РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 331 913** (13) **C2**

(51) МПК
G06F 1/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005124681/09, 25.02.2004**

(24) Дата начала отсчета срока действия патента:
25.02.2004

(30) Конвенционный приоритет:
03.03.2003 US 10/378,463

(43) Дата публикации заявки: **20.01.2006**

(45) Опубликовано: **20.08.2008 Бюл. № 23**

(56) Список документов, цитированных в отчете о поиске: **US 2002/0199095 A1, 26.12.2002. US 6161130 A, 12.12.2000. US 6052709 A, 18.04.2000. RU 2170494 C2, 10.07.2001. RU 2179738 C2, 20.02.2002.**

(85) Дата перевода заявки PCT на национальную фазу:
02.08.2005

(86) Заявка PCT:
US 2004/005501 (25.02.2004)

(87) Публикация PCT:
WO 2004/079514 (16.09.2004)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
РАУНТВЭЙТ Роберт Л. (US),
ХЕКЕРМЭН Дэвид Э. (US),
МЕР Джон Д. (US),
ХОУВЕЛЛ Натан Д. (US),
РУПЕРСБУРГ Мика К. (US),
СЛОУСОН Дин А. (US),
ГУДМАН Джошуа Т. (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

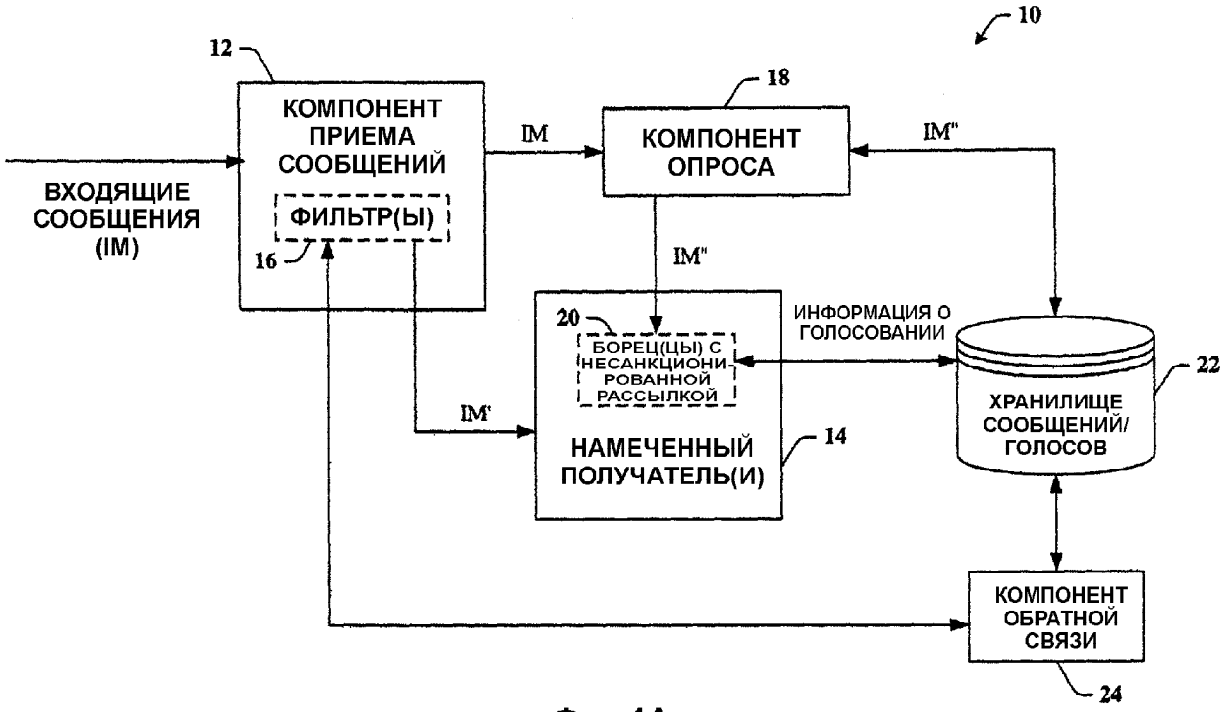
RU 2331913 C2

RU 2331913 C2

(54) КОНТУР ОБРАТНОЙ СВЯЗИ ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКИ

(57) Реферат:

Изобретение относится к системам и способам идентификации как легитимной (полезной почты), так и нежелательной информации (бесполезная почта), и к классификации электронной почтовой корреспонденции для предотвращения спама. Технический результат изобретения заключается в обучении и в усовершенствовании фильтра несанкционированной рассылки. Технический результат достигается за счет того, что производят выборку по случайной схеме входящих почтовых сообщений, так чтобы были получены примеры и легитимной, и бесполезной почты/несанкционированной рассылки, чтобы сгенерировать наборы обучающих данных. Пользователям, определенным как борцы с несанкционированной рассылкой, выдается задание проголосовать по тому, является ли выборка их входящих почтовых сообщений по отдельности легитимной почтой или бесполезной почтой. База данных сохраняет свойства каждой почтовой транзакции и транзакции голосования, например информацию о пользователе, свойства сообщения и сводку по содержимому, а также результаты голосования, чтобы сгенерировать обучающие данные для систем обучения фильтра. 5 н. и 40 з.п.ф-лы, 11 ил.



Фиг. 1A

RU 2331913 C2

RU 2331913 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 331 913** (13) **C2**

(51) Int. Cl.
G06F 1/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005124681/09, 25.02.2004**

(24) Effective date for property rights: **25.02.2004**

(30) Priority:
03.03.2003 US 10/378,463

(43) Application published: **20.01.2006**

(45) Date of publication: **20.08.2008 Bull. 23**

(85) Commencement of national phase: **02.08.2005**

(86) PCT application:
US 2004/005501 (25.02.2004)

(87) PCT publication:
WO 2004/079514 (16.09.2004)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
RAUNTVEhJT Robert L. (US),
KhEKERMEhN Dehvid Eh. (US),
MER Dzhon D. (US),
KhOUVELL Natan D. (US),
RUPERSBURG Mika K. (US),
SLOUSON Din A. (US),
GUDMAN Dzhoshua T. (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) FEEDBACK LOOP FOR UNAUTHORISED MAILING PREVENTION

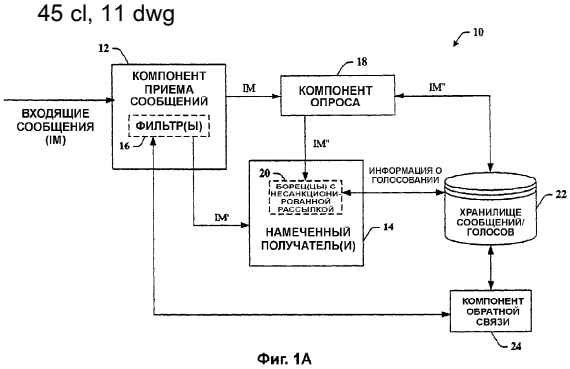
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention refers to the systems and methods of the legitimate (useful) and unwanted (spam) information identification and classification of e-mail for spam prevention. The incoming email messages are randomly selected in order to obtain both the samples of legitimate and useless mail/unauthorised mailing to generate sets of training data. Those users who were determined as extirpators against unauthorised mailing should vote whether selection of separate incoming messages refers to legitimate or unwanted mail. The data base saves properties of each mailing transaction and voting transactions, for example, user info, message properties and content summary, and also the voting results for generating data for training the spam-filter.

