотные характеристики символов сертификата,
- смещения строк в сертификате и их длина,
- и т.д.

При построении N-мерного вектора сертификата в N-мерном пространстве для каждого признака при расчете координат могут использоваться разные веса, которые, например, определяются частотой встречаемости данного признака в сертификатах (ниже частота, больше вес). Также веса могут быть рассчитаны при помощи нейросетей, например, посредством использования метода обратного распространения ошибки совместно с методом градиентного спуска. Полученный вектор сравнивается (путем определения взаимного расстояния, например, между полученным вектором и центром кластера) с кластерами запрещенных сертификатов, в частном случае кластер может быть образован N-мерным вектором только одного запрещенного сертификата. В результате сравнения перехваченный сертификат признается похожим на запрещенные, когда:

- расстояние, между N-мерным вектором сертификата и центром по меньшей мере одного кластера в базе, в N-мерном пространстве, меньше радиуса этого кластеров; или

- мера близости между N-мерным вектором элемента и центром по меньшей мере одного кластера, в N-мерном пространстве, меньше порогового значения.

Когда для сравнения используется не N-мерный вектор, а правило, например, в виде регулярного выражения к строкам из сертификата применяется это правило. Например для TOR-соединений правило выглядит следующим образом: O=, L=, S=, C=, CN=www\.[0-9a-zA-Z]+\.net. Если правило выполняется перехваченный сертификат признается похожим на запрещенные сертификаты.

Если перехваченный сертификат похож на запрещенные сертификаты, на этапе 430 данное соединение блокируется средством перехвата 110 системы 100. Блокировка данного сетевого соединения может осуществляться любыми известными из уровня техники способами.

Система категоризации сертификатов 300 и система блокировки сетевых соединений 100 используются для осуществления способа блокировки сетевых соединений с ресурсами, которые относятся к запрещенным категориям ресурсов. На этапе 510 получают список запрещенных категорий ресурсов, где в каждой категории содержатся адреса сетевых ресурсов, отнесенных к категории запрещенных. На этапе 520 получают список сертификатов и соответствующих им адресов сетевых ресурсов. Далее на этапе

530 формируют список запрещенных сертификатов на основании списка запрещенных категорий ресурсов, где к запрещенным сертификатам относят сертификаты, соответствующие адресам сетевых ресурсов, отнесенных к категории запрещенных ресурсов. На этапе 540 перехватывают сертификат в момент установки защищенного соединения и определяют на этапе 550 похожесть перехваченного сертификата на запрещенные сертификаты, если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты, на этапе 560 устанавливаемое соединение блокируется. В общем случае получают список категорий без отнесения их к запрещенным, это необходимо в случаях гибких систем, когда заранее определить запрещенную категорию невозможно, или средство блокировки сетевых соединений обслуживает несколько устройств, к которым применены разные сетевые политики. В данном случае способ будет выполняться следующим образом. На этапе 510а получают список категорий ресурсов, где в каждой категории содержатся адреса сетевых ресурсов, отнесенных к данной категории. На этапе 520 получают список сертификатов и соответствующих им адресов сетевых ресурсов. Далее на этапе 530а сертификату из полученного списка сертификатов присваивают категорию, соответствующую категории сетевого ресурса, которому данный сертификат принадлежит. На этапе 540 перехватывают сертификат в момент установки защищенного соединения клиента с сервером и на этапе 541 получают категории сетевых ресурсов соединение с которыми данному клиенту запрещено. На этапе 550 определяют похожесть перехваченного сертификата на сертификаты, которые относятся к категориям ресурсов, соединения с которыми запрещены. Если перехваченный сертификат в результате определения похожести признается похожим на указанные сертификаты, то на этапе 560 устанавливаемое соединение блокируется.

В другом случае на этапе 550 может определяться категория перехваченного сертификата путем определения похожести данного сертификата на известные сертификаты, категория которых определена, где перехваченному сертификату присваивается категория известного сертификата, на который он похож. В данном случае если определенная категория перехваченного сертификата тождественна запрещенной категории сетевого ресурса, полученной на этапе 541, соединение блокируется.

