(19) Евразийское патентное ведомство

(21) 201891320 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2019.11.29

(22) Дата подачи заявки
2018.06.29

(51) Int. Cl. ***H04M 3/436*** (2006.01)
H04M 15/00 (2006.01)

(54) ПЛАТФОРМА ДЛЯ ОБНАРУЖЕНИЯ НЕЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ И МОШЕННИЧЕСТВА В ДЕЙСТВУЮЩЕЙ СЕТИ ПРИМЕНИТЕЛЬНО К ТЕЛЕФОННОЙ СЕТИ

(31) **15/979,859**
(32) **2018.05.15**
(33) **US**

(71) Заявитель:
ЛЕВИ ДИНОР АДАМ ВЕСТЕРГАРД (ES)

(72) Изобретатель:
Леви Динор Адам Вестергард (ES), Хальперин Арик, Трабельси Ярив (IL)

(74) Представитель:
Медведев В.Н. (RU)

(57) Процессор сервера обнаружения, подсоединенного к телефонной сети, может быть выполнен с возможностью обнаружения события вызова, происходящего в текущий момент. Процессор может быть выполнен с возможностью анализа данных, связанных с событием вызова, для определения того, что вызов, запускающий событие вызова, приведет к неэффективности в телефонной сети в ответ на стандартную обработку вызова телефонной сетью. Процессор может быть выполнен с возможностью предписывать телефонной сети обрабатывать вызов нестандартным образом, предотвращая тем самым неэффективность.

201891320 A1

201891320 A1

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

2420-550672EA/061

ПЛАТФОРМА ДЛЯ ОБНАРУЖЕНИЯ НЕЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ И МОШЕННИЧЕСТВА В ДЕЙСТВУЮЩЕЙ СЕТИ ПРИМЕНИТЕЛЬНО К ТЕЛЕФОННОЙ СЕТИ

ПЕРЕКРЕСТНАЯ ССЫЛКА НА РОДСТВЕННЫЕ ЗАЯВКИ

Эта заявка основана и **притязает на приоритет** ранее поданной заявки на патент США № 15/979,859 от 15 мая 2018 г. Полное содержание этой заявки во всей полноте включено в настоящий документ посредством ссылки.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

ФИГ. 1 показывает примерную платформу обнаружения неэффективности и мошенничества согласно варианту осуществления изобретения.

ФИГ. 2 показывает примерный сервер согласно варианту осуществления изобретения.

ФИГ. 3 показывает примерный процесс анализа и классификации вызова согласно варианту осуществления изобретения.

ФИГ. 4 показывает примерный процесс тестирования правил часовых поясов согласно варианту осуществления изобретения.

ФИГ. 5 показывает примерный процесс тестирования правил геолокации согласно варианту осуществления изобретения.

ФИГ. 6 показывает примерный процесс тестирования задержанного прекращения разговора согласно варианту осуществления изобретения.

ФИГ. 7 показывает примерный процесс тестирования голоса согласно варианту осуществления изобретения.

ФИГ. 8 показывает примерную диаграмму состояний эскалации вызовов согласно варианту осуществления изобретения.

ФИГ. 9 показывает процесс принудительного выполнения согласно варианту осуществления изобретения.

ФИГ. 10 показывает эвристическую таблицу согласно варианту осуществления изобретения.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

Системы и способы, описываемые здесь, могут облегчить обнаружение и предотвращение в реальном времени неэффективности использования и мошенничества в сети внутри телефонной сети.

Например, платформа, описываемая здесь, может быть способной предупреждать продавцов провайдеров телефонных услуг, что трафик вызовов, который может привести к неэффективности использования и мошенничеству в сети (например, к мошеннической и/или неэффективной для сети транзакции), предпринимается или выполняется в сети, и/или блокировать трафик вызовов от прохождения через сеть.

Эта платформа может обладать способностью к классификации вызовов, подлежащих выполнению, как неэффективных и/или мошеннических, используя ряд конфигурируемых правил, эвристических и/или определяемых с помощью машинного обучения данных из реального трафика. Голосовой трафик может быть объявлен системой неэффективным и/или мошенническим, если он производит шаблон, значительно отличающийся от регулярного VoIP трафика, и/или несет в себе характеристики, подобные неэффективным и/или мошенническим характеристикам, которые определены, например, системой или данными машинного обучения. Система может быть способной к обнаружению неэффективного и/или мошеннического трафика, когда он возникает реально, и предотвращению влияния неэффективных и/или мошеннических действий на трафик и/или производительность сети. Примеры возможных неэффективных и/или мошеннических действий могут включать в себя, не ограничиваясь этим, следующие:

вызовы от или на номера не из числа определенных телефонной системой,

пропорционально ненормальное число вызовов в необычные часы дня (например, вызовы между одним поясом в 3 часа утра и другим поясом в 6 часов утра),

несоразмерное число вызовов между областями народонаселения,

несоразмерное число вызовов от или на ряд номеров, более длительных, чем обычно, или очень коротких.

Перечисленные ниже определения и принципы могут быть полезными для понимания систем и способов, описанных здесь.

i. Обнаружение в платформе, описываемой здесь, может быть определено, используя ряд правил, которые подробно раскрывают,

как можно классифицировать вызов в качестве мошеннического или приводящего к неэффективности сети.

ii. Входящие несущие: несущие, которые принимают вызовы и используют платформу для подтверждения их правомочности.

iii. Исходящие несущие: несущие, которые являются целям вызовов, проверенных платформой.

iv. Сервер сигнализации: шлюз к телефонной системе, управляющий сигнализацией в телефонной сети.

v. Регион: телефонная система может быть развернута в нескольких географических регионах, и каждый регион может иметь сервер сигнализации, ответственный за поступающий телефонный трафик.

vi. Региональный сервер: сервер, используемый сервером сигнализации с целью классификации вызовов как мошеннических или приводящих к неэффективности сети, и классификации вызовов как легитимных.

vii. Центральный сервер: сервер для системы обнаружения мошенничества или неэффективности, который содержит главную базу данных системы.

viii. Легитимный вызов: вызов, который является частью нормального трафика телефонной системы и не направлен на совершение мошенничества в системе или возникновение неэффективности.

ix. Таблица регистрации вызовов: содержит регистрацию вызовов, время, когда они были сделаны, часовые пояса источника и пункта назначения, географические местоположения источника и пункта назначения.

x. Таблица правил часовых поясов: содержит пары часовых поясов для каждого часа и каждого дня года, определяя максимальное ожидаемое число вызовов между часовыми поясами для каждого дня и часа.

xi. Таблица правил геолокации: содержит пары географических местоположений для каждого часа и каждого дня года, определяя максимальное ожидаемое число вызовов между парами географических местоположений для каждого дня и часа.

xii. Эвристика: правило, которое объявляет вызов как

мошеннический или неэффективный для сети, если он обладает определенными свойствами.

xiii. Таблица политики сбоев: политика, которая определяет, сбросить ли вызов, основываясь на его исходящей и входящей несущих.

xiv. Компонент принятия решения о мошенничестве: группа блоков принятия решения, каждым из которых должен быть утвержден вызов, для того чтобы вызов был объявлен приемлемым вызовом.

xv. Анализатор трафика: компьютер, который просматривает события протокола и данные трафика, и генерирует события, относящиеся к вызовам.

xvi. База данных телефонных номеров: база данных, которая содержит данные по телефонным номерам, перечисляя возможные правомочные номера с указанием географического местоположения и часового пояса для каждого номера.

xvii. Контроль ложного ответа (FAS): ситуация, при которой лицо, принимающее вызов, имитирует ложный ответ на вызов, для того чтобы запустить ложную оплату вызова.

xviii. Wangiri мошенничество в сети: тип мошеннического действия в сети, когда лицо, совершающее мошенническое действие в сети, звонит с определенного ряда номеров на номера в пункте назначения и отключатся, прежде чем получающее вызов лицо сможет ответить, в попытке принять ответный вызов.

xix. Время отмены: продолжительность между инициаций вызова и временем, кода вызов отменяется с вызывающей стороны.

xx. Задержанное прекращение разговора: ситуация, кода получающее вызов лицо задерживает прекращение ответа, для того чтобы искусственно продлить вызов.

xxi. Степень свободы в шаблоне набираемого номера: число цифр с правой стороны номера, которые не являются частью шаблона. Например, шаблон из 5 цифр для номеров из 6 цифр имеет 1 степень свободы, шаблон из 4 цифр имеет 2 степени свободы.

xxii. Окно вызова: период времени, в течение которого каждый инициированный вызов считается принадлежащим этому окну.

xxiii. Продолжительность окна вызова: длина окна вызова.

xxiv. Операция подрезки (trim (n)): процесс удаления n цифр

с правой стороны номера. Если мы используем номер с размером N=m+n и исключаем N.trim(n), мы получим последовательность S с размером m. Тогда мы можем сказать, что S=N.trim(n).

xxv. Инициация вызова: процесс набора номера, в котором после инициации инициатор ожидает принятия или отклонения вызова.

xxvi. Окончание вызова: процесс окончания вызова, который происходит, когда одна из сторон сигнализирует, что хочет завершить вызов и другая сторона соглашается с этим.

На фиг. 1 показана примерная платформа 100 для обнаружения неэффективности и мошенничества согласно варианту осуществления изобретения. Платформа 100 может включать в себя по меньшей мере один главный сервер 110 и/или по меньшей мере один региональный сервер 120. Например, платформа 100 может включать в себя один главный сервер 110 или множество главных северов 110, выполненных с возможностью совместной или индивидуальной работы в качестве центральных компонентов платформы 100. Платформа 100 может включать в себя по меньшей мере один региональный сервер 120 в каждом регионе телефонной сети. Разделение на регионы может быть произведено любым образом. Например, может быть региональный сервер 120 в каждой географической области, такой как страна, в каждом городе или в некотором другом региональном подразделении.

Главный сервер 110 может принимать данные 102 вызовов от анализатора трафика. Главный сервер 110 может включать в себя модуль 112 обнаружения, выполненный с возможностью анализировать данные 102 и поднимать тревогу, когда данные 102 указывают на то, что вызов может быть мошенническим для сети. Модуль 112 может использовать данные из базы данных 114 часовых поясов и/или демографической базы данных 116 для анализа данных 102. Тревожные предупреждения могут посылаться региональным серверам 120 для принудительного выполнения и/или могут храниться (например, в базе данных 118 тревожных предупреждений). Например, главный сервер 110 может регистрировать вызовы с их географическими местоположениями и часовыми поясами, и моментами времени для начала вызова, временем окончания запроса и

окончания вызова. Генерация тревожных предупреждений подробно описана ниже. Примеры ситуаций, в которых могут подаваться тревожные предупреждения, включают в себя, не ограничиваясь этим, следующие:

подозрение на FAS, используя анализ голоса или эвристику обнаружения мошеннических действий,

задержанное прекращение разговора,

шаблоны мошеннических вызовов,

необычная частота вызовов между географическими местоположениями,

необычная частота вызовов между часовыми поясами.

Каждый региональный сервер 120 может включать в себя региональный модуль 112 обнаружения, который может принуждать к выполнению правил, основываясь на тревожных предупреждениях, генерируемых главным сервером 110. Региональный сервер 120 может включать в себя подчиненную базу данных 124 часовых поясов, подчиненную демографическую базу данных 126 и/или подчиненную базу данных 118 тревожных предупреждений. В некоторых вариантах осуществления региональный сервер 120 может включать в себя только подчиненную ступень базы данных 118 тревожных предупреждений и может не иметь базы данных 124 часовых поясов и демографической базы данных 126. Региональный модуль 112 обнаружения может осуществлять доступ к тревожным предупреждениям в подчиненной ступени базы данных 118 тревожных предупреждений и/или принимать тревожные предупреждения от главного сервера 110. Региональный модуль 112 обнаружения может принуждать к выполнению правил обнаружения, основываясь на информации, собранной главным сервером 110, и/или подтверждая правомочность номеров, используемых для источника и пункта назначения вызовов, поступающих в телефонную систему. Принуждение к выполнению и подтверждение правомочности описываются подробно ниже.