EFFECT: training and improvement of the spam-filter.

45 cl, 11 dwg



Фиг. 1А

RU 2331913 C2

RU 2331913 C2

Область техники, к которой относится изобретение

Изобретение относится к системам и способам идентификации как легитимной (к примеру, полезной почты), так и нежелательной информации (к примеру, бесполезной почты), и более конкретно, к классификации электронной почтовой корреспонденции для предотвращения спама (несанкционированной рассылки; практически бесполезной информации (обычно рекламы), большому числу абонентов электронной почты).

Предшествующий уровень техники

Появление глобальных сетей связи, например Интернета, представило коммерческие возможности для охвата огромного количества потенциальных клиентов. Обмен электронными сообщениями и, в частности, сообщениями электронной почты, становится все более широко используемым средством распространения нежелательных рекламных объявлений и предложений (также называемых несанкционированной рассылкой или "спамом") пользователям сети.

Radicati Group, Inc., фирма по оказанию консультационных услуг и исследованию рынка, дает оценку, что по состоянию на август 2002 года ежедневно отправляется два миллиарда бесполезных сообщений электронной почты, и это число, по прогнозам, утраивается каждые два года. Физические и юридические лица (к примеру, бизнес-компании, правительственные организации) испытывают все больше неудобств и зачастую несут потери от бесполезных сообщений. По существу, бесполезные сообщения электронной почты сейчас или вскоре станут основной угрозой защищенной работы вычислительной техники.

Ключевая методика, используемая, чтобы отсеивать бесполезную электронную почту, заключается в использовании систем/методик фильтрации. Одна из проверенных методик фильтрации основана на подходе обучения машины - машинно-обучаемые фильтры назначают входящему сообщению вероятность того, что сообщение бесполезно. При этом подходе признаки в типичном случае извлекаются из двух классов примеров сообщений (к примеру, бесполезных и небесполезных сообщений), а обучаемый фильтр применяется, чтобы различать в вероятностном смысле эти два класса. Поскольку многие признаки сообщений относятся к содержимому (к примеру, словам и фразам в теме и/или теле сообщения), эти типы фильтров обычно называют "основанными на содержимом фильтрами".

Некоторые фильтры бесполезной информации/несанкционированной рассылки являются адаптивными, что важно в том, что пользователям, которые говорят на нескольких языках, и пользователям, которые говорят на редких языках, необходим фильтр, который может адаптироваться к их конкретным потребностям. Более того, не все пользователи согласны с тем, что считать, а что не считать бесполезной информацией/несанкционированной рассылкой. Следовательно, посредством использования фильтра, который может быть обучен неявным образом (к примеру, посредством наблюдения за поведением пользователей), соответствующий фильтр может быть приспособлен динамически, чтобы удовлетворять конкретным потребностям пользователя по идентификации сообщений.

Один из подходов к адаптации фильтрации - предписать пользователю(ям) помечать сообщения как бесполезные или небесполезные. К сожалению, подобные методики обучения с большим количеством операций вручную неудобны для многих пользователей вследствие сложности, ассоциированной с таким обучением, не говоря уже о количестве времени, требуемом, чтобы надлежащим образом проводить это обучение. Помимо этого, такие методики обучения вручную зачастую искажаются отдельными пользователями. Например, подписки на бесплатные рассылки часто забываются пользователями и, таким образом, некорректно помечаются как бесполезная почта. В результате легитимная почта блокируется неявно из почтового ящика пользователя. Другой подход к обучению на основе адаптивной фильтрации - использовать скрытые ключи обучения. Например, если пользователь(и) отвечает или переадресовывает сообщение, этот подход считает, что сообщение не бесполезно. Тем не менее, использование только ключей сообщений такого

типа привносит статистические отклонения в процесс обучения, что имеет следствием фильтры с более низкой соответствующей достоверностью.

Еще один подход - использовать для обучения всю электронную почту пользователя(ей), где исходные метки назначены используемым фильтром, и пользователь(и) иногда переопределяет эти назначения явными ключами (к примеру, способ "пользовательской коррекции"), например, выбирая такие параметры, как "удалить как бесполезное" и "небесполезное", и/или скрытыми ключами. Хотя такой подход более оптимален, чем ранее описанные методики, он по-прежнему неполный по сравнению с представленным изобретением, описанным и заявленным далее.

Сущность изобретения

Далее представлено упрощенное изложение сущности изобретения, для того чтобы предоставить базовое понимание некоторых аспектов изобретения. Это изложение сущности не является всесторонним обзором изобретения. Оно не предназначено, чтобы определить ключевые/важнейшие элементы изобретения или обрисовать область применения изобретения. Его единственная цель - представить некоторые понятия изобретения в упрощенной форме в качестве вступления в более подробное описание, которое представлено далее.

Представленное изобретение предоставляет систему и способ контура обратной связи, которые обеспечивают выполнение классификации элементов в связи с предотвращением несанкционированной рассылки. Изобретение использует подход обучения машины при применении к фильтрам несанкционированной рассылки, и, в частности, производит выборку по случайной схеме входящих сообщений электронной почты, так чтобы были получены примеры и легитимной, и бесполезной почты/несанкционированной рассылки для генерирования наборов обучающих данных. Заранее выбранные люди служат в качестве борцов с несанкционированной рассылкой и принимают участие в категоризировании соответствующих дублирований (которые в необязательном порядке могут быть немного модифицированными) выборок.

Как правило, сообщения, выбранные для опроса, модифицируются в различных аспектах, чтобы представать как сообщения для опроса. Уникальный аспект изобретения состоит в том, что делается копия входящего сообщения, выбранного для опроса, с тем чтобы некоторые пользователи (к примеру, борцы с несанкционированной рассылкой) получали одно и то же сообщение (к примеру, в терминах содержимого сообщения) дважды: один раз в форме сообщения для опроса и повторно в исходной форме. Другой уникальный аспект представленного изобретения состоит в том, что для опроса учитываются все сообщения, включая и те, которые используемыми фильтрами были помечены как несанкционированная рассылка. Помеченные как несанкционированная рассылка сообщения учитываются для опроса и, если выбраны, не интерпретируются как несанкционированная рассылка согласно спецификациям используемого фильтра (к примеру, перемещение в папку бесполезной почты, удаление...).