Под средством перехвата 110, средством сравнения 120, средством кластеризации 160, генератором правил 170 в настоящем изобретении понимаются реальные устройства, системы, компоненты, группа компонентов, реализованные с использованием аппаратных средств, таких как интегральные микросхемы (англ. application-specific integrated circuit, ASIC) или программируемой вентильной матрицы (англ. field-programmable gate array, FPGA) или, например, в виде комбинации программных и аппаратных средств, таких как микропроцессорная система и набор программных инструкций, а также на нейроморфных чипах (англ. neurosynaptic chips) Функциональность указанных средств может быть реализована исключительно аппаратными средствами, а также в виде комбинации, где часть функциональности реализована программными средствами, а часть аппаратными. В некоторых вариантах реализации средства могут быть исполнены на процессоре компьютера общего назначения (например, который изображен на Фиг. 6). Базы данных могут быть реализованы всеми возможными способами и содержаться как на одном физическом носителе, так и на разных, располагаться как локально, так и удаленно.

Фиг. 6 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21,

системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) 26, содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20 в свою очередь содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий диск 27, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации 56, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.), которые подключены к системной шине 23 через контроллер 55.

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35, а также дополнительные программные приложения 37, другие программные модули 38 и данные программ 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканнер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 1з через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например, колонками, принтером и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг. 6. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или

иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 50 и глобальную вычислительную сеть (WAN). Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 50 через сетевой адаптер или сетевой интерфейс 51. При использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения техническими средствами связи одного компьютера с другим.

В заключение следует отметить, что приведенные в описании сведения являются примерами, которые не ограничивают объем настоящего изобретения, определенного формулой. Специалисту в данной области становится понятным, что могут существовать и другие варианты осуществления настоящего изобретения, согласующиеся с сущностью и объемом настоящего изобретения.

(57) Формула изобретения

1. Способ блокировки сетевых соединений в режиме реального времени, в котором:

а) перехватывают сертификат в момент установки защищенного соединения;

б) определяют похожесть перехваченного сертификата на запрещенные сертификаты, где

- похожим признается сертификат, который может быть отображен на множество запрещенных сертификатов, при этом отображение проверяется посредством применения правила, сформированного из общих признаков запрещенных сертификатов, полученных в результате кластеризации множества запрещенных сертификатов;

в) блокируют устанавливаемое соединение если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты.

2. Способ по п. 1, в котором дополнительно извлекают из перехваченного сертификата признаки.

3. Способ по п. 1 или 2, в котором правило выражается регулярным выражением.

4. Способ по п. 1, в котором определение похожести перехваченного сертификата на запрещенные сертификаты осуществляется посредством применения правила, где сертификат, который удовлетворяет правилу, признается похожим.

5. Способ блокировки сетевых соединений в режиме реального времени, в котором:

а) перехватывают сертификат в момент установки защищенного соединения;

б) извлекают из перехваченного сертификата признаки и преобразуют в N-мерный вектор признаков;

в) определяют похожесть перехваченного сертификата на запрещенные сертификаты, где

- определение похожести осуществляется посредством определения расстояния между N-мерным вектором перехваченного сертификата и кластером, содержащим векторы признаков запрещенных сертификатов;