Региональный сервер 120 может находиться в связи с сервером 130 сигнализации, который может быть выполнен с возможностью разрешения или отклонения соединения вызовов, основываясь на процессах принуждения к выполнению и подтверждения

правомочности, описанных здесь. В примере на фиг. 1 сервер 130 сигнализации представлен как отдельный от регионального сервера 120 элемент (например, отдельный сервер, находящийся в связи с региональным сервером 120), но в некоторых вариантах осуществления сервер 130 сигнализации может быть компонентом регионального сервера 120, или региональный сервер 120 может быть компонентом сервера 130 сигнализации. Как более подробно описано ниже, региональный сервер 120 может сообщать связанные с вызовом тревожные предупреждение серверу 130 сигнализации, а сервер 130 сигнализации может определять, разрешать или отклонять вызовы, основываясь на тревожных предупреждениях.

На фиг. 2 показана блок-схема примерного вычислительного устройства, которое может реализовывать различные признаки и процессы, описанные здесь. Например, главный сервер 110 и/или региональный сервер 120 могут иметь конфигурацию вычислительного устройства согласно фиг 2. Главный сервер 110 и/или региональный сервер 120 могут быть реализованы на любом электронном устройстве, которое работает с приложениями программного обеспечения, выведенными из откомпилированных инструкций, включая сюда, не ограничиваясь этим, персональные компьютеры, серверы, смартфоны, медиаплееры, электронные планшеты, игровые приставки, устройства электронной почты, и т.п. В некоторых реализациях главный сервер 110 и/или региональный сервер 120 могут включать в себя один или более процессоров 202, одно или более устройств 204 ввода, одно или более дисплейных устройств 206, один или более сетевых интерфейсов 208 и один или более машиночитаемых носителей 210. Каждый из этих компонентов может быть связан шиной 212.

Дисплейное устройство 206 может принадлежать к любой известной технологии отображения, включая сюда, но не ограничиваясь этим, дисплейные устройства, использующие технологию жидкокристаллических дисплеев (LCD) или светоизлучающих диодов (LED). Процессор (процессоры) 202 может использовать любую известную для процессоров технологию, включая сюда, но не ограничиваясь этим, графические процессоры и многоядерные процессоры. Устройство 204 ввода может быть любым

известным устройством ввода, включая сюда, но не ограничиваясь этим, клавиатуру (в том числе виртуальную клавиатуру), мышь, шаровой манипулятор и сенсорную площадку или дисплей. Шина 212 может быть любой известной для внутренних или внешних шин технологии, включая сюда, но не ограничиваясь этим, ISA, EISA, PCI, PCI Express, NuBus, USB, Serial ATA или FireWire. Машиночитаемый носитель 210 может быть любым носителем, который участвует в предоставлении команд процессору (процессорам) 202 для исполнения, включая сюда, не ограничиваясь этим, энергонезависимые носители (например, оптические диски, магнитные диски, флэш-память и т.п.) или энергозависимые носители (например, SDRAM, ROM, и т.п.).

Машиночитаемый носитель 210 может включать в себя различные команды 214 для реализации операционной системы (например, MaC OS®, Windows®, Linux). Операционная система может быть многопользовательской, многопроцессорной, многозадачной, в реальном времени, и т.п. Операционная система может выполнять базовые задачи, включая сюда, но не ограничиваясь этим: распознавание ввода от устройства 204 ввода; посылку выходных данных на дисплейное устройство 206; отслеживание файлов и директорий на машиночитаемом носителе 210; управление периферийными устройствами (например, дисководами, принтерами, и т.п.), которые могут управляться непосредственно или через контроллер ввода/вывода; и управление трафиком на шине 212. Команды 216 по сетевым соединениям могут устанавливать и поддерживать сетевые соединения (например, программное обеспечение для реализации протоколов связи, таких как TCP/IP, HTTP, Ethernet, телефония, и т.п.).

Команды 218 по услуге обнаружения могут включать в себя команды для модуля 112 обнаружения и/или регионального модуля 122 обнаружения, как описано здесь. Например, команды 218 по услуге обнаружения могут осуществлять мониторинг данных для выявления мошеннического трафика и/или ограничения трафика, который моет быть мошенническим.

Приложение (приложения) 220 может быть приложением, которое

использует или реализует процессы, описанные здесь, и/или другие процессы. Процессы могут быть также реализованы в операционной системе 214.

Описанные признаки могут быть реализованы в одной или более компьютерных программах, которые могут быть выполнимыми на программируемой системе, включающей в себя по меньшей мере один программируемый процессор, подсоединенный для приема данных и команд от системы хранения данных, и передачи данных и команд в эту систему, по меньшей мере одно устройство ввода и по меньшей мере одно устройство вывода. Компьютерная программа является рядом команд, которые могут быть использованы непосредственно или опосредствованно в компьютере для выполнения определенных действий или получения определенного результата. Компьютерная программа может быть написана в любой форме языка программирования (например, Objective-C, Java), включая сюда транслируемые или интерпретируемые языки, и она может быть развернута в любой форме, включая сюда форму автономной программы или модуля, компонента, подпрограммы или другую форму, пригодную для использования в вычислительной среде.

Подходящие процессоры для исполнения команд программы могут включать в себя, в качестве примера, микропроцессоры как общего пользования, так и специального назначения, и единственный процессор или один из множества процессоров или ядер любого типа компьютера. В общем случае процессор может принимать команды и данные от постоянной памяти или оперативной памяти, или от той и другой. Неотъемлемые элементы компьютера могут включать в себя процессор для исполнения команд и одно или более запоминающих устройств для хранения команд и данных. В общем случае компьютер может также включать в себя или быть функционально связан для сообщения с одним или более массовыми запоминающими устройствами с целью хранения файлов данных; такие устройства включают в себя магнитные диски, такие как внутренние жесткие диски и съемные диски; магнитооптические диски; и оптические диски. Запоминающие устройства, пригодные для реального воплощения команд и данных компьютерной программы, могут включать в себя все формы энергонезависимых запоминающих устройств, включая сюда, в

качестве примера, полупроводниковые запоминающие устройства, такие как EPROM, EEPROM и флэш-память; магнитные диски, такие как внутренние жесткие диски и съемные диски; магнитооптические диски; и CD-ROM и DVD-ROM диски. Процессор и запоминающее устройство могут быть дополнены специализированными интегральными схемами (ASIC) или внедрены в них.

Для обеспечения взаимодействия с пользователем эти признаки могут быть реализованы на компьютере, имеющем дисплейное устройство, такое как электронно-лучевая трубка (CRT) или жидкокристаллический (LCD) монитор, для отображения информации пользователю, и клавиатуру и позиционирующее устройство, такое как мышь или шаровой манипулятор, посредством которого пользователь может обеспечить ввод в компьютер.

Эти признаки могут быть реализованы в компьютерной системе, которая включает в себя серверный (back-end) компонент, такой как сервер данных, или которая включает в себя посреднический компонент, такой как сервер приложений или интернет-сервер, или которая включает в себя компонент пользовательского интерфейса (front-end), такой как клиентский компьютер, имеющий графический пользовательский интерфейс или интернет-браузер, или же любое их сочетание. Компоненты системы могут быть соединены любой формой или средой для передачи цифровых данных, такой как сеть связи. Примеры сетей связи включают в себя, например, телефонную сеть, LAN, WLAN и компьютеры и сети, формирующие интернет.

Компьютерная система может включать в себя клиентов и серверы. Клиент и сервер в общем случае могут быть удалены друг от друга и могут обычно взаимодействовать через сеть. Взаимоотношение клиента и сервера может возникать в силу компьютерных программ, исполняемых на соответствующих компьютерах и имеющих взаимоотношение клиент-сервер, связывающее их друг с другом.

Один или более признаков или этапов описываемых вариантов осуществления могут быть реализованы, используя API. API может определять один или более параметров, которые проходят между вызывающим приложением и другим программным кодом (например, операционной системой, библиотечной программой, функцией),

которая обеспечивает услугу, которая обеспечивает данные или которая выполняет операцию или вычисление. API может быть реализован как один или более вызовов в программном коде, который посылает или принимает один или более параметров через список параметров или другую структуру, основываясь на правилах поведения вызовов, определенных в документе спецификации API. Параметр может быть постоянной, ключом, структурой данных, объектом, классом объекта, переменной, типом данных, указателем, массивом, списком или другим вызовом. Вызовы и параметры API могут быть реализованы на любом языке программирования. Язык программирования может определять словарь и правила осуществления вызовов, которые программист должен использовать, чтобы получить доступ к функциям, поддерживаемым API.

В некоторых вариантах осуществления API вызов может сообщать приложению возможности устройства, работающего с приложением, такие как возможность ввода, возможность вывода, возможность обработки, возможность мощности, возможность связи, и т.п.

На фиг. 3 представлен примерный процесс 300 анализа и классификации вызова согласно варианту осуществления изобретения. Например, модуль 112 обнаружения может выполнять процесс 300, когда он принимает данные 102 вызова, как описано выше.

На этапе 302 модуль 112 обнаружения может запустить анализ вызова, основываясь на данных о событии в данных 102 вызова. Например, данные о событии, запускающие анализ, могут включать в себя данные, указывающие на начало или окончание вызова (например, запрос на соединение вызова или запрос на завершение вызова). В зависимости от того, какой тип события обнаружен (например, начало или окончание), могут выполняться разные типы анализа.

На этапе 304 модуль 112 обнаружения может анализировать данные 102 вызова, чтобы определить, являются ли запрошенные действия на вызов мошенническими или вызывающими неэффективность сети. Например, в зависимости от того, является ли запускающее событие началом или окончанием вызова, модуль 112 обнаружения

может применить одну или более эвристик и/или тестов к данным 102 вызова, чтобы оценить похожесть вызова на мошеннический или неэффективный. Примерные эвристики могут включать в себя, не ограничиваясь этим, следующие:

подтверждение правомочности номера,

эвристика по типу, времени и количеству вызовов между источником и пунктом назначения в заданное время,

эвристика по поведению при отмене вызова,

число вызовов между географическими местоположениями в заданное время,

число вызовов между часовыми поясами в заданное время,

идентификация ложного ответа, используя анализ голоса для идентификации механического голоса.

На этапе 306 модуль 112 обнаружения может классифицировать вызов, связанный с событием, основываясь на этом анализе. Например, модуль 112 обнаружения может классифицировать вызов как правильный (OK) или подозрительный. В некоторых вариантах осуществления модуль 112 обнаружения может классифицировать подозрительные вызовы на различных уровнях, указывающих уровень тяжести. Когда вызовы маркируются как подозрительные, модуль 112 обнаружения может указывать это, сохраняя предупреждения о мошенничестве или неэффективности использования в бае данных 118. Как было сказано выше, база данных 118 с тревожными предупреждениями о мошенничестве или неэффективности использования может быть повторена чрез зоны к региональным серверам 120 для принудительного выполнения. Примеры классификации вызов могут включать в себя, не ограничивая этим, следующие:

OK: вызов не подозрительный,

маркировка: вызов подозрителен, но ряд номеров, использованных для него, имел сбой только один раз, или происходил сбой вызова для пары географических местоположений или часовых поясов (например, в некоторых вариантах осуществления сбои для географических местоположений и часовых поясов могут не возрастать),

предупреждение: сбой вызова происходил дважды при

тестировании на мошенничество в сети для его номеров

блокировка: сбой вызова происходил три раза при тестировании на мошенничество в сети для его номеров.

Как было отмечено выше, модуль 112 обнаружения может использовать одну или более эвристик, которые могут определить обуславливающие тревогу шаблоны вызовов. Неограничивающий ряд образцов эвристик определен в таблице 1000 на фиг. 10.

Эвристический случай №1 может включать в себя ряды с 1 степенью свободы, одновременно производимые вызовы, продолжающиеся более 2 минут. String.trim(X) может быть определена как строка (например, номер телефона) без X правых цифр.

1. Живые вызовы из одной и той же страны могут быть сгруппированы, основываясь на последовательностях <Source.trim(1),Destination.trim(1)> (где Source - источник, Destination - пункт назначения), до 10 вызовов в группе (различие может быть только в последней цифре).