В отличие от традиционных фильтров несанкционированной рассылки, более точные фильтры несанкционированной рассылки могут быть созданы посредством обучения фильтров несанкционированной рассылки в соответствии с методикой обратной связи представленного изобретения, чтобы научиться проводить различие между полезной почтой и несанкционированной рассылкой, тем самым уменьшая объем необъективной и неточной фильтрации. Обратная связь осуществляется, по меньшей мере, частично посредством опроса любого подходящего числа пользователей, чтобы получить обратную связь по их входящей электронной почте. Пользователям, определенным как борцы с несанкционированной рассылкой, выдается задание голосования по тому, является ли выборка входящих сообщений легитимной почтой или бесполезной почтой. И позитивная, и негативная классификация входящей электронной почты предназначена, чтобы уменьшить неправильную фильтрацию как несанкционированной рассылки почты, которая является полезной (к примеру, не несанкционированной рассылкой), предназначенной для пользователя. Соответствующие классификации вместе с любой другой информацией,

ассоциированной с каждой почтовой транзакцией, переносятся в базу данных, чтобы облегчить обучение фильтров несанкционированной рассылки. База данных и относящиеся к ней компоненты позволяют компилировать и сохранять свойства выбранного сообщения(ий) (или выбранной почтовой транзакции), что включает в себя пользовательские свойства, информацию и предысторию голосований пользователей, свойства сообщений, такие как уникальные идентификационные номера, назначенные каждому выбранному сообщению, классификации сообщений и сводки по содержимому сообщений или статистические данные, связанные с любым из вышеперечисленного, чтобы сгенерировать наборы обучающих данных для систем обучения машины. Системы обучения машины (к примеру, нейронные сети, реализации метода опорных векторов (SVM), сети байесовских представлений) обеспечивают создание усовершенствованных фильтров несанкционированной рассылки, которые обучены распознавать как легитимную почту, так и несанкционированную рассылку и, дополнительно, различать их. После того, как новый фильтр несанкционированной рассылки был обучен в соответствии с изобретением, он может быть распространен почтовым серверам и клиентским почтовым программам. Более того, новый фильтр несанкционированной рассылки может быть подготовлен по отношению к конкретному пользователю(ям), чтобы повысить эффективность персонализированного фильтра(ов). После того, как новые наборы обучающих данных созданы, фильтр несанкционированной рассылки может пройти дополнительное обучение посредством обучения машины, чтобы оптимизировать свои рабочие характеристики и точность. Обратная связь от пользователей посредством классификации сообщений также может быть использована, чтобы сгенерировать списки для фильтров несанкционированной рассылки и родительские элементы управления, чтобы протестировать эффективность фильтров несанкционированной рассылки и/или определить происхождение несанкционированной рассылки.

Другой аспект изобретения предоставляет способ распознавания недоверенных пользователей посредством методик перекрестной проверки и /или тестовых сообщений с известным результатом. Перекрестная проверка влечет за собой обучение фильтра, из которого исключены результаты опросов некоторых пользователей. Т.е. фильтр обучается с помощью результатов опросов поднабора пользователей. В среднем этот поднабор пользователей даст достаточно хорошие результаты даже при некоторых ошибках, чтобы распознавать тех, кто обычно не согласуется с ними. Результаты опроса исключенных пользователей сравниваются с результатами обученного фильтра. Это сравнение по существу определяет, как пользователи из обучающего поднабора проголосовали бы по сообщениям, принадлежащим исключенным пользователям. Если согласование между голосами исключенного пользователя и фильтром незначительное, то результаты голосования этого пользователя могут либо быть отброшены, либо помечены для изучения вручную. Эта методика может быть повторена при необходимости, исключая данные каждый раз от различных пользователей.

Ошибки по отдельным сообщениям также могут быть распознаны, например сообщение, по которому фильтр и голос пользователя сильно расходятся. Эти сообщения могут быть помечены либо для автоматического удаления, либо для изучения вручную. В качестве альтернативы перекрестной проверке фильтр может быть обучен на всех или практически всех пользователях. Голоса и/или сообщения пользователя, которые расходятся с фильтром, могут быть отброшены. Другая альтернатива перекрестной проверки влечет за собой тестовые сообщения с известным результатом, в которых пользователя(ей) просят проголосовать по сообщению(ям), где результат известен. Точная классификация (к примеру, голос пользователя совпадает с действием пользователя) сообщения пользователем удостоверяет доверенность пользователя и определяет, следует ли удалять классификации пользователя из обучения и следует ли удалять пользователя из будущего опроса.

Еще один аспект изобретения предусматривает создание известных мишеней несанкционированной рассылки (к примеру, электронных приманок), чтобы

идентифицировать входящую почту как несанкционированную рассылку и/или отслеживать обработку конкретных коммерческих адресов электронной почты. Известная мишень несанкционированной рассылки, или электронная приманка, - это адрес электронной почты, где адрес легитимной почты может быть определен и вся остальная почта может считаться несанкционированной рассылкой. Например, адрес электронной почты может быть ограниченно раскрыт на Web-сайте, чтобы практически не мог быть обнаружен людьми. Следовательно, вся почта, отправленная на этот адрес, может считаться несанкционированной рассылкой. Альтернативно, адрес электронной почты может быть раскрыт только коммерсанту, от которого, как ожидается, должна быть принята легитимная почта. Таким образом, почта, принятая от коммерсанта, является легитимной почтой, а вся остальная принятая почта может безошибочно считаться несанкционированной рассылкой. Данные несанкционированной рассылки, полученной из электронных приманок и/или других источников (к примеру, пользователей), могут быть интегрированы в систему контура обратной связи, но вследствие значительного расширения классификации несанкционированной рассылки с помощью электронных приманок вес этих данных должен быть понижен, как более подробно описано ниже, чтобы уменьшить получение необъективных результатов опроса.

Другой аспект изобретения предусматривает помещение на карантин сообщений, которые считаются неопределенными либо системой контура обратной связи, либо фильтром. Эти сообщения сохраняются любой надлежащий период вместо того, чтобы быть отброшенными или классифицированными. Этот период времени может быть задан заранее, либо сообщение может быть сохранено до получения определенного числа результатов опроса, аналогичных сообщению, к примеру, с того же самого IP-адреса или с аналогичным содержимым.

Для достижения вышеупомянутых и связанных целей определенные иллюстрационные аспекты изобретения описаны в данном документе в связи со следующим описанием и прилагаемыми чертежами. Эти аспекты, тем не менее, указывают только на некоторые из множества способов, которыми могут быть использованы принципы изобретения. Изобретение предназначено, чтобы включить в себя все такие аспекты и их эквиваленты. Другие преимущества и новые признаки изобретения могут стать явными из следующего подробного описания изобретения, если рассматривать их вместе с чертежами.

Перечень фигур чертежей

Фиг.1A - блок-схема обучающей системы контура обратной связи в соответствии с аспектом настоящего изобретения.