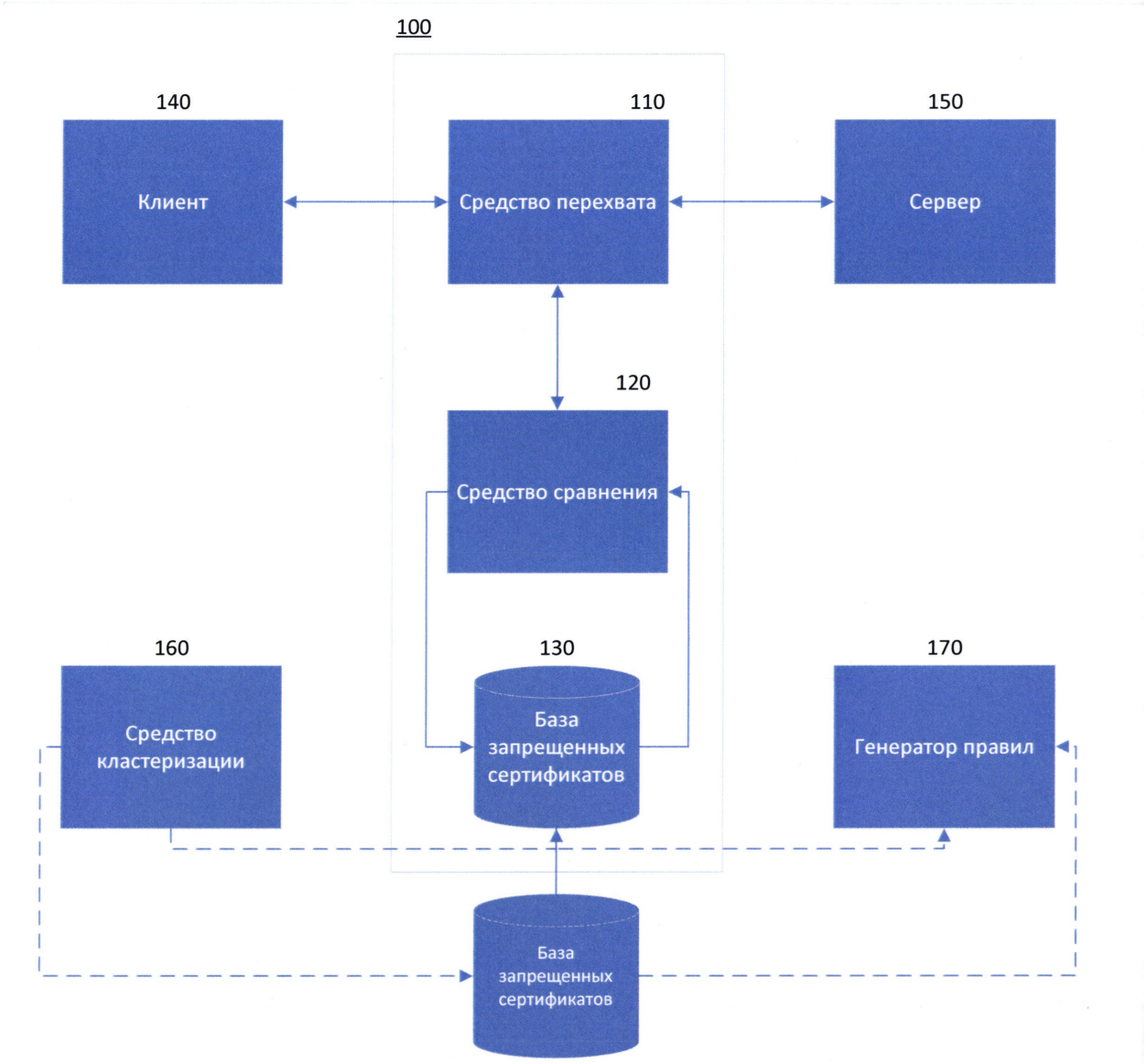
г) блокируют устанавливаемое соединение, если перехваченный сертификат в результате определения похожести признается похожим на запрещенные сертификаты.

6. Способ по п. 5, в котором перехваченный сертификат признается похожим, если:

- расстояние между N-мерным вектором сертификата и центром кластера в N-мерном пространстве меньше радиуса этого кластера или