2. Любая пара <Source.trim(1),Destination.trim(1)>, которая имеет 5 вызовов или более с продолжительностью свыше 2 минут, не может принимать больше вызовов.

Эвристический случай №2 может включать в себя ряды с 2 степенями свободы с продолжительностью свыше 2 минут.

1. Живые вызовы из одной и той же страны могут быть сгруппированы, основываясь на последовательностях <Source.trim(2),Destination.trim(2)>, до 100 вызовов в группе (различие может быть только в последних двух цифрах цифре).

2. Любая пара <Source.trim(2),Destination.trim(2)>, которая имеет 10 вызовов или более с продолжительностью свыше 2 минут, не может принимать больше вызовов.

Эвристический случай №3 может включать в себя исходящий от источника ряд с 2 степенями свободы, окно вызовов продолжительностью в 1 минуту, вызовы, принадлежащие этому окну, с продолжительностью менее 15 секунд или вызовы, которые были прекращены в течение 5 секунд вслед за инициацией вызова.

Прекращенные вызовы могут быть сгруппированы, основываясь на последовательностях <Source.trim(2)>.

1. Любая последовательность<Source.trim(2)>, которая имела более 50 вызовов в последнюю минуту с продолжительностью менее 15 секунд или временем отмены менее 5 секунд, не может принимать больше вызовов.

Эвристический случай №4 может включать в себя ряд для пункта назначения с 2 степенями свободы, окно в 1 минуту, короткие вызовы.

1. Прекращенные вызовы могут быть сгруппированы, основываясь на последовательности Destination.trim(2)>.

2. Любая последовательность <Source.trim(2)>, которая имела более 100 вызовов в последнюю минуту с продолжительностью менее 2 минут или временем отмены менее 5 секунд, не может принимать больше вызовов.

Модуль 112 обнаружения может использовать компоненты обнаружения мошенничества в сети подобно эвристике, но модуль 112 обнаружения не ограничивается использованием эвристики для обнаружения. Модуль 112 обнаружения может использовать другие способы, такие как тестирование правил часовых поясов, тестирование геолокации и/или тестирование задержанного окончания разговора, как описано ниже, в дополнение или вместо эвристик, таких как те, которые описаны здесь.

На фиг. 4 показан примерный процесс 400 тестирования правил часовых поясов согласно варианту осуществления изобретения. Например, модуль 112 обнаружения может выполнять процесс 400 по обнаружении начала вызова в данных 102 вызова.

На этапе 402 модуль 112 обнаружения может идентифицировать номер телефона источника (например, номер телефона субъекта, пытающегося сделать вызов). Модуль 112 обнаружения может определить часовой пояс источника вызова, основываясь на номере телефона источника. Например, используя коды стран, коды областей и/или другое основанное на местоположении кодирование номера телефона, модуль 112 обнаружения может определить часовой пояс, из которого производится вызов.

На этапе 404 модуль 112 обнаружения может идентифицировать номер телефона пункта назначения (например, номер телефона субъекта, к которому подсоединяется вызов). Модуль 112

обнаружения может определить часовой пояс для пункта назначения вызова, основываясь на номере телефона в пункте назначения. Например, используя коды стран, коды областей и/или другое основанное на местоположении кодирование номера телефона, модуль 112 обнаружения может определить часовой пояс, в который послан вызов.

На этапе 406 модуль 112 обнаружения может определить число вызовов между номером телефона источника и номером телефона в пункте назначения для периода времени. Например, анализируя данные регистрации вызовов, модуль 112 обнаружения может определить следующее: <Number of calls> - число вызовов за последний час для пары (source t, destination tz) (источник, пункт назначения).

На этапе 408 модуль 112 обнаружения может определить максимальное число вызовов, разрешенных между часовым поясом для номера телефона источника и часовым поясом для номера телефона в пункте назначения. Например, одно или более правил, запомненных в памяти главного сервера 110, могут устанавливать предел на число разрешенных вызовов. Модуль 112 обнаружения может определить следующее: <maximum number of calls> - максимальное число вызовов, разрешенное для пары (source tz, destination tx) (источник, пункт назначения) в этот день и час.

На этапе 410 модуль 112 обнаружения может определить, превышает ли или равно определенное на этапе 406 число вызовов максимальному числу вызовов, определенному на этапе 408. Например, модуль 112 обнаружения может определить, справедливо ли выражение <number of calls> >= <maximum number of calls> (число вызовов >= максимальное число вызовов).

На этапе 412, если число вызовов больше или равно максимальному числу вызовов, модуль 112 обнаружения может генерировать тревожное предупреждение. Например, модуль 112 обнаружения может сохранять предупреждение в базе данных 118 тревожных предупреждений, которая может быть отображена как подчиненная база данных 128 тревожных предупреждений в региональном сервере 120, и/или тревожное предупреждение может быть иным образом сообщено региональному серверу 120.

На этапе 414, если число вызовов меньше максимального числа вызовов, модуль 112 обнаружения может определить, что вызов не нарушает правила часовых поясов. Исходя из предположения, что вызов не нарушает любого из других тестов (например, см. фиг. 3), модуль 112 обнаружения может разрешить вызову проходить в сеть для обработки (например, включая сюда маршрутизацию и соединение).

На фиг. 5 показан примерный процесс 500 тестирования правил геолокации согласно варианту осуществления изобретения. Например, модуль 112 обнаружения может выполнять процесс 500 по обнаружении начала вызова в данных 102 вызова.

На этапе 502 модуль 112 обнаружения может идентифицировать номер телефона источника (например, номер телефона субъекта, пытающегося сделать вызов). Модуль 112 обнаружения может определить географическое местоположение источника вызова, основываясь на номере телефона источника. Например, используя коды стран, коды областей и/или другое основанное на местоположении кодирование номера телефона, модуль 112 обнаружения может определить географическое местоположение, из которого послан вызов.

На этапе 504 модуль 112 обнаружения может идентифицировать номер телефона пункта назначения (например, номер телефона субъекта, к которому подсоединяется вызов). Модуль 112 обнаружения может определить географическое местоположение пункта назначения вызова, основываясь на номере телефона в пункте назначения. Например, используя коды стран, коды областей и/или другое основанное на местоположении кодирование номера телефона, модуль 112 обнаружения может определить географическое местоположение, в которое послан вызов.

На этапе 506 модуль 112 обнаружения может определить число вызовов между номером телефона источника и номером телефона в пункте назначения для периода времени. Например, анализируя данные регистрации вызовов, модуль 112 обнаружения может определить следующее: <Number of calls> - число вызовов за последний час для пары (source t, destination tz) (источник, пункт назначения).

На этапе 508 модуль 112 обнаружения может определить максимальное число вызовов, разрешенных между географическим местоположением для номера телефона источника и географическим местоположением для номера телефона в пункте назначения. Например, одно или более правил, запомненных в памяти главного сервера 110, могут устанавливать предел на число разрешенных вызовов. Модуль 112 обнаружения может определить следующее: <maximum number of calls> - максимальное число вызовов, разрешенное для пары (source tz, destination tx) (источник, пункта назначения) в этот день и час.

На этапе 510 модуль 112 обнаружения может определить, превышает ли или равно определенное на этапе 506 число вызовов максимальному числу вызовов, определенному на этапе 508. Например, модуль 112 обнаружения может определить, справедливо ли выражение <number of calls> >= <maximum number of calls> (число вызовов >= максимальное число вызовов).

На этапе 512, если число вызовов больше или равно максимальному числу вызовов, модуль 112 обнаружения может генерировать тревожное предупреждение. Например, модуль 112 обнаружения может сохранять предупреждение в базе данных 118 тревожных предупреждений, которая может быть отображена как подчиненная база данных 128 тревожных предупреждений в региональном сервере 120, и/или тревожное предупреждение может быть иным образом сообщено региональному серверу 120.

На этапе 514, если число вызовов меньше максимального числа вызовов, модуль 112 обнаружения может определить, что вызов не нарушает правила геолокации. Исходя из предположения, что вызов не нарушает любого из других тестов (например, см. фиг. 3), модуль 112 обнаружения может разрешить вызову проходить в сеть для обработки (например, включая сюда маршрутизацию и соединение).

На фиг. 6 показан примерный процесс 600 тестирования задержанного прекращения разговора согласно варианту осуществления изобретения. Например, модуль 112 обнаружения может выполнять процесс 600 по обнаружении окончания вызова в данных 102 вызова.

На этапе 602 модуль 112 обнаружения может определить максимальное легитимное время для окончания вызова. Например, одно или более правил, запомненных в памяти главного сервера 110 могут устанавливать предельное значение времени для окончания вызова (например, после завершения разговора). Модуль 112 обнаружения может определить следующее: ByeTimetoFinish=Call Finish Time-Call By Time (время от момента прощания до окончания=время окончания вызова-время момента прощания).

На этапе 604 модуль 112 обнаружения может определить время окончания вызова для вызова.

На этапе 606 модуль 112 обнаружения может определить, превышает ли или равно время окончания вызова для вызова на этапе 604 максимальному легитимному времени окончания вызова, определенному на этапе 602. Например, модуль 112 обнаружения может определить, справедливо ли выражение <ByteTimeToFinish> >= <MAXIMAL_LEGITIMATE_FINISH_TIME> (время от момента прощания до окончания >= максимальное легитимное время окончания).

На этапе 608, если <ByteTimeToFinish >= <MAXIMAL_LEGITIMATE_FINISH_TIME>, модуль 112 обнаружения может генерировать тревожное предупреждение. Например, модуль 112 обнаружения может сохранять тревожное предупреждение в базе данных 118 тревожных предупреждений, которая может быть отображена как подчиненная база данных 128 тревожных предупреждений в региональном сервере 120, и/или тревожное предупреждение может быть иным образом сообщено региональному серверу 120.

На этапе 610, если <ByeTimeToFinish> <MAXIMAL_LEGITIMATE_FINISH_TIME>, модуль 112 обнаружения может определить, что вызов не нарушает правила времени окончания вызова. Исходя из предположения, что вызов не нарушает любого из других тестов (например, см. фиг. 3), модуль 112 обнаружения может поднять тревогу, если более 10 вызовов на ряд номеров с одной степенью свободы проявляют такое поведение в течение периода в 1 час. В таком случае дополнительные вызовы на этот ряд номеров могут быть блокированы.

На фиг. 7 показан примерный процесс 700 тестирования голоса

согласно варианту осуществления изобретения. Например, модуль 112 обнаружения может выполнять процесс 700 часто или постоянно, кода поступают данные 102 вызова.

На этапе 702 модуль 112 обнаружения может выбрать номер телефона, на который поступает вызов, для анализа голоса. Например, модуль 112 обнаружения может анализировать данные 102 голоса, чтобы идентифицировать запрошенные соединения вызовов и выбрать один или более запрошенных вызовов для анализа голоса. В некоторых вариантах осуществления модуль 112 обнаружения может выбрать вызов для анализа голоса, если этот вызов направлен в сторону или со стороны ранее промаркированного номера (например, классифицированного как подозрительный на этапе 306 в процессе 300). В некоторых вариантах осуществления модуль 112 обнаружения может выбрать вызов для анализа голоса, если какой-то номер вызывается более определенного числа раз в течение часа.

На этапе 704 модуль 112 обнаружения может анализировать выбранный вызов. Номер, который выбирается для анализа голоса, может анализироваться программным обеспечением для анализа голоса с элементами искусственного интеллекта (AI). Голосовые векторы в звуке вызова могут анализироваться и определять, совпадают ли они (или по существу подобны) с голосовыми векторами в других вызовах на вызываемый номер (например, совпадают или подобны более чем 10 вызовам на этот номер или некоторому другому пороговому значению).

На этапе 706, если анализ голоса определят, что звук подобен другим голосовым векторам, модуль 112 обнаружения может запустить маркер мошенничества. В этом случае система может набирать номер и регистрировать вызов, созданный системой.

На этапе 708, если анализ голоса определяет, что звук не подобен другим голосовым векторам, модуль 112 обнаружения может определить, что вызов не нарушает правил анализа голоса. Исходя из предположения, что вызов не нарушает любого из других тестов (например, см. фиг. 3), модуль 112 обнаружения может объявить вызываемый номер подозрительным и блокировать последующие вызовы на этот номер.