Фиг.1B - блок-схема алгоритма типичного процесса обучения в контуре обратной связи в соответствии с аспектом настоящего изобретения.

Фиг.2 - блок-схема последовательности операций типичного способа, который обеспечивает классификацию почты пользователями, чтобы создавать фильтры несанкционированной рассылки, в соответствии с аспектом настоящего изобретения.

Фиг.3 - блок-схема последовательности операций типичного способа, который обеспечивает перекрестную проверку пользователей, принимающих участие в способе по фиг.2, в соответствии с аспектом настоящего изобретения.

Фиг.4 - блок-схема последовательности операций типичного способа, который обеспечивает определение того, какие пользователи являются недоверенными, в соответствии с аспектом настоящего изобретения.

Фиг.5 - блок-схема последовательности операций типичного способа, который обеспечивает выявление несанкционированной рассылки и определение инициаторов несанкционированной рассылки, в соответствии с аспектом настоящего изобретения.

Фиг.6 - блок-схема основанной на клиенте архитектуры контура обратной связи в соответствии с аспектом настоящего изобретения.

Фиг.7 - блок-схема основанной на сервере архитектуры контура обратной связи в соответствии с аспектом настоящего изобретения.

Фиг.8 - блок-схема межкорпоративной основанной на сервере системы контура обратной

связи, включающей в себя внутренний сервер с собственной базой данных, чтобы извлекать данные обучения, сохраненные во внешних пользовательских базах данных, в соответствии с аспектом настоящего изобретения.

Фиг.9 - иллюстрация типичной среды для реализации различных аспектов изобретения.

Фиг.10 - блок-схема типичной коммуникационной среды в соответствии с настоящим изобретением.

Подробное описание изобретения

Настоящее изобретение описано далее со ссылками на чертежи, на которых одинаковые номера ссылок соответствуют идентичным элементам. В последующем описании, для целей пояснения, многие конкретные детали объяснены, чтобы обеспечить полное понимание настоящего изобретения. Тем не менее, может быть очевидно, что настоящее изобретение может быть применено на практике без этих конкретных деталей. В иных случаях, на модели блок-схемы показаны широко известные структуры и устройства, чтобы облегчить описание настоящего изобретения.

При использовании в данной заявке термины "компонент" и "система" предназначены, чтобы ссылаться на связанную с вычислительной машиной объектную сущность, а именно либо аппаратные средства, либо сочетание аппаратных средств и программного обеспечения, либо программное обеспечение, либо программное обеспечение в ходе исполнения. Например, компонент может быть, но не только, процессом, запущенным на процессоре, процессором, объектом, исполняемым файлом, потоком исполнения, программой и/или вычислительной машиной. В качестве иллюстрации, и приложение, запущенное на сервере, и сервер может быть компонентом. Один или более компонентов могут постоянно находиться внутри процесса и/или потока исполнения, и компонент может быть размещен на вычислительной машине и/или распределен между двумя и более вычислительными машинами.

Представленное изобретение может содержать различные схемы и/или методики умозаключения в связи с генерацией обучающих данных для машинообученной фильтрации несанкционированной рассылки. При использовании в данном документе термин "умозаключение" обычно означает процесс рассуждения или обозначения состояний системы, окружения и/или пользователя из набора данных наблюдения, полученных посредством событий и/или данных. Умозаключение может быть использовано, чтобы определить конкретный контекст или действие, либо может генерировать распределение вероятностей, к примеру, по состояниям. Умозаключение может быть вероятностным, т.е. вычислением распределения вероятностей по интересующим состояниям на основе анализа данных и событий. Умозаключение также может означать методики, используемые для компоновки событий более высокого уровня из набора событий и/или данных. Такое умозаключение приводит к составлению новых событий или действий из набора наблюдаемых событий и/или сохраненных данных событий, независимо от того, коррелированны ли события в тесной временной близости и исходят ли события и данные из одного или нескольких источников событий и данных.

Следует принимать во внимание, что хотя термин "сообщение" широко используется в данном подробном описании, этот термин не ограничен электронной почтой самой по себе, но может быть надлежащим образом адаптирован, чтобы включать в себя электронное сообщение любой формы, обмен которыми может быть распределен по любой надлежащей коммуникационной архитектуре связи. Например, приложения проведения конференций, которые обеспечивают конференцию между двумя и более людьми (к примеру, программы интерактивных дискуссий и программы мгновенного обмена сообщениями), могут также использовать преимущества фильтрации, раскрытые в настоящем документе, поскольку лишний текст может электронным образом распространяться в обычных дискуссионных комнатах, когда пользователи обмениваются сообщениями, и/или вставлен в качестве начального сообщения, завершающего сообщения, или всего из вышеперечисленного. В этом конкретном приложении фильтр может быть обучен автоматически отфильтровывать конкретное содержимое сообщений

(текст и изображения), чтобы фиксировать и помечать как бесполезное нежелательное содержимое (к примеру, коммерческие предложения, продвижения товаров или рекламные объявления).

В представленном изобретении термин "получатель" означает адресата входящего сообщения или элемента. Термин "пользователь" означает получателя, который выбрал, пассивно или активно, принимать участие в системах и процессах контура обратной связи, описанных в данном документе.

Обратимся теперь к фиг.1A, где проиллюстрирована общая блок-схема обучающей системы 10 обратной связи в соответствии с аспектом настоящего изобретения. Компонент 12 приема сообщений принимает и доставляет входящие сообщения (обозначаемые как IM) намеченным получателям 14. Компонент приема сообщений может включать в себя, по меньшей мере, один фильтр 16, что является обычным в случае многих компонентов приема сообщений (к примеру, фильтр бесполезной почты), чтобы уменьшить доставку нежелательных сообщений (к примеру, несанкционированной рассылки). Компонент 12 приема сообщений вместе с фильтром 16 обрабатывает сообщения (IM) и предоставляет отфильтрованный поднабор сообщений (IM') намеченным получателям 14.

Как часть аспекта обратной связи представленного изобретения, компонент 18 опросов принимает все входящие сообщения (IM) и определяет соответствующих намеченных получателей 14. Компонент опросов выбирает поднабор намеченных получателей 14 (называемых борцами 20 с несанкционированной рассылкой), чтобы классифицировать поднабор входящих сообщений (отмеченных как IM") как несанкционированную рассылку или не несанкционированную рассылку, например. Связанная с классификацией информация (отмеченная как "ИНФОРМАЦИЯ О ГОЛОСОВАНИИ") отправляется в хранилище 22 сообщений/голосов, в котором информация о голосовании, а также копии соответствующих IM" сохраняются для будущего использования, например компонентом 24 обратной связи. В частности, компонент 24 обратной связи использует методики обучения машины (к примеру, нейронные сети, SVM, байесовы сети или любую систему обучения машины, подходящую для использования с представленным изобретением), которые используют информацию о голосовании, чтобы обучить и/или усовершенствовать фильтр 16 (и/или создать новый фильтр(ы)), например, в отношении определения несанкционированной рассылки. Поскольку новые потоки входящих сообщений обрабатываются посредством нового обученного фильтра 16, меньше несанкционированной рассылки и больше легитимных сообщений (отмечены как IM') доставляется намеченным получателям 14. Таким образом, система 10 обеспечивает определение несанкционированной рассылки и обучение усовершенствованных фильтров несанкционированной рассылки посредством использования обратной связи, сгенерированной борцами 20 с несанкционированной рассылкой. Данный аспект обратной связи представленного изобретения предоставляет имеющую широкие возможности и в высшей степени динамичную схему детализации системы распознавания несанкционированной рассылки. Далее подробно описаны подробности, касающиеся более детальных аспектов представленного изобретения.