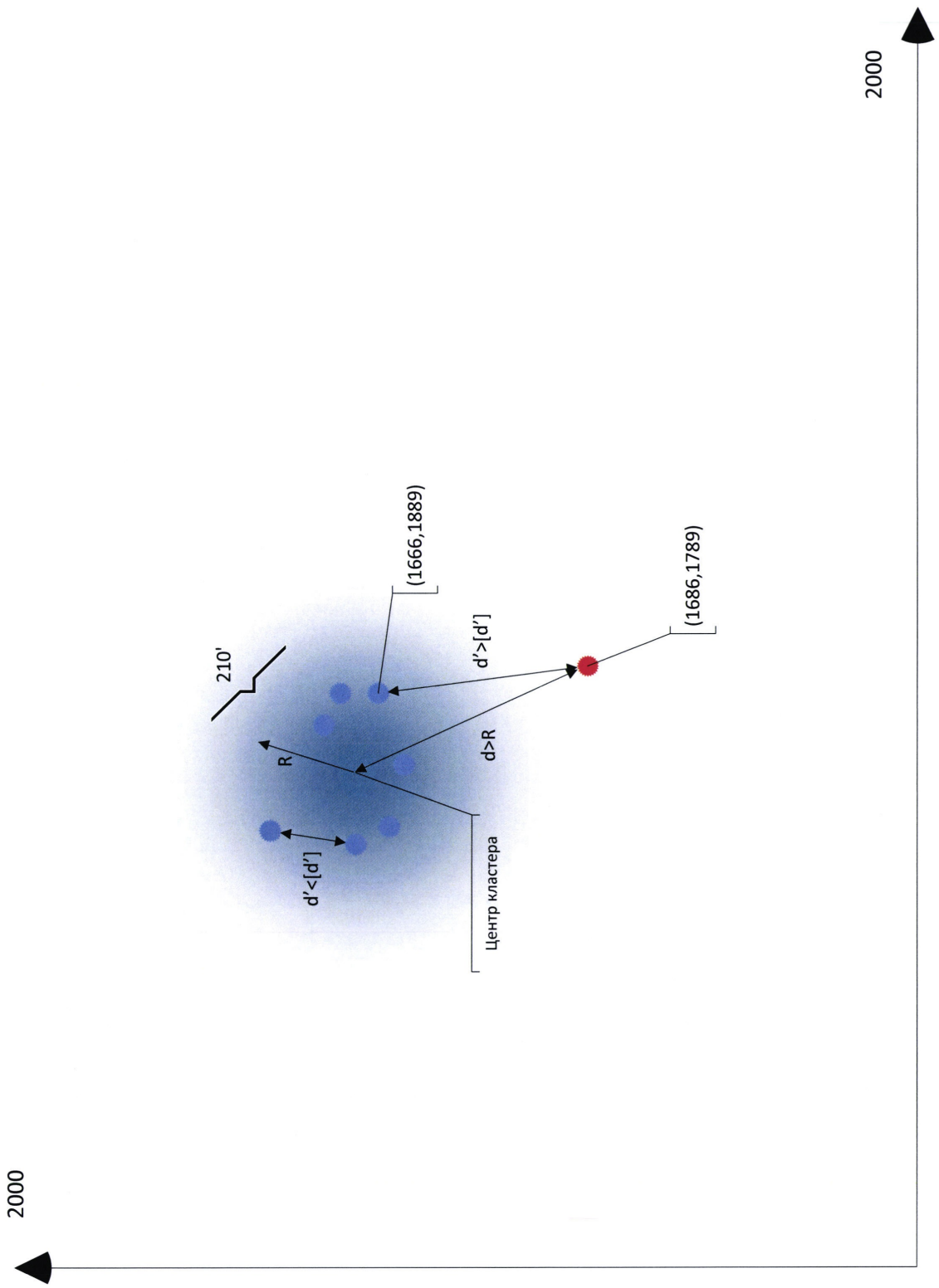
- мера близости между N-мерным вектором элемента и центром кластера, в N-мерном пространстве, меньше порогового значения.

1


100
140
Клиент
110
Средство перехвата
150
Сервер
120
Средство сравнения
160
Средство кластеризации
130
База запрещенных сертификатов
170
Генератор правил
База запрещенных сертификатов