Предшествующие описания процессов представляют примеры

тестов, которые модуль 112 обнаружения может выполнять для определения того, является ли вызов подозрительным или нет. В некоторых вариантах осуществления модуль 112 обнаружения может выполнять множество тестов на одном вызове или попытке вызова. Основываясь на этих определениях, модуль 112 обнаружения может регулировать состояние вызова, что в конечном итоге может приводить к отклонению или блокировке вызова в сети 100, если вызов достаточно подозрителен.

На фиг. 8 показана примерная диаграмма 800 состояний эскалации вызова согласно варианту осуществления изобретения. Диаграмма 800 состояний показывает пример того, как вызовы могут перерастать из нормального (ОК) состояния (не мошеннического для сети) в блокированное согласно тестированию, выполняемому модулем 112 обнаружения, как описано выше. Например, эскалация вызовов может происходить следующим образом:

ОК - вызовы, не являющиеся мошенническими для сети,

маркировка- мошеннические для сети вызовы, обнаруженные для пары номеров (источник вызова и пункт назначения вызова),

тревога - мошеннические для сети вызовы, обнаруженные снова, немного спустя после маркировки этой пары,

блокировка - возникает слишком много мошеннических событий в сети, соединение блокируется до тех пор, пока администратор не разрешит его.

Как показано на фиг. 8, эскалация между состояниями и деэскалация, когда вызовы классифицируются как легитимные, может основываться на ряде из 6 таймеров.

Пара из рядов номеров может быть в одном из 6 состояний и может совершать переход между состояниями, основываясь на тестировании, как описано выше, следующим образом:

пара ОК (802): нет подозрений в мошенничестве или неэффективности сети для пары,

пара промаркирована (804): обнаружено подозрение в мошенничестве или неэффективности сети для пары из ряда номеров,

пара ОК после маркировки (806): не было обнаружено последующих попыток мошенничества или неэффективности сети в течение времени X секунд после вхождения в маркированное

состояние,

пара в состоянии тревоги (808): была обнаружена попытка мошенничества или неэффективности сети в течение времени менее X1 после вхождения пары ОК в маркированное состояние,

пара ОК после состояния тревоги (810): не обнаружены попытки мошенничества или неэффективность сети в течение X3 секунд после вхождения в состояние тревоги,

пара блокирована (812): была обнаружена попытка мошенничества или неэффективности сети за время короче X5 после вхождения в состояние "пара ОК" вслед за состоянием тревоги,

перемещение из состояния "ОК после маркировки" (806) в состояние ОК (802): если не было обнаружено попыток мошенничества или неэффективности сети за время X2,

перемещение из состояния "пара ОК после состояния тревоги" (810) в "пара ОК после маркировки" (806): если не было обнаружено попыток мошенничества или неэффективности сети за время X4.

На фиг. 9 показан процесс 900 принуждения к выполнению согласно варианту осуществления изобретения. Как было сказано выше, сервер 120 может иметь доступ к данным анализа мошенничества или неэффективности сети, генерируемым модулем 112 обнаружения. Сервер 130 сигнализации может быть выполнен с возможностью принимать входящие вызовы и либо подсоединять их через сеть 100 к их пунктам назначения, либо отклонять их. Например, когда вызов поступает в телефонную систему, он может проходить через сервер 130 сигнализации. Сервер 130 сигнализации может отделить входящую несущую для вызова и исходящую несущую для вызова. На этапе 902 сервер 130 сигнализации может запросить региональный сервер 120 через API, не является ли этот вызов мошенническим для сети. Основываясь на процессе анализа, описанном выше, на этапе 904 региональный сервер 120 может ответить с указанием о статусе вызова (например, мошеннический или не мошеннический). Сервер 130 сигнализации может обратиться к одному или более правилам (например, к тем, которые могут быть запомнены в памяти сервера 130 сигнализации или могут быть другим образом доступны для сервера 130 сигнализации), чтобы

определить, разрешить ли или блокировать вызов, основываясь на его статусе. В первом случае сервер 130 сигнализации может обеспечивать образование соединения между конечными точками вызова через сеть 100. Во втором случае сервер 130 сигнализации может отклонять вызов, который не может войти в сеть 100.

Например, по приему вызова от сервера сигнализации на этапе 902 региональный сервер 120 может выполнять перечисленные ниже процессы для генерации ответа, посылаемого на этапе 904.

1. Проверка правомочности номеров, включенных в состав вызова.

2. Проверка базы данных тревожных предупреждений для определения того, имеет ли пара часовых поясов (источник, пункт назначения) тревожное предупреждение.

3. Проверка базы данных тревожных предупреждений для определения того, имеет ли пара географических местоположений номеров тревожное предупреждение.

4. Проверка того, имеет ли какая-либо из эвристик системы тревожное предупреждение для пары номеров вызова.

5. Проверка того, имеет ли номер пункта назначения FAS предупреждение.

6. Если тревожное предупреждение не найдено ни в каком из упомянутых компонентов, региональный сервер 120 может утвердить вызов.

7. Если тревожное предупреждение найдено, региональный сервер 120 может обратиться к тревожной конфигурации для входящей и исходящей несущих, должен ли быть блокирован вызов. Несущие могут определить, установить ли просто предупреждение или установить предупреждение и действительно блокировать подозрительные вызовы.

8. Если вызов должен быть блокирован по тревожной конфигурации, региональный сервер 120 может возвратить состояние тревоги и, в некоторых вариантах осуществления, указание блокировки для сервера 130 сигнализации. Сервер 130 сигнализации может определить, основываясь на состоянии тревоги и/или указании блокировки, блокировать ли или разрешить вызов.

Хотя выше были описаны различные варианты осуществления,

должно быть понятно, что они были представлены в качестве примера, но не ограничения. Специалистам в соответствующей области (областях) техники должно быть понятно, что различные изменения в форме и деталях могут быть произведены здесь без отклонения от сущности и объема. Фактически после прочтения представленного выше описания специалистам в соответствующей области (областях) техники станет понятно, как реализовать альтернативные варианты осуществления. Например, могут быть введены другие этапы, или же этапы могут быть исключены из описанных процессов, и другие компоненты могут быть добавлены или исключены из описанных систем. В соответствии с этим другие реализации находятся в пределах объема приведенной ниже формулы изобретения.

Кроме того, должно быть понятно, что любые чертежи, которые выявляют функциональные возможности и преимущества, представлены только в целях примера. Раскрываемые способы и система достаточно гибкие и конфигурируемые, так что они могут быть использованы другими способами, чем описанные здесь.

Хотя термин "по меньшей мере один" может быть часто использован в описании, пунктах формулы изобретения и в чертежах, термины в единственном числе, , термин "упомянутый" и т.п. также означают "по меньшей мере один" в описании, пунктах формулы изобретения и в чертежах.

Наконец, намерением заявителя было то, чтобы только те пункты формулы изобретения, которые включают в себя явно высказанное выражение "средство для" или "этап для", трактовались по 35 U.S.C. 112(f). Пункты формулы изобретения, которые явно не включают в себя выражение "средство для" или "этап для", не должны трактоваться по 35 U.S.C. 112(f).

ПРИМЕЧАНИЯ

1. На стр. 14 оригинала при описании этапов 602-610 процесса 600 использованы два разных наименования одного и того же параметра: **Byte**TimeToFinish и **Bye**TimeToFinish. Поскольку речь идет о тесте на задержанное завершение разговора, в тексте перевода этот параметр определен как "время от момента прощания (т.е. Bye Time) до окончания вызова".
2. На стр. 14 оригинала при описании этапа 610 вызывает сомнение заключение о классификации вызова как подозрительного и подлежащего блокировке, противоречащее отсутствию нарушения им правил тестирования. На фиг. 6 в блоке 610 вызов обозначен как правомочный (ОК).
3. Последний абзац описания ссылается на статью патентного права США

Переводчик Воробьев Виктор Викторович
E-mail: vovictor@yandex.ru
Тел.: +7 916 160 3373

ОПИСАНИЕ ИЗОБРЕТЕНИЯ..... 1
ФОРМУЛА ИЗОБРЕТЕНИЯ..... 24
РЕФЕРАТ..... 29
ПЕРЕВОД ЧЕРТЕЖЕЙ..... 30

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ обнаружения и предотвращения нежелательного трафика в сети, содержащий этапы, на которых:

обнаруживают посредством процессора сервера обнаружения, подсоединенного к телефонной сети, событие вызова, происходящее в текущий момент;

анализируют посредством этого процессора данные вызова, связанные с событием вызова, для определения того, что вызов, запустивший событие вызова, приведет к неэффективности в телефонной сети в ответ на стандартную обработку данного вызова телефонной сетью; и

предписывают посредством упомянутого процессора телефонной сети обработать упомянутый вызов нестандартным образом, предотвращая тем самым неэффективность.

2. Способ по п. 1, в котором событие вызова содержит начало вызова или окончание вызова.

3. Способ по п. 1, в котором упомянутый анализ содержит по меньшей мере один из этапов, на которых:

проверяют правильность номера телефона источника для упомянутого вызова;

проверяют правильность номера телефона пункта назначения для упомянутого вызова;

классифицируют упомянутый вызов, основываясь на по меньшей мере одном правиле для по меньшей мере одного шаблона вызова;

классифицируют упомянутый вызов, основываясь на числе вызовов между часовым поясом для номера телефона источника и часовым поясом для номера телефона пункта назначения;

классифицируют упомянутый вызов, основываясь на числе вызовов между географическим местоположением для номера телефона источника и географическим местоположением для номера телефона пункта назначения;

обнаруживают контроль ложного ответа;

обнаруживают быструю отмену.

4. Способ по п. 1, в котором упомянутый анализ содержит этап, на котором маркируют упомянутый вызов для дополнительного анализа.

5. Способ по п. 4, в котором упомянутый нестандартный подход к обработке вызова содержит этап, на котором выполняют посредством упомянутого процессора упомянутый дополнительный анализ.

6. Способ по п. 5, дополнительно содержащий этап, на котором предписывают телефонной сети осуществить соединение упомянутого вызова в ответ на определение при упомянутом дополнительном анализе того, что данный вызов не приведет к неэффективности.

7. Способ по п. 5, дополнительно содержащий этап, на котором предписывают телефонной сети блокировать упомянутый вызов в ответ на определение при упомянутом дополнительном анализе того, что данный вызов приведет к неэффективности.

8. Способ по п. 1, в котором упомянутый анализ содержит этап, на котором генерируют тревожное предупреждение для упомянутого вызова.

9. Способ по п. 8, в котором упомянутый нестандартный подход к обработке вызова содержит этап, на котором анализируют, посредством второго процессора регионального сервера, подсоединенного к телефонной сети, тревожное предупреждение, чтобы определить, блокировать ли упомянутый вызов.

10. Способ по п. 1, в котором упомянутый нестандартный подход к обработке вызова содержит этап, на котором блокируют упомянутый вызов, посредством второго процессора регионального сервера, подсоединенного к телефонной сети.

11. Способ по п. 1, дополнительно содержащий этапы, на которых:

обнаруживают посредством упомянутого процессора, второе событие вызова, происходящее в текущий момент;

анализируют посредством этого процессора данные вызова, связанные со вторым событием вызова, для определения того, что второй вызов, запускающий второе событие вызова, не приведет к неэффективности в телефонной сети в ответ на стандартную обработку второго вызова телефонной сетью; и

предписывают посредством данного процессора телефонной сети обработать второй вызов стандартным образом.

12. Способ по п. 11, в котором упомянутый стандартный подход к обработке вызова содержит соединение упомянутого вызова.

13. Система для обнаружения и предотвращения нежелательного трафика в сети, содержащая:

сервер обнаружения, подсоединенный к телефонной сети, причем сервер обнаружения содержит процессор, выполненный с возможностью:

обнаруживать событие вызова, происходящее в текущий момент;

анализировать данные вызова, связанные с событием вызова, для определения того, что вызов, запускающий событие вызова, будет приводить к неэффективности телефонной сети в ответ на стандартную обработку этого вызова телефонной сетью; и

предписывать телефонной сети обработать данный вызов нестандартным образом, предотвращая тем самым неэффективность.