Обратимся теперь к фиг.1B, где проиллюстрирована блок-схема 100 обучающей системы контура обратной связи в связи с борьбой с несанкционированной рассылкой и предотвращением несанкционированной рассылки в соответствии с аспектом настоящего изобретения. В ходе подготовки и/или до процесса обучения выбирают пользователей в качестве борцов с несанкционированной рассылкой (к примеру, из главного набора, содержащего всех пользователей электронной почты). Этот выбор может быть основан на случайной выборке или уровне доверия, либо любой другой схеме/критериях выбора в соответствии с представленным изобретением. Например, выбранный поднабор пользователей может включать в себя всех пользователей, случайно выбранный набор пользователей, тех, кто выбран в качестве борца с несанкционированной рассылкой, или тех, кто не выбран, и/или любое их сочетание, и/или частично на основе их демографического местоположения и связанной информации.

Альтернативно, главный набор пользователей электронной почты, из которого осуществляют выбор, может быть ограничен платящими пользователями, что может сделать более затратным для распространителей несанкционированной рассылки нанести вред представленному изобретению. Таким образом, поднабор пользователей, выбранных, чтобы принимать участие в борьбе с несанкционированной рассылкой, может содержать только платящих пользователей. После этого может быть создан список или таблица клиентов, включающий имена и свойства выбранных пользователей (к примеру, борцов с несанкционированной рассылкой).

Когда входящий поток сообщений 102 принят, получатель каждого сообщения проверяется на соответствие списку борцов с несанкционированной рассылкой на этапе 104. Если получатель находится в списке, то сообщение учитывается для опроса. Далее выполняется определение того, следует ли выбирать сообщение для опроса. В отличие от традиционных борцов с несанкционированной рассылкой изобретение не удаляет какие-либо сообщения (к примеру, несанкционированную рассылку) до тех пор, пока, по меньшей мере, вся входящая почта не будет учтена для опроса. Т.е. почта классифицируется до того, как она подвергается какому-либо присваиванию меток (к примеру, несанкционированная рассылка, не несанкционированная рассылка). Это облегчает получение объективной выборки сообщений, доступных для опроса пользователей.

Компонент выбора сообщений (не показан) может быть использован, чтобы выбрать сообщения с некоторой случайной вероятностью, чтобы уменьшить необъективность данных. Другой подход влечет за собой использование демографической информации, а также других атрибутов и свойств пользователя/получателя. Таким образом, сообщения могут быть выбраны на основе, по меньшей мере, частично пользователя/получателя. Для выбора сообщений существуют другие альтернативные алгоритмы. Тем не менее, возможны ограничения по числу сообщений, выбираемых на каждого пользователя или на каждого пользователя на каждый период времени, либо по вероятности выбора сообщения от любого заданного пользователя. Без этих ограничений распространитель несанкционированной рассылки может создать учетную запись, отправить ей миллионы сообщений с несанкционированной рассылкой и классифицировать все эти сообщения как полезные: это позволит распространителю несанкционированной рассылки повредить базу данных по обучению с помощью некорректно помеченных сообщений.

Некоторые формы фильтрации несанкционированной рассылки, чаще всего называемые списками черных дыр, могут не быть пропускаемыми. Списки черных дыр запрещают серверу прием какой-либо почты из списка IP-адресов. Поэтому выбор сообщений может быть выбран из набора почты, которая не из списка черных дыр.

Уникальный аспект изобретения состоит в том, что сообщения, выбранные для опроса, которые помечены используемыми в настоящее время фильтрами как несанкционированная рассылка, не удаляются или перемещаются в папку бесполезной почты. Вместо этого они помещаются в стандартную папку или почтовый ящик, куда принимаются все сообщения для учета в опросе. Тем не менее, если имеется две копии сообщения и сообщение считается фильтром несанкционированной рассылки, то копия доставляется в папку несанкционированной рассылки или иным образом интерпретируется согласно заданным параметрам (к примеру, удалено, специально помечено или перемещено в папку бесполезной почты).

Когда сообщение выбрано, оно переадресуется пользователю и помечается каким-либо специальным способом, чтобы указывать, что оно является сообщением для опроса. В частности, выбранное сообщение может быть модифицировано компонентом 106 модификации сообщений. Примеры модификации сообщений включают в себя, но не только, помещение сообщения для опроса в отдельную папку, изменение адреса "от" или строки темы и/или использования специального значка или специального цвета, который будет определять сообщение пользователю как сообщение для опроса. Выбранное сообщение также может быть заключено в другое сообщение, которое содержит инструкции пользователю о том, как голосовать и/или классифицировать заключенное сообщение. Эти

инструкции могут включать в себя, по меньшей мере, две кнопки или ссылки: одна, чтобы проголосовать за то, что сообщение является несанкционированной рассылкой, и одна, чтобы проголосовать за то, что сообщение не является несанкционированной рассылкой, например.

Кнопки для голосования могут быть реализованы посредством модификации содержимого сообщений перед отправкой копии сообщения для опроса пользователю. Когда изобретение используется по отношению к клиентскому почтовому программному обеспечению (в противоположность почтовому серверу), пользовательский интерфейс может быть модифицирован, чтобы включать в себя кнопки для голосования.

Более того, сообщение для опроса может содержать инструкции и кнопки для голосования, а также выбранное сообщение, прикрепленное к нему. Сообщение для опроса также может содержать сводку по выбранному сообщению, например строку темы, адрес от кого, отправленные и/или принятые данные и текст или, по меньшей мере, первые несколько строк текста. Другой подход влечет за собой отправку сообщения с инструкциями по голосованию и кнопками для голосования, присоединенными к нему. На практике, когда пользователь открывает и/или загружает копию сообщения для опроса, кнопки (или ссылки), включающие в себя, но не только, кнопки "несанкционированная рассылка" и "не несанкционированная рассылка", могут появиться на экране в пользовательском интерфейсе или могут быть заключены в сообщение для опроса. Таким образом, возможно, что каждое сообщение для опроса содержит набор инструкций и надлежащие кнопки для голосования. Могут быть необходимы другие модификации, включая вероятное удаление фоновых HTML-инструкций (которые могут сделать незаметным текст инструкций или кнопки).