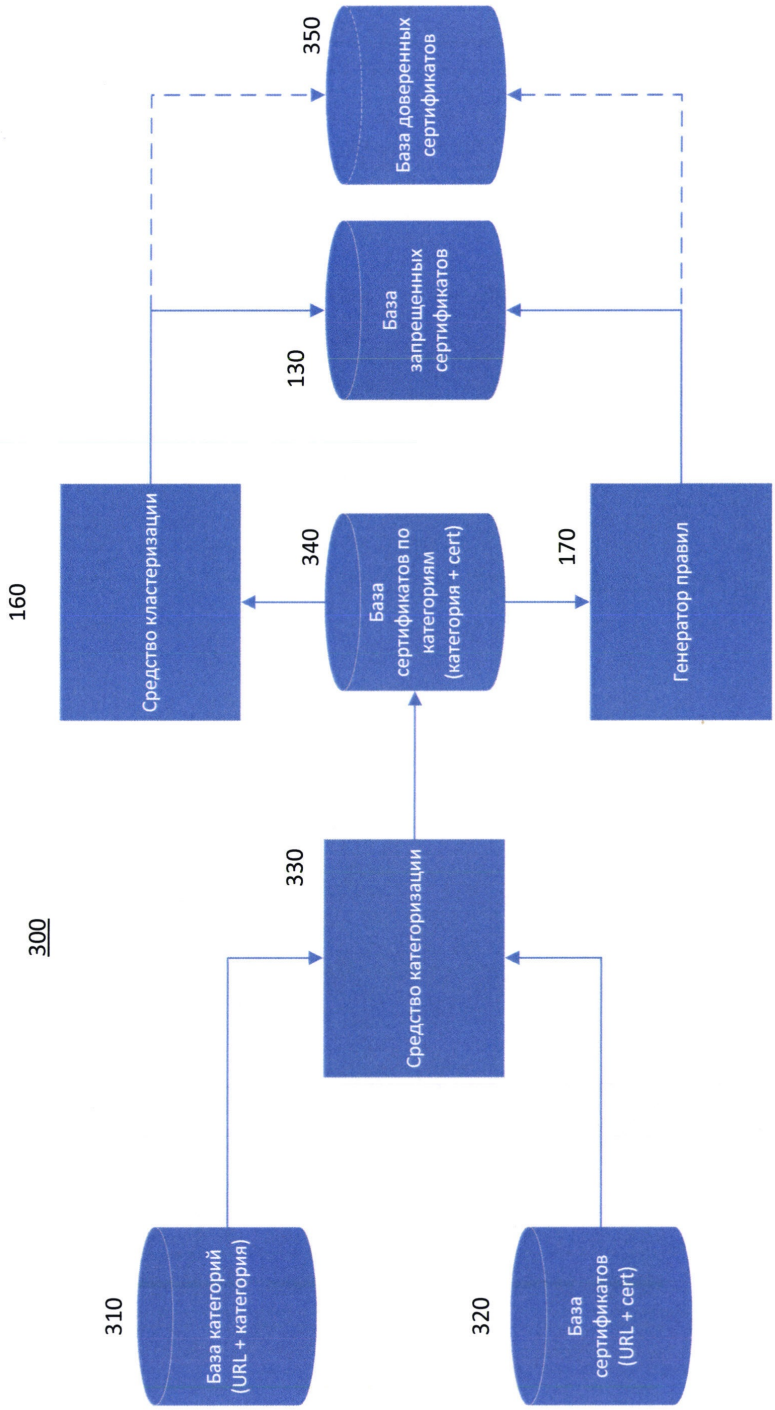
Фиг.1

2



Фиг.2

3


350
База доверенных сертификатов
130
База запрещенных сертификатов
160
Средство кластеризации
340
База сертификатов по категориям (категория + cert)
170
Генератор правил
300
330
Средство категоризации
310
База категорий (URL + категория)
320
База сертификатов (URL + cert)