14. Система по п. 13, в которой событие вызова содержит начало вызова и окончание вызова.

15. Система по п. 13, в которой упомянутый анализ содержит по меньшей мере одно из:

проверки правильности номера телефона источника для упомянутого вызова;

проверки правильности номера телефона пункта назначения для упомянутого вызова;

классификации упомянутого вызова на основе по меньшей мере одного правила для по меньшей мере одного шаблона вызова;

классификации упомянутого вызова на основе числа вызовов между часовым поясом для номера телефона источника и часовым поясом для номера телефона пункта назначения;

классификации упомянутого вызова на основе числа вызовов между географическим местоположением для номера телефона источника и географическим местоположением для номера телефона пункта назначения;

обнаружения контроля ложного ответа;

обнаружения быстрой отмены.

16. Система по п. 13, в которой упомянутый анализ содержит маркировку упомянутого вызова для дополнительного анализа.

17. Система по п. 16, в которой процессор выполнен с возможностью осуществления упомянутого дополнительного анализа.

18. Система по п. 17, в которой процессор выполнен с возможностью предписывать телефонной сети соединять упомянутый вызов в ответ на определение при упомянутом дополнительном анализе того, что данный вызов не приведет к неэффективности.

19. Система по п. 17, в которой процессор выполнен с возможностью предписывать телефонной сети блокировать упомянутый вызов в ответ на определение при упомянутом дополнительном анализе того, что данный вызов приведет к неэффективности.

20. Система по п. 13, в которой упомянутый анализ содержит генерирование тревожного предупреждения для упомянутого вызова.

21. Система по п. 20, дополнительно содержащая региональный сервер, подсоединенный к телефонной сети, содержащий второй процессор, выполненный с возможностью осуществлять упомянутый нестандартный подход к обработке вызова посредством анализа тревожного предупреждение для определения того, блокировать ли данный вызов.

22. Система по п. 13, дополнительно содержащая региональный сервер, подсоединенный к телефонной сети, содержащий второй процессор, выполненный с возможностью осуществлять упомянутый нестандартный подход к обработке вызова посредством блокировки данного вызова.

23. Система по п. 13, в которой процессор выполнен с возможностью:

обнаруживать второе событие вызова, происходящее в текущий момент;

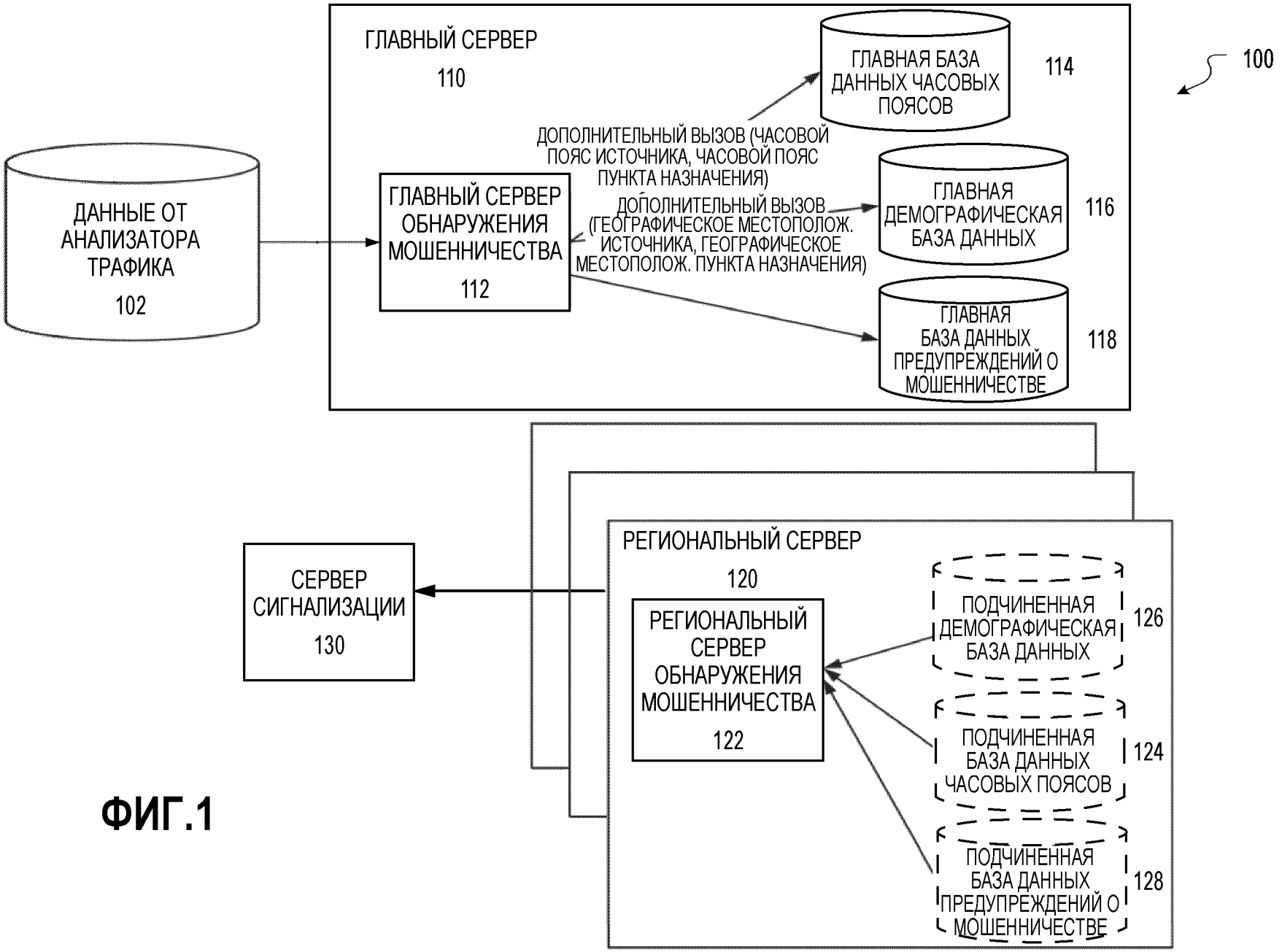
анализировать данные вызова, связанные со вторым событием вызова, для определения того, что второй вызов, запускающий второе событие вызова, не приведет к неэффективности в телефонной сети в ответ на стандартную обработку второго вызова телефонной сетью; и

предписывать телефонной сети обрабатывать второй вызов стандартным образом.

24. Система по п. 23, дополнительно содержащая региональный сервер, подсоединенный к телефонной сети, содержащий второй

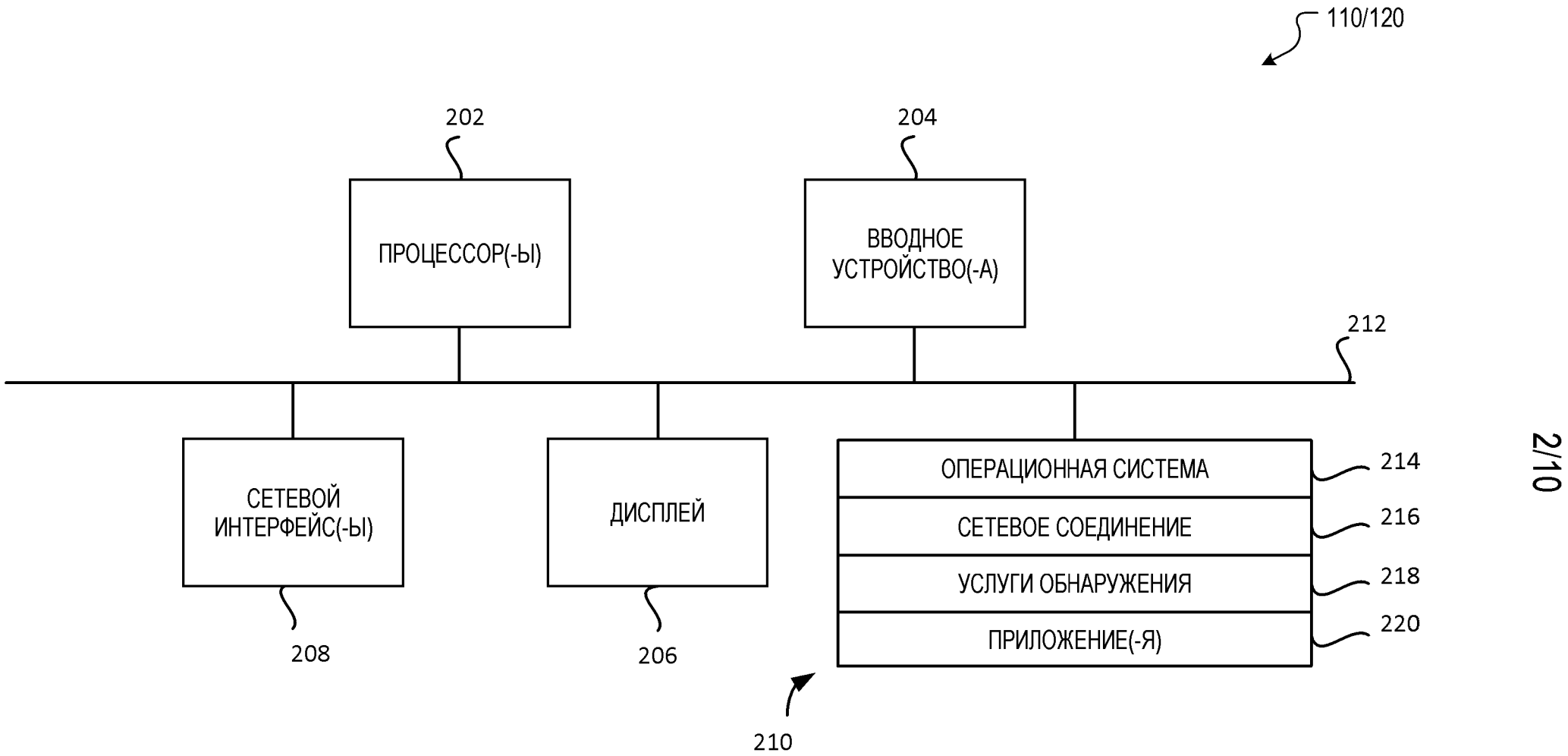
процессор, выполненный с возможностью осуществлять упомянутый стандартный подход к обработке вызова посредством соединения упомянутого вызова.