Также может быть предусмотрена еще одна кнопка, такая как "электронная почта с коммерческим предложением", в зависимости от типа информации, который нужен. Сообщение также может включать в себя кнопку/ссылку на исключение из будущего опроса. Инструкции переводятся на предпочтительный язык пользователя и могут быть вложены в сообщение для опроса.

Более того, сообщения, выбранные для опроса, могут быть просканированы на вирусы компонентом 106 модификации сообщений или каким-либо другим подходящим компонентом сканирования на вирусы (не показан). Если обнаружен вирус, либо вирус может быть удален, либо сообщение может быть отброшено. Следует принимать во внимание, что удаление вируса может осуществляться в любой точке системы 100, в том числе и когда сообщение выбрано и перед тем, как пользователь загружает сообщение.

После модификации сообщения компонент 108 доставки сообщений доставляет сообщение для опроса пользователю для голосования. Обратной связи от пользователей (к примеру, сообщению для опроса, голосу пользователя и любым свойствам пользователя, ассоциированным с ним) назначается уникальный идентификатор (ID) 110 (к примеру, метаданные). ID 110 и/или информация, соответствующая ему, отправляется в хранилище 112 сообщений/голосов (к примеру, в центральную базу данных), где классификации/голоса пользователей компилируются и сохраняются.

На уровне базы данных сообщения, доступные для опроса, могут быть сохранены для дальнейшего опроса или использования. Помимо этого, база данных может выполнять анализ повторяемости на временной основе, чтобы удостоверяться, что в отношении конкретного пользователя выборка не осуществляется излишне часто и что от пользователя собирается объем данных в рамках ограничений, заданных пользователем. В частности, система 100 обратной связи отслеживает процентное ограничение почты пользователя, а также период выборки, чтобы уменьшить необъективность и выборки, и данных. Это особенно важно, если пользователи выбраны из всех доступных пользователей, включая и нечасто пользующихся почтой пользователей, и часто пользующихся почтой пользователей. Например, нечасто пользующийся почтой пользователь принимает и отправляет значительно меньший объем почты по сравнению с часто пользующимся почтой пользователем. Таким образом, система 100 отслеживает

процесс выбора сообщений, чтобы быть уверенной, что выбранное сообщение - это приблизительно одно из каждых T сообщений, принятых пользователем, и не более чем одно сообщение, принятое пользователем каждые Z часов. Следовательно, система может опросить 1 из каждых 10 входящих сообщений, которые должны быть отобраны (к примеру, рассмотрены для опроса), но не более 1 каждые 2 часа, к примеру. Ограничение по частоте или проценту уменьшает вероятность выборки непропорционального количества сообщений для пользователя, нечасто пользующегося почтой, по сравнению с пользователем, часто пользующимся почтой, а также уменьшает чрезмерное досаждение пользователю.

С небольшой периодичностью центральная база 112 данных сканирует сообщения, которые были выбраны системой 100 для опроса, но не были классифицированы. База данных извлекает эти сообщения и выполняет их локализацию относительно демографических свойств соответствующего пользователя, а также создает сообщения для опроса, чтобы запросить пользователя(ей) голосовать и классифицировать сообщение(я). Тем не менее, фильтр несанкционированной рассылки не может быть модифицирован или обучен сразу после приема каждой новой входящей классификации. Вместо этого автономное обучение позволяет блоку обучения постоянно проверять данные, принятые в базу 112 данных на запланированной, текущей или ежедневной основе. Т.е. блок обучения начинает с заданной начальной точки или с заданного времени в прошлом и проверяет все данные с этой точки вперед, чтобы обучить фильтр. Например, заданный период времени может быть от полуночи до 6:00.

Новый фильтр несанкционированной рассылки может быть обучен на текущей основе посредством анализа классификаций сообщений, сохраненных в базе 112 данных, с помощью методик 114 обучения машины (к примеру, нейронных сетей, методов опорных векторов (SVM)). Методики обучения машины требуют примеров и полезной почты, и несанкционированной рассылки, чтобы они могли научиться различать их. Даже методики, основанные на приведение в соответствие с известными примерами несанкционированной рассылки, могут извлечь пользу из наличия примеров полезной почты, чтобы они могли удостоверяться, что случайно не отлавливают полезную почту.

Следовательно, важно иметь положительные и отрицательные примеры несанкционированной рассылки вместо простых жалоб. Существуют некоторые домены, которые отправляют большие объемы и несанкционированной рассылки, и легитимной почты, например бесплатные рассылки. Если создана система только на основе жалоб, вся почта из этих доменов может быть отфильтрована, приводя к большому количеству ошибок. Следовательно, знание о том, что этот домен также отправляет большие объемы полезной почты, важно. Помимо этого, пользователи часто делают ошибки, например забывая, что они подписались на бесплатную рассылку. Например, крупный легитимный поставщик, такой как New York Times, регулярно отправляет легитимную почту. Некоторые пользователи забывают, что они подписались, и жалуются, классифицируя эти сообщения как несанкционированную рассылку. Без данных о том, что большинство пользователей понимают, что эта почта легитимна, почта с этого сайта может быть заблокирована.

Новый фильтр 116 может быть распространен на текущей основе компонентом 118 распространения между участвующими поставщиками услуг Интернета (ISP), почтовым серверам или серверам сообщений, отдельным почтовым клиентам, серверу обновлений и/или центральным базам данных отдельных компаний. Более того, система 100 обратной связи функционирует на текущей основе, так чтобы выборки сообщений, учитываемых и используемых для опроса, могли следовать фактическому распространению электронной почты, принятой системой 100. В результате наборы обучающих данных, используемые, чтобы обучать новые фильтры несанкционированной рассылки, актуализированы по отношению к адаптивным распространителям несанкционированной рассылки. Когда создаются новые фильтры, данные опроса могут быть отброшены или их вес может быть понижен (к примеру, пропущены) на основе того, как давно они были получены.

Система 100 может быть реализована, когда почта принята на сервере, например

шлюзе, сервере электронной почты и/или сервере сообщений. Например, когда почта приходит на сервер электронной почты, сервер проверяет свойства намеченных получателей, чтобы определить, были ли получатели выбраны в системе 100. Если их свойства указывают это, почта получателей потенциально доступна для опроса. Существуют также архитектуры только с клиентами. Например, клиентское почтовое программное обеспечение может принимать решения об опросе для одного пользователя и доставлять электронную почту либо центральной базе данных, либо использовать информацию по опросу, чтобы повысить эффективность персонализированного фильтра. Помимо описанных в данном документе существуют другие альтернативные архитектуры для этой системы 100, и они считаются подпадающими под объем настоящего изобретения.