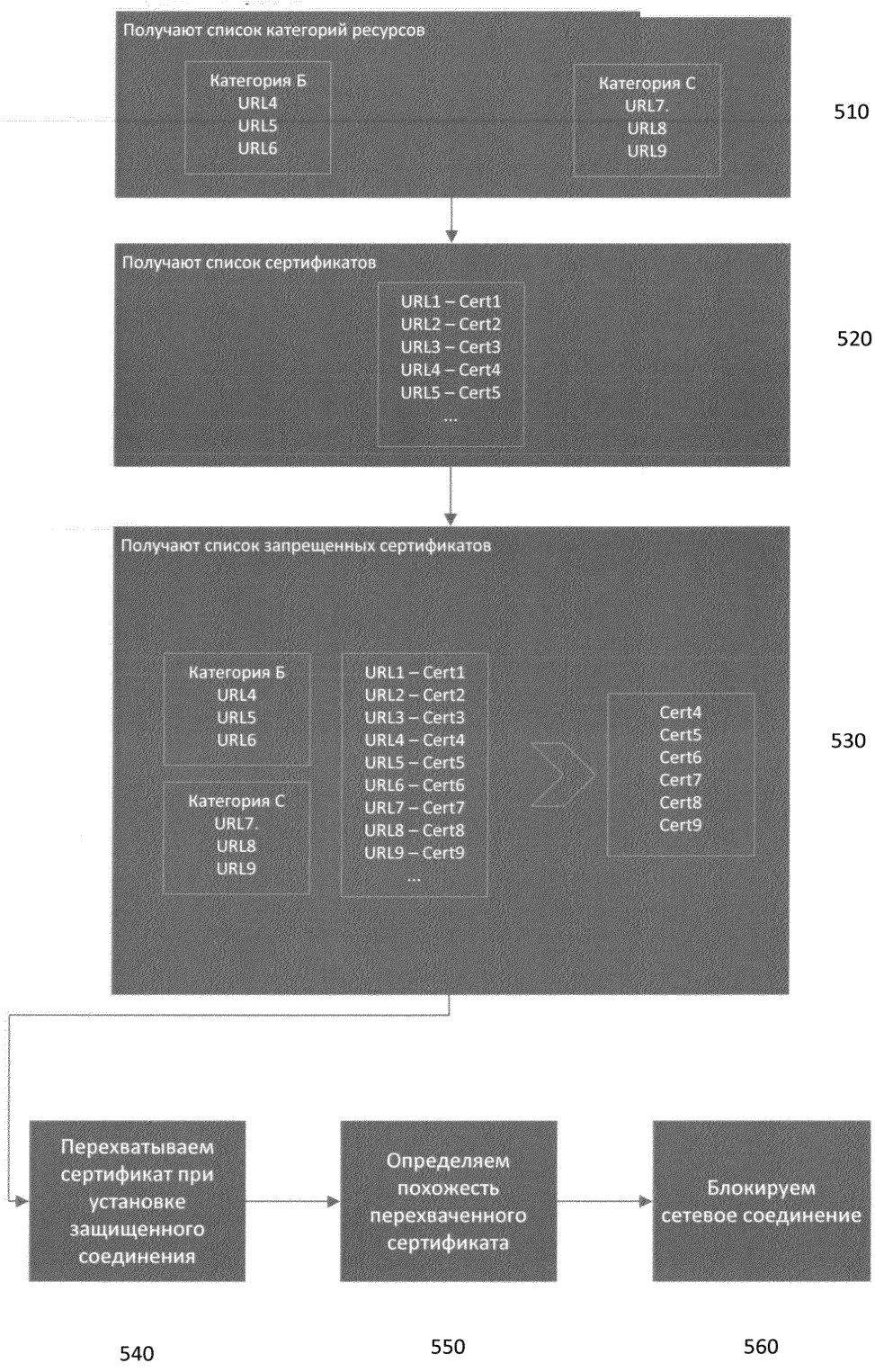
Фиг.3

4


Перехватываем сертификат при установке защищенного соединения
410
Определяем похожесть перехваченного Сертификата на запрещенные
420
Блокируем сетевое соединение
430