По доверенности

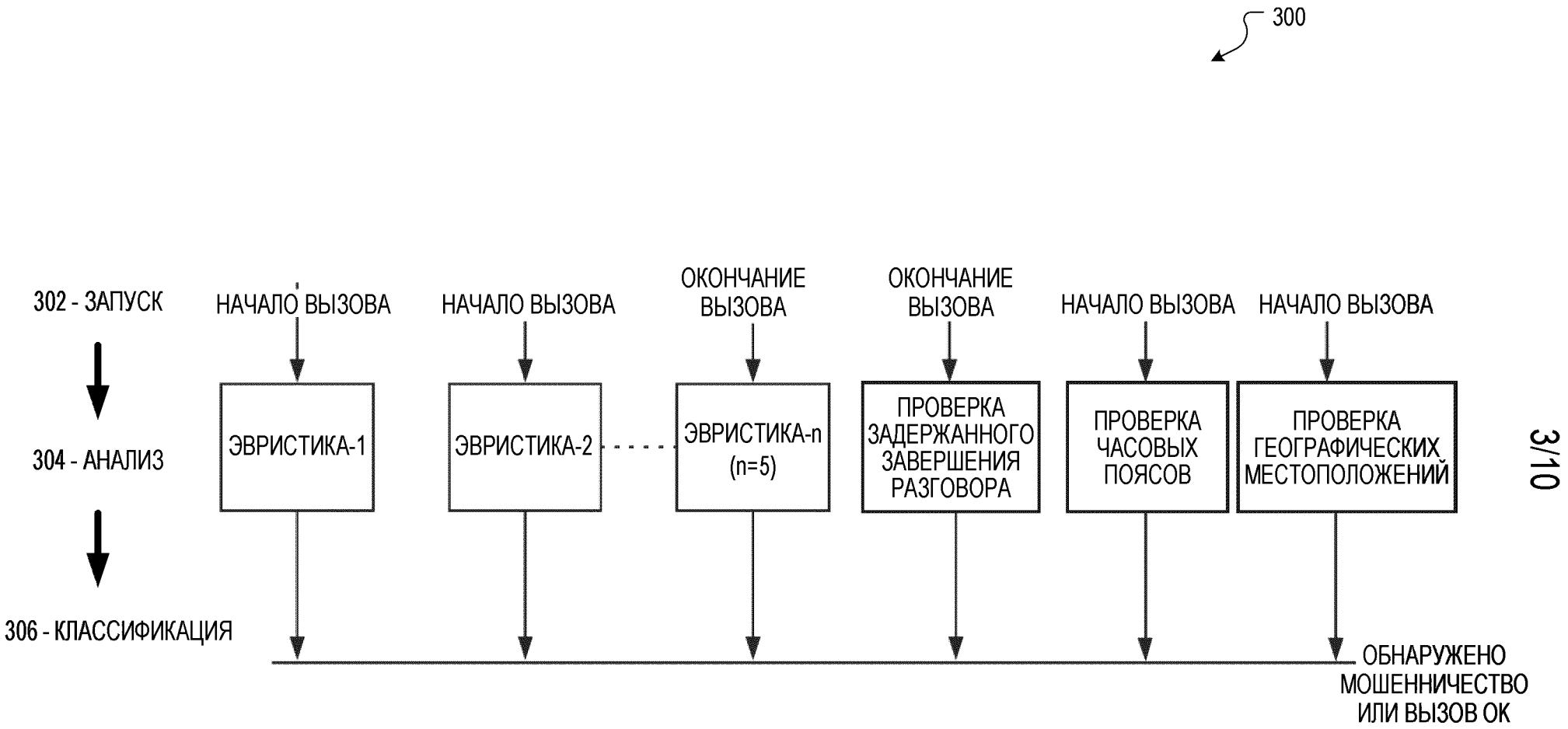

ГЛАВНЫЙ СЕРВЕР
110
ГЛАВНАЯ БАЗА ДАННЫХ ЧАСОВЫХ ПОЯСОВ
114
100
ДОПОЛНИТЕЛЬНЫЙ ВЫЗОВ (ЧАСОВОЙ ПОЯС ИСТОЧНИКА, ЧАСОВОЙ ПОЯС ПУНКТА НАЗНАЧЕНИЯ)
ДАННЫЕ ОТ АНАЛИЗАТОРА ТРАФИКА
102
ГЛАВНЫЙ СЕРВЕР ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА
112
ДОПОЛНИТЕЛЬНЫЙ ВЫЗОВ (ГЕОГРАФИЧЕСКОЕ МЕСТОПОЛОЖ. ИСТОЧНИКА, ГЕОГРАФИЧЕСКОЕ МЕСТОПОЛОЖ. ПУНКТА НАЗНАЧЕНИЯ)
ГЛАВНАЯ ДЕМОГРАФИЧЕСКАЯ БАЗА ДАННЫХ
116
ГЛАВНАЯ БАЗА ДАННЫХ ПРЕДУПРЕЖДЕНИЙ О МОШЕННИЧЕСТВЕ
118
СЕРВЕР СИГНАЛИЗАЦИИ
130
РЕГИОНАЛЬНЫЙ СЕРВЕР
120
РЕГИОНАЛЬНЫЙ СЕРВЕР ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА
122
ПОДЧИНЕННАЯ ДЕМОГРАФИЧЕСКАЯ БАЗА ДАННЫХ
126
ПОДЧИНЕННАЯ БАЗА ДАННЫХ ЧАСОВЫХ ПОЯСОВ
124
ПОДЧИНЕННАЯ БАЗА ДАННЫХ ПРЕДУПРЕЖДЕНИЙ О МОШЕННИЧЕСТВЕ
128

ФИГ.1

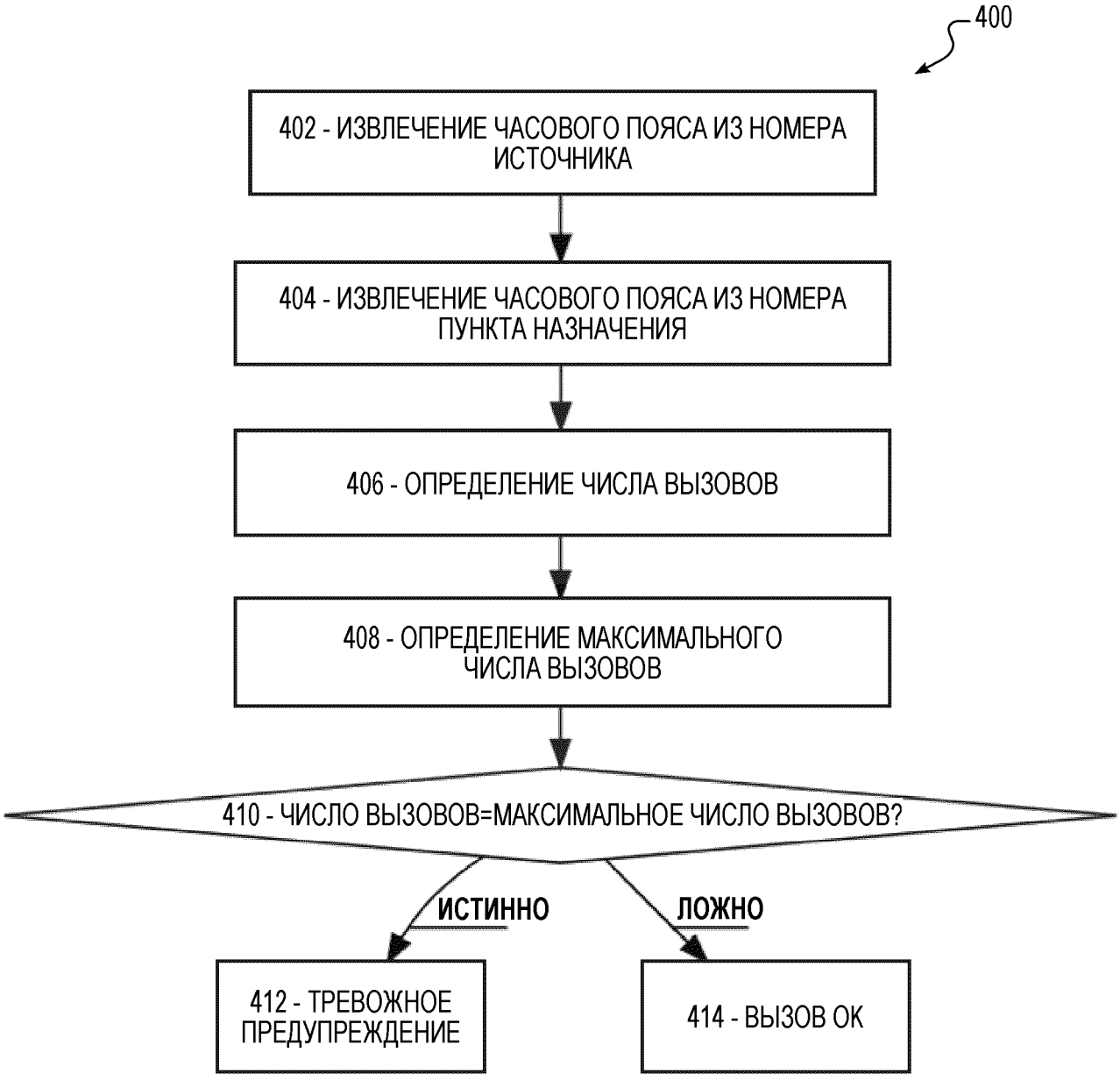
550672


110/120
202
204
ПРОЦЕССОР(-Ы)
ВВОДНОЕ УСТРОЙСТВО(-А)
212
СЕТЕВОЙ ИНТЕРФЕЙС(-Ы)
ДИСПЛЕЙ
ОПЕРАЦИОННАЯ СИСТЕМА
СЕТЕВОЕ СОЕДИНЕНИЕ
УСЛУГИ ОБНАРУЖЕНИЯ
ПРИЛОЖЕНИЕ(-Я)
214
216
218
220
208
206
210

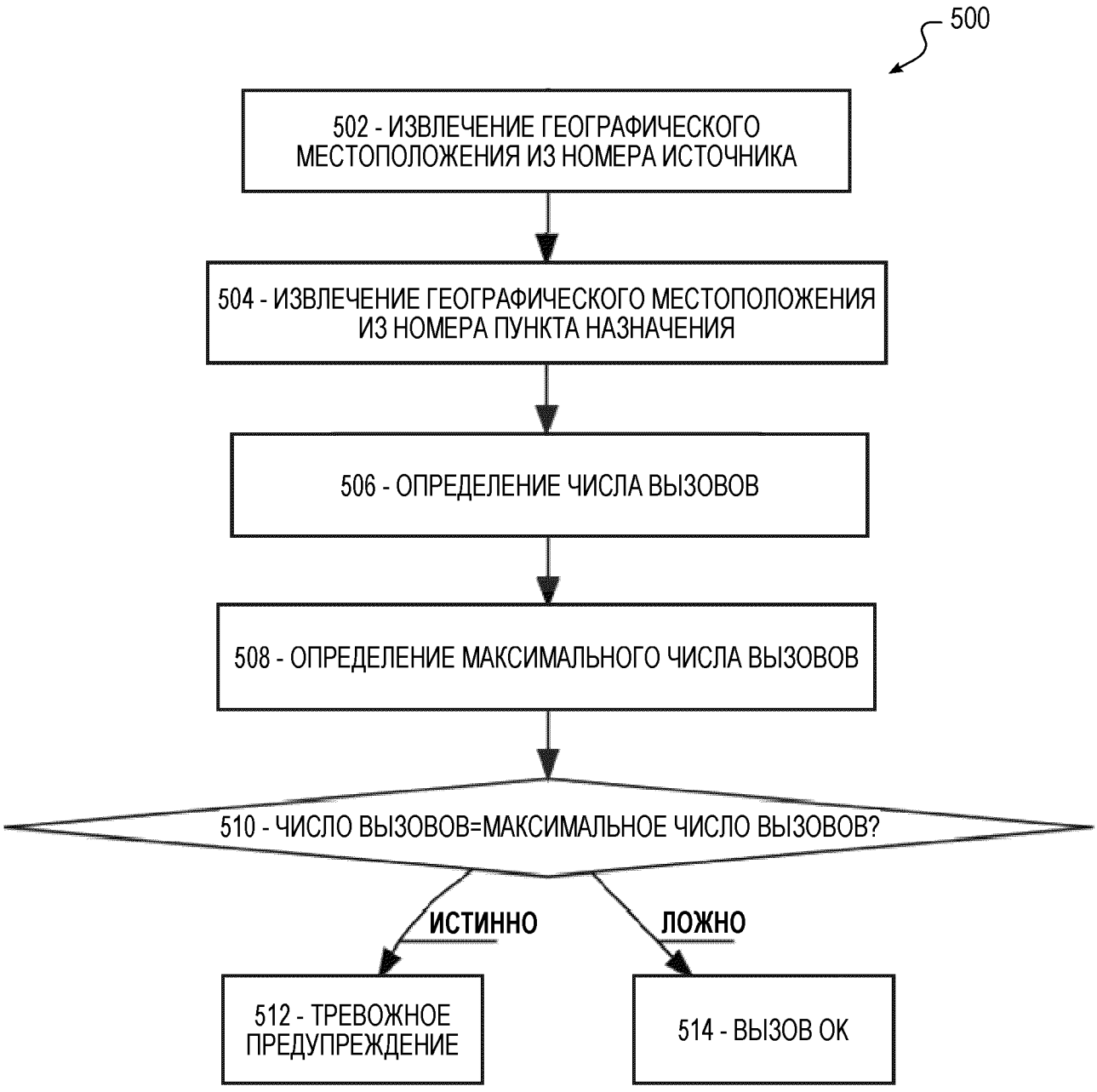
ФИГ.2


300
302 - ЗАПУСК
304 - АНАЛИЗ
306 - КЛАССИФИКАЦИЯ
НАЧАЛО ВЫЗОВА
НАЧАЛО ВЫЗОВА
ОКОНЧАНИЕ ВЫЗОВА
ОКОНЧАНИЕ ВЫЗОВА
НАЧАЛО ВЫЗОВА
НАЧАЛО ВЫЗОВА
ЭВРИСТИКА-1
ЭВРИСТИКА-2
ЭВРИСТИКА-n (n=5)
ПРОВЕРКА ЗАДЕРЖАННОГО ЗАВЕРШЕНИЯ РАЗГОВОРА
ПРОВЕРКА ЧАСОВЫХ ПОЯСОВ
ПРОВЕРКА ГЕОГРАФИЧЕСКИХ МЕСТОПОЛОЖЕНИЙ
ОБНАРУЖЕНО МОШЕННИЧЕСТВО ИЛИ ВЫЗОВ ОК