Обратимся теперь к фиг.2, где проиллюстрирована блок-схема процесса 200 базового контура обратной связи в соответствии с аспектом настоящего изобретения. Хотя в целях упрощения пояснения методика показана и описана как последовательность действий, необходимо понимать и принимать во внимание, что настоящее изобретение не ограничено порядком действий, поскольку некоторые действия могут, в соответствии с настоящим изобретением, осуществляться в ином порядке и/или параллельно с другими действиями, что показано и описано в данном документе. Например, специалисты в данной области техники поймут и примут во внимание, что методика может быть альтернативно представлена как последовательность взаимосвязанных состояний или событий, например, на диаграмме состояний. Более того, не все проиллюстрированные действия могут быть необходимы, чтобы реализовать методику в соответствии с настоящим изобретением.

Процесс 200 начинается с почты, приходящей и принимаемой компонентом, например сервером, на этапе 202. Когда почта приходит на сервер, сервер определяет свойства намеченных получателей, чтобы определить, были ли намеченные получатели ранее выбраны в качестве борцов с несанкционированной рассылкой для опроса (на этапе 204). Таким образом, процесс 200 использует поле свойств пользователя, где может быть указано, был ли получатель выбран в системе обратной связи, или принимает во внимание список пользователей, которые были выбраны. Если определено, что пользователь является участником системы обратной связи, и был выбран для опроса на этапе 206, система обратной связи предпринимает действие посредством определения того, какие сообщения выбраны для опроса (этап 208). В противном случае процесс 200 возвращается к 202 до тех пор, пока не будет определено, что, по меньшей мере, один намеченный получатель входящего сообщения не является пользователем (к примеру, борцом с несанкционированной рассылкой).

На практике все сообщения учитываются для опроса, включая те сообщения, которые помечены (или будут помечены) как несанкционированная рассылка используемым в настоящее время фильтром (к примеру, персонализированным фильтром, фильтром Brightmail). Поэтому сообщения не удаляются, отбрасываются или отправляются в папки бесполезной почты до того, как они будут учтены для опроса.

Каждое сообщение или элемент почты, принятый сервером, имеет набор свойств, соответствующий почтовой транзакции. Сервер компилирует эти свойства и отправляет их вместе с сообщениями для опроса в центральную базу данных. Примеры свойств включают в себя список получателей (к примеру, перечисленных в полях "Кому:", "Копия: " и/или "Скрытая копия:"), вердикт используемого в настоящее время фильтра (к примеру, определил ли фильтр сообщение в качестве несанкционированной рассылки), вердикт другого необязательного фильтра несанкционированной рассылки (к примеру, фильтра Brightmail) и информацию о пользователе (к примеру, имя пользователя, пароль, настоящее имя, частота опрошенных сообщений, данные об использовании,...). Сообщению для опроса и/или его содержимому, а также соответствующему пользователю/получателю назначается уникальный идентификатор. Идентификатор также может быть отправлен в базу данных и впоследствии обновлен как требуется.

На этапе 214 сообщение(я), выбранное для опроса (к примеру, исходное сообщение 1-

M, где M - целое число, большее или равное одному), модифицируется, чтобы указать пользователю, что сообщение 1-M - это сообщение P1-PM для опроса, и затем доставляется пользователю для опроса (на этапе 216). Например, сообщение для опроса может включать в себя исходное сообщение, по которому необходимо проголосовать, в качестве вложения, и набор инструкций о том, как проголосовать по сообщению. Набор инструкций включает в себя, по меньшей мере, две кнопки, например кнопку "полезная почта" и кнопку "несанкционированная рассылка", например. Когда пользователь щелкает на одной из кнопок (на этапе 218), чтобы классифицировать сообщение как полезную почту или несанкционированную рассылку, пользователь направляется к уникальному указателю информационного ресурса (URL), который соответствует уникальному идентификатору для классификации, которую отправляет пользователь. Эта информация отправляется, и ассоциированная запись в центральной базе данных для этого исходного сообщения 1-M обновляется.

На этапе 216 или в любое другое подходящее время в процессе 200 исходное сообщение может в необязательном порядке быть доставлено пользователю. Таким образом, пользователь принимает сообщение дважды - один раз в его исходной форме и повторно в его модифицированной форме для опроса.

Позднее новый фильтр несанкционированной рассылки создается и обучается на этапе 220 на основе, по меньшей мере, частично обратной связи от пользователя. После того, как новый фильтр несанкционированной рассылки был создан и обучен, фильтр может сразу же быть использован на сервере электронной почты и/или может быть распространен клиентским серверам, клиентскому почтовому программному обеспечению и т.п. (на этапе 222). Обучение и распространение нового или обновленного фильтра несанкционированной рассылки является текущей деятельностью. Таким образом, процесс 200 переходит к этапу 204, когда принят новый поток входящих сообщений. Когда создаются новые фильтры, старые данные отбрасываются или их вес понижается на основе того, как давно они были получены.

Система 100 обратной связи и процесс 200 основываются на обратной связи от участвующих пользователей. К сожалению, некоторым пользователям нельзя доверять или они просто ленивы и не предоставляют непротиворечивые и точные классификации. Центральная база 112 данных (фиг.1a) хранит предысторию пользовательских классификаций. Таким образом, система 100 обратной связи может отслеживать число несоответствий, число раз, когда пользователь передумал, ответы пользователя на известную полезную почту или известную несанкционированную рассылку, а также число или частоту ответов пользователя на сообщения для опроса.

Когда любое из этих чисел превышает заданный порог, или просто для каждого пользователя системы система 100 обратной связи может активировать одну из нескольких методик проверки, чтобы оценить степень доверия конкретному пользователю или пользователям. Один подход - способ 300 перекрестной проверки, проиллюстрированный на фиг.3, в соответствии с другим аспектом настоящего изобретения.

Методика перекрестной проверки начинается на этапе 302 с приема центральной базой данных входящих данных, например результатов опроса и соответствующей информации о пользователе. Далее необходимо определить, требуется ли перекрестная проверка, чтобы протестировать надлежащее число пользователей на этапе 304. Если она требуется, то новый фильтр несанкционированной рассылки обучается с помощью определенной части входящих данных на этапе 306. Т.е. данные от пользователей, которые тестируются, исключаются из обучения. Например, фильтр обучается с помощью около 90% данных опрошенного пользователя (обозначен как фильтр 90%), в связи с этим исключая около 10% данных (обозначены как протестированный на 10% пользователь), что соответствует данным, отправленным протестированным пользователем.