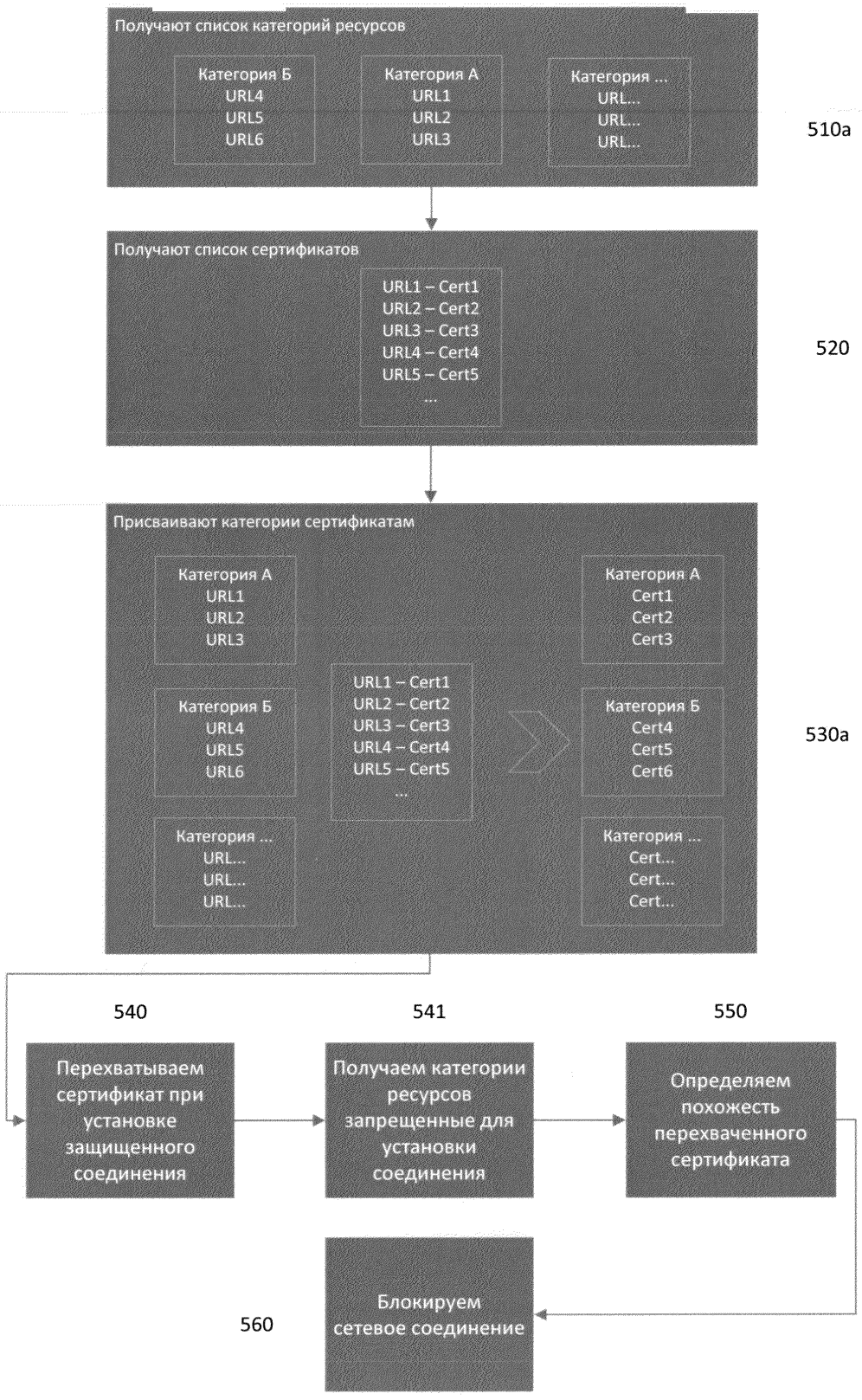
Фиг.4

5


Получают список категорий ресурсов
Категория Б
URL4
URL5
URL6
Категория С
URL7.
URL8
URL9
510
Получают список сертификатов
URL1 – Cert1
URL2 – Cert2
URL3 – Cert3
URL4 – Cert4
URL5 – Cert5
...
520
Получают список запрещенных сертификатов
Категория Б
URL4
URL5
URL6
Категория С
URL7.
URL8
URL9
URL1 – Cert1
URL2 – Cert2
URL3 – Cert3
URL4 – Cert4
URL5 – Cert5
URL6 – Cert6
URL7 – Cert7
URL8 – Cert8
URL9 – Cert9
...
Cert4
Cert5
Cert6
Cert7
Cert8
Cert9
530
Перехватываем сертификат при установке защищенного соединения
Определяем похожесть перехваченного сертификата
Блокируем сетевое соединение
540
550
560