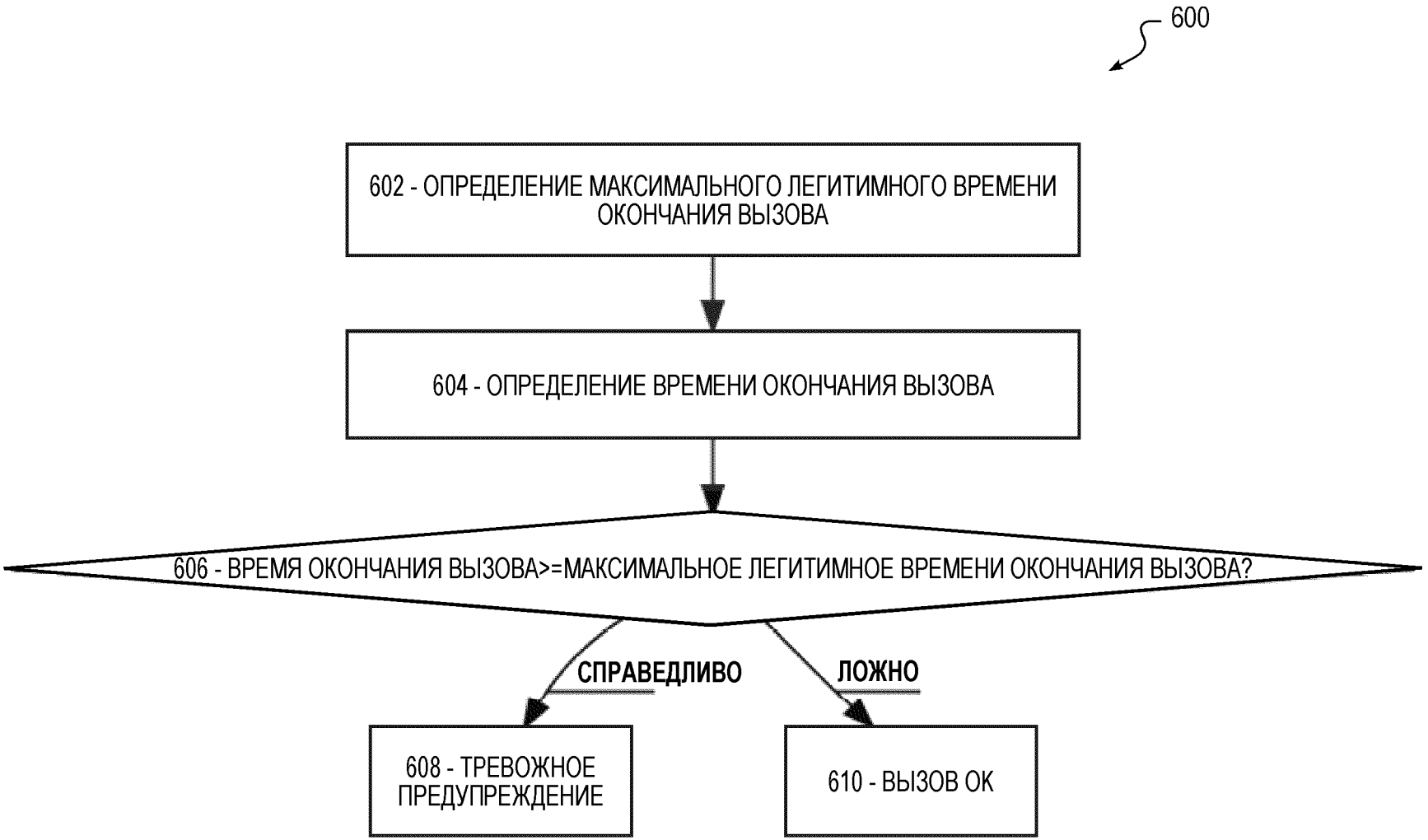
ФИГ.3


400
402 - ИЗВЛЕЧЕНИЕ ЧАСОВОГО ПОЯСА ИЗ НОМЕРА ИСТОЧНИКА
404 - ИЗВЛЕЧЕНИЕ ЧАСОВОГО ПОЯСА ИЗ НОМЕРА ПУНКТА НАЗНАЧЕНИЯ
406 - ОПРЕДЕЛЕНИЕ ЧИСЛА ВЫЗОВОВ
408 - ОПРЕДЕЛЕНИЕ МАКСИМАЛЬНОГО ЧИСЛА ВЫЗОВОВ
410 - ЧИСЛО ВЫЗОВОВ=МАКСИМАЛЬНОЕ ЧИСЛО ВЫЗОВОВ?
ИСТИННО
ЛОЖНО
412 - ТРЕВОЖНОЕ ПРЕДУПРЕЖДЕНИЕ
414 - ВЫЗОВ ОК

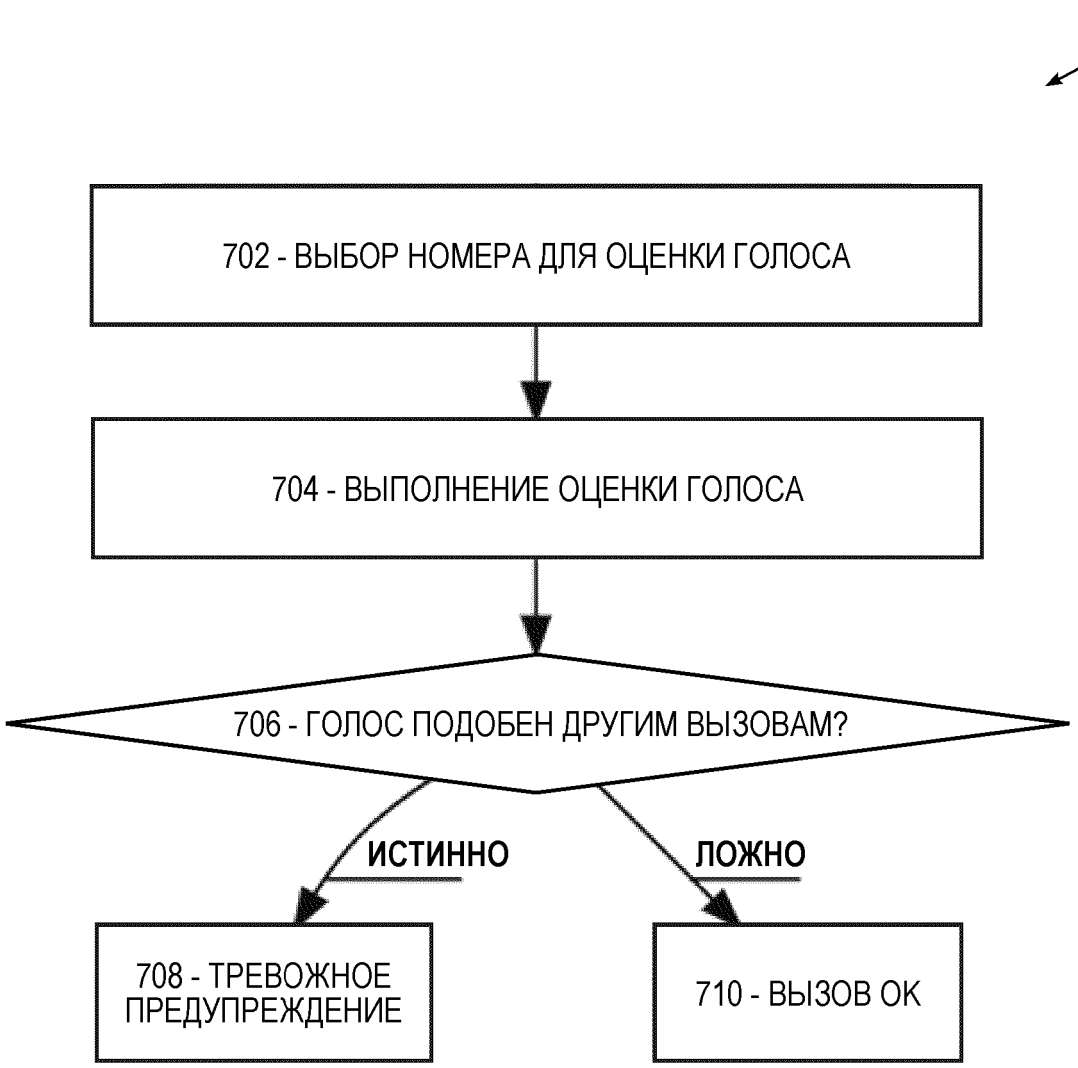
ФИГ.4


500
502 - ИЗВЛЕЧЕНИЕ ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ ИЗ НОМЕРА ИСТОЧНИКА
504 - ИЗВЛЕЧЕНИЕ ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ ИЗ НОМЕРА ПУНКТА НАЗНАЧЕНИЯ
506 - ОПРЕДЕЛЕНИЕ ЧИСЛА ВЫЗОВОВ
508 - ОПРЕДЕЛЕНИЕ МАКСИМАЛЬНОГО ЧИСЛА ВЫЗОВОВ
510 - ЧИСЛО ВЫЗОВОВ=МАКСИМАЛЬНОЕ ЧИСЛО ВЫЗОВОВ?
ИСТИННО
ЛОЖНО
512 - ТРЕВОЖНОЕ ПРЕДУПРЕЖДЕНИЕ
514 - ВЫЗОВ ОК