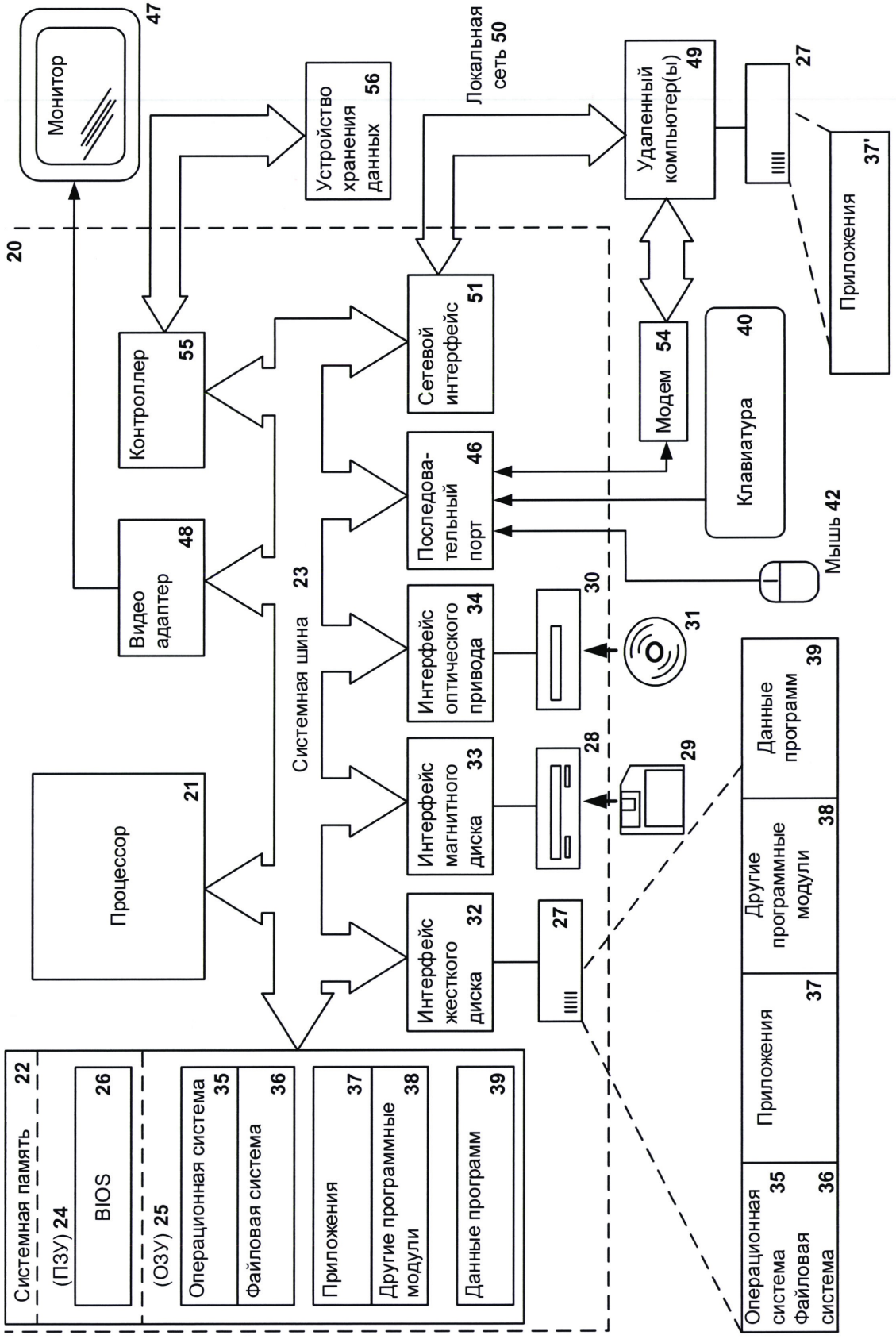
Фиг.5а

6


Получают список категорий ресурсов
Категория Б
URL4
URL5
URL6
Категория А
URL1
URL2
URL3
Категория ...
URL...
URL...
URL...
510a
Получают список сертификатов
URL1 – Cert1
URL2 – Cert2
URL3 – Cert3
URL4 – Cert4
URL5 – Cert5
...
520
Присваивают категории сертификатам
Категория А
URL1
URL2
URL3
Категория Б
URL4
URL5
URL6
Категория ...
URL...
URL...
URL...
URL1 – Cert1
URL2 – Cert2
URL3 – Cert3
URL4 – Cert4
URL5 – Cert5
...
Категория А
Cert1
Cert2
Cert3
Категория Б
Cert4
Cert5
Cert6
Категория ...
Cert...
Cert...
Cert...
530a
540
541
550
Перехватываем сертификат при установке защищенного соединения
Получаем категории ресурсов запрещенные для установки соединения
Определяем похожесть перехваченного сертификата
560
Блокируем сетевое соединение

Фиг.5б

7


Монитор 47
Устройство хранения данных 56
Локальная сеть 50
Удаленный компьютер(ы) 49
27
Приложения 37'
20
Контроллер 55
Сетевой интерфейс 51
Модем 54
Клавиатура 40
Видео адаптер 48
Последова-тельный порт 46
Мышь 42
Системная шина 23
Интерфейс оптического привода 34
30
31
Процессор 21
Интерфейс магнитного диска 33
28
29
Данные программ 39
Другие программные модули 38
Интерфейс жесткого диска 32
27
Приложения 37
Операционная система 35
Файловая система 36
Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг.6