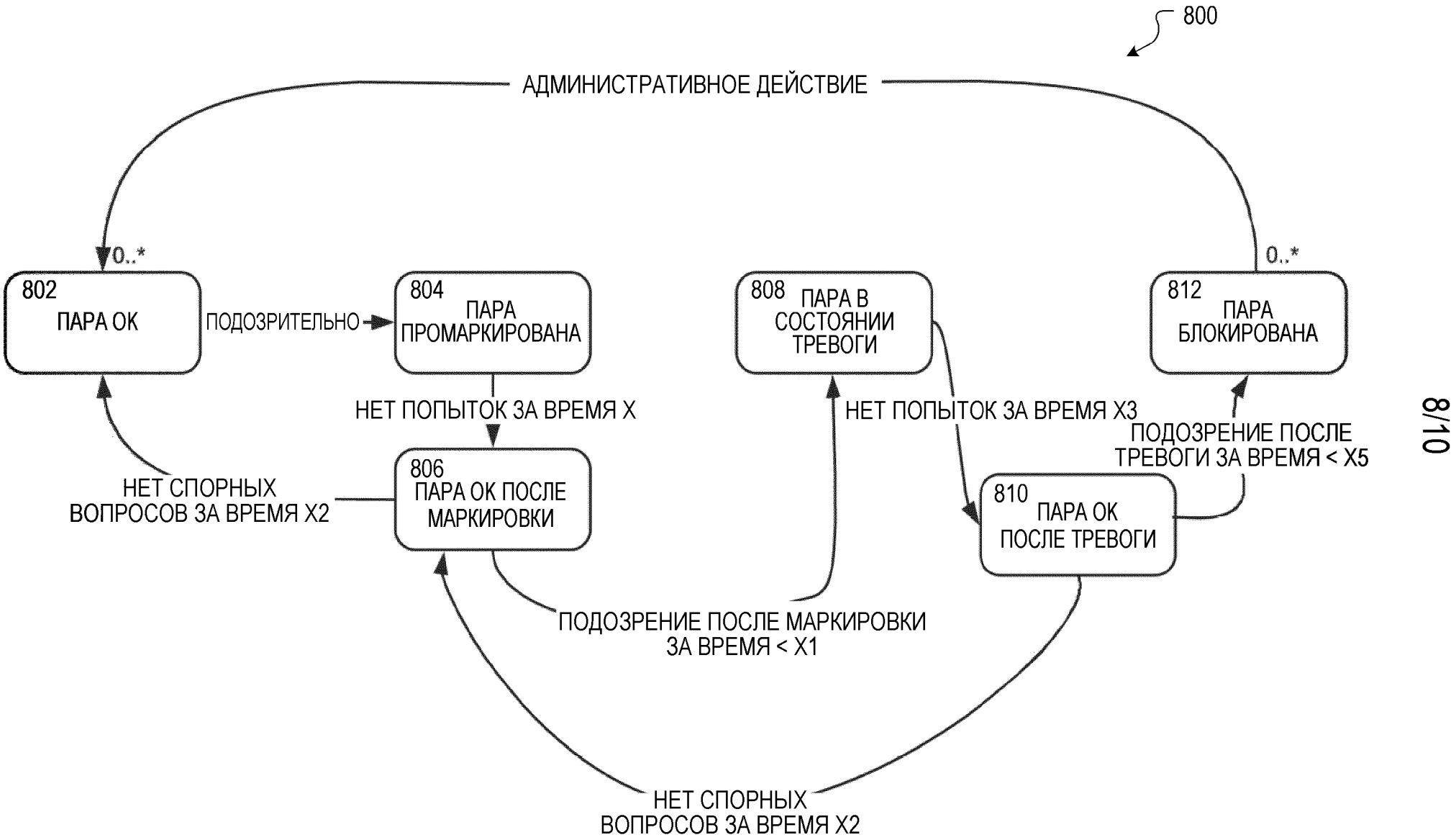
ФИГ.5


600
602 - ОПРЕДЕЛЕНИЕ МАКСИМАЛЬНОГО ЛЕГИТИМНОГО ВРЕМЕНИ ОКОНЧАНИЯ ВЫЗОВА
604 - ОПРЕДЕЛЕНИЕ ВРЕМЕНИ ОКОНЧАНИЯ ВЫЗОВА
606 - ВРЕМЯ ОКОНЧАНИЯ ВЫЗОВА>=МАКСИМАЛЬНОЕ ЛЕГИТИМНОЕ ВРЕМЕНИ ОКОНЧАНИЯ ВЫЗОВА?
СПРАВЕДЛИВО
ЛОЖНО
608 - ТРЕВОЖНОЕ ПРЕДУПРЕЖДЕНИЕ
610 - ВЫЗОВ ОК

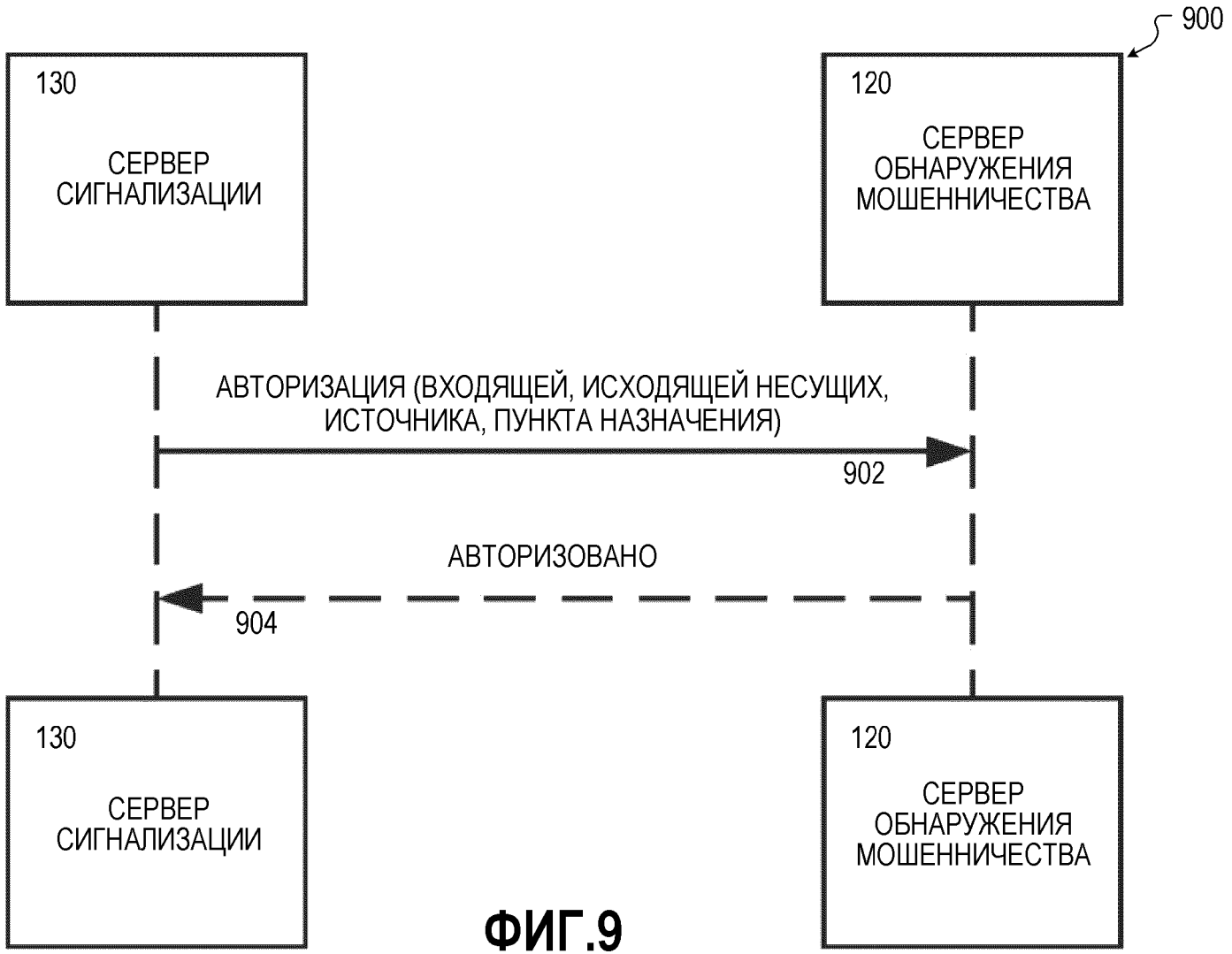
ФИГ.6


700
702 - ВЫБОР НОМЕРА ДЛЯ ОЦЕНКИ ГОЛОСА
704 - ВЫПОЛНЕНИЕ ОЦЕНКИ ГОЛОСА
706 - ГОЛОС ПОДОБЕН ДРУГИМ ВЫЗОВАМ?
ИСТИННО
ЛОЖНО
708 - ТРЕВОЖНОЕ ПРЕДУПРЕЖДЕНИЕ
710 - ВЫЗОВ ОК

ФИГ.7


800
АДМИНИСТРАТИВНОЕ ДЕЙСТВИЕ
0..*
802
ПАРА ОК
ПОДОЗРИТЕЛЬНО
804
ПАРА ПРОМАРКИРОВАНА
НЕТ ПОПЫТОК ЗА ВРЕМЯ X
НЕТ СПОРНЫХ ВОПРОСОВ ЗА ВРЕМЯ X2
806
ПАРА ОК ПОСЛЕ МАРКИРОВКИ
ПОДОЗРЕНИЕ ПОСЛЕ МАРКИРОВКИ ЗА ВРЕМЯ < X1
808
ПАРА В СОСТОЯНИИ ТРЕВОГИ
НЕТ ПОПЫТОК ЗА ВРЕМЯ X3
810
ПАРА ОК ПОСЛЕ ТРЕВОГИ
ПОДОЗРЕНИЕ ПОСЛЕ ТРЕВОГИ ЗА ВРЕМЯ < X5
0..*
812
ПАРА БЛОКИРОВАНА
НЕТ СПОРНЫХ ВОПРОСОВ ЗА ВРЕМЯ X2

ФИГ.8


900
130
СЕРВЕР СИГНАЛИЗАЦИИ
120
СЕРВЕР ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА
АВТОРИЗАЦИЯ (ВХОДЯЩЕЙ, ИСХОДЯЩЕЙ НЕСУЩИХ, ИСТОЧНИКА, ПУНКТА НАЗНАЧЕНИЯ)
902
АВТОРИЗОВАНО
904
130
СЕРВЕР СИГНАЛИЗАЦИИ
120
СЕРВЕР ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА

ФИГ.9

1000

Случай	Число вызовов	Период времени	A Профиль номера (исходящий вызов)	B Профиль номера (входящий вызов)	Условие	
1	5	Одновременно	Тот же код страны или блокированный номер То же множество значений X (0 | 9)	То же множество значений X (0 | 9)	Вызов длится свыше 2 минут	Случай 1
2	10	Одновременно	Тот же код страны или блокированный номер То же множество значений XX (00 | 99)	То же множество значений XX (00 | 99)	Вызов длится свыше 2 минут	Случай 2
3	50	1 минута	Тот же код страны или блокированный номер То же множество значений XX (00 | 99)	Случайный не последовательный	Вызов длится менее 15 секунд Время отмены менее 5 секунд	Случай 3
4	100	1 час	Случайный не последовательный, из сети той же страны	То же множество значений XX (00 | 99)	Вызов длится менее 2 минут Время отмены менее 5 секунд	Случай 4

ФИГ.10

ЕВРАЗИИСКОЕ ПАТЕНТНОЕ ВЕДОМСТВО

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки: 201891320

Дата подачи: 29 июня 2018 (29.06.2018) | Дата испрашиваемого приоритета: 15 мая 2018 (15.05.2018)

Название изобретения: Платформа для обнаружения неэффективности использования и мошенничества в действующей сети применительно к телефонной сети

Заявитель: ЛЕВИ Динор Адам Вестергард

☐ **Некоторые пункты формулы не подлежат поиску (см. раздел I дополнительного листа)**

☐ **Единство изобретения не соблюдено (см. раздел II дополнительного листа)**

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

МПК: ***H04M 3/436*** *(2006.01)* СПК: ***H04M 3/436*** *(2013.01)*
H04M 15/00 *(2006.01)* ***H04M 15/47*** *(2013.01)*

Согласно Международной патентной классификации (МПК) или национальной классификации и МПК

Б. ОБЛАСТЬ ПОИСКА:

Минимум просмотренной документации (система классификации и индексы МПК)
H04M 3/00, 3/22, 3/36, 3/42, 15/00, 15/47, H04W 4/00, 12/00, 12/12, H04Q 3/00

Другая проверенная документация в той мере, в какой она включена в область поиска:

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X	US 5805686 A (MCI CORPORATION) 08.09.1998, кол. 1, строка 4 - кол. 4, строка 27, кол. 4, строка 64- кол. 8, строка 14	1-6, 12-18, 24
Y		7-11, 19-23
Y	US 2014/0128047 A1 (LOOKOUT, INC.) 08.05.2014, параграфы [0074]-[0086], [0102]-[0129]	7-11, 19-23
A	US 6442265 B1 (AT & T CORP) 28.08.2002	1-24

☐ последующие документы указаны в продолжении графы В ☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:

"A" документ, определяющий общий уровень техники
"E" более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
"O" документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета
"D" документ, приведенный в евразийской заявке
"T" более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
"X" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
"Y" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
"&" документ, являющийся патентом-аналогом
"L" документ, приведенный в других целях

Дата действительного завершения патентного поиска: 29 ноября 2018 (29.11.2018)

Наименование и адрес Международного поискового органа:
Федеральный институт промышленной собственности
РФ, 125993,Москва, Г-59, ГСП-3, Бережковская наб., д. 30-1.Факс: (499) 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо: Т. М. Иванова
Телефон № (499) 240-25-91