На этапе 308 фильтр 90% запускается для оставшихся данных протестированного на 10% пользователя, чтобы определить, как бы проголосовали пользователи 90% по сообщениям протестированного пользователя. Если количество несовпадений между

фильтром 90% и данными протестированного на 10% пользователя превышает заданный порог (на этапе 310), то классификации пользователя могут быть проверены вручную на этапе 312. Альтернативно или помимо этого, тестовые сообщения могут быть отправлены вызывающим подозрения или недоверенным пользователям, и/или эти конкретные пользователи могут быть исключены из будущего опроса, и/или их прошлые данные отброшены. Тем не менее, если порог не превышен, то процесс возвращается к этапу 306. На практике методика 300 перекрестной проверки может быть использована с любым подходящим набором тестовых пользователей, исключая различных пользователей при необходимости, чтобы определять и поддерживать доверие данных голосования/классификации.

Второй подход, чтобы оценивать лояльность и надежность пользователей, включает в себя обучение фильтра на данных, собранных в заданный период, и затем тестирование на обучающих данных с помощью фильтра. Эта методика известна как "тестирование на обучении". Если сообщение было включено в обучение, фильтр должен изучить его рейтинг, к примеру обучающийся фильтр должен классифицировать сообщение так же, как это сделал пользователь. Тем не менее, фильтр может продолжить делать ошибку на нем, помечая его как несанкционированную рассылку, когда пользователь пометил его как не несанкционированную рассылку, или наоборот. Чтобы фильтр разошелся со своими обучающими данными, сообщение должно сильно расходиться с другими сообщениями. В противном случае, обученный фильтр практически достоверно нашел бы какой-либо способ, чтобы корректно классифицировать его. Таким образом, сообщение может быть отброшено как имеющее ненадежную пометку. Может быть использована либо эта методика, либо перекрестная проверка: перекрестная проверка позволяет извлекать больше ошибок в классификациях менее надежно; наоборот, тестирование на обучении находит меньше ошибок более надежно.

И методика тестирования на обучении, и методика 300 перекрестной проверки может быть применена к отдельным сообщениям, при этом классификация или рейтинг сообщения отдельного пользователя исключается посредством общего соглашения (к примеру, следуя рейтингу большинства). Альтернативно, обе методики могут быть использованы, чтобы определять потенциально ненадежных пользователей.

Помимо или вместо методик перекрестной проверки и/или тестирования на обучении мы можем использовать методику "известных результатов", чтобы удостовериться в доверии пользователю (переход к этапу 314 на фиг.4). Хотя методики фиг.3 и 4 продемонстрированы отдельно, следует принимать во внимание, что оба подхода могут быть использованы одновременно. Т.е. информация из известных как полезные и известных как несанкционированная рассылка сообщений может быть объединена с результатами перекрестной проверки или тестирования на обучении, чтобы определить, каких пользователей отбросить.

Обратимся теперь к фиг.4, где проиллюстрирована блок-схема процесса 400 проверки лояльности голосования пользователя в соответствии с одним аспектом настоящего изобретения. Процесс 400 направляется с этапа 314, как показано на фиг.3. На этапе 402 тестовое сообщение(я) с известным результатом отправляется вызывающему подозрение пользователю(ям) (или всем пользователям). Например, тестовое сообщение может быть добавлено во входящую почту и затем классифицировано вручную, так что база данных принимает "известный" результат. В противном случае процесс 400 может подождать, пока сообщение с известным результатом не будет отправлено третьей стороной. Пользователям разрешено голосовать по одним и тем же тестовым сообщениям. Результаты голосования сравниваются с известными результатами на этапе 404. Если голоса пользователей расходятся на этапе 406, то их текущие и/или будущие, и/или прошлые классификации могут быть проверены вручную за подходящий период времени (на этапе 408), пока они не продемонстрируют соответствие и надежность. Альтернативно, их текущие или будущие, либо прошлые классификации могут быть пропущены или удалены. Наконец, пользователи могут быть удалены из будущего

голосования. Тем не менее, если результаты их голосования совпадают с результатами тестовых сообщений, то пользователи могут быть рассмотрены как доверенные на этапе 410. Процесс 400 возвращается на этапе 412 к фиг.3, чтобы определить, какой тип методики проверки требуется для следующей группы вызывающих подозрения пользователей.

Четвертый подход (не показан) для оценки надежности пользователей - активное обучение. С помощью методик активного обучения сообщения не перебираются на случайной основе. Вместо этого система обратной связи может оценить, насколько полезным будет сообщение для системы. Например, если фильтр возвращает вероятность несанкционированной рассылки, можно предпочтительно выбрать сообщения, которые наиболее неопределенно классифицированы текущим фильтром для опроса, т.е. те, вероятность несанкционированной рассылки которых ближе всего к 50%. Другой способ выбирать сообщения - определять, насколько сообщение обычно. Чем более обычно сообщение, тем более полезно оно, чтобы опрашивать. Уникальные сообщения менее полезны, поскольку они мене обычны. Активное обучение может быть использовано с помощью уровней доверия существующих фильтров, с помощью того, насколько обычными являются признаки сообщения, и с помощью уровней доверия параметров или содержимого (к примеру, метадоверия) существующего фильтра. Существует множество других методик активного обучения, например запрос комиссией, широко известных специалистам в области техники обучения машины, и любые из этих методик могут быть использованы.

Обратимся теперь к фиг.5, где проиллюстрирована блок-схема процесса 500 для добавления обратной связи от электронной приманки в дополнение к обратной связи от пользователей в обучение фильтра несанкционированной рассылки в соответствии с одним аспектом настоящего изобретения. Электронные приманки - это адреса электронной почты, для которых известно, кто должен отправлять на них электронную почту. Например, вновь созданный адрес электронной почты может быть сохранен в секрете и раскрыт только избранным лицам (на этапе 502). Они также могут быть раскрыты публично, но ограниченно, незаметно для людей (к примеру, помещение их на белом фоне белым шрифтом как почтовой ссылки). Электронные приманки особенно полезны при словарных атаках распространителей несанкционированной рассылки. Словарная атака - это атака, при которой распространитель несанкционированной рассылки пытается отправить по почте очень большое число адресов, возможно всех адресов из словаря, или составленных из пар слов в словаре, или аналогичные методики, чтобы находить допустимые адреса. Любая электронная почта, отправленная электронной приманке (на этапе 504), или любая электронная почта не от нескольких избранных лиц (на этапе 506) считается несанкционированной рассылкой (на этапе 508). Адрес электронной почты также может быть подписан вызывающим подозрение коммерсантом. Таким образом, любая почта, принятая от коммерсанта, считается легитимной почтой (на этапе 510), а вся остальная почта считается несанкционированной рассылкой. Фильтр несанкционированной рассылки может быть обучен соответствующим образом (на этапе 512). Более того, определяется вызывающий подозрение коммерсант, чтобы продавать или иным образом раскрывать информацию о пользователе (к примеру, по меньшей мере, адрес электронной почты) третьей стороне. Это может быть повторено с другими вызывающими подозрение коммерсантами, и может быть сгенерирован список, чтобы предупреждать пользователей, что их информация может быть распространена распространителям несанкционированной рассылки. Существует небольшое количество методик получения электронной почты, отправленной электронным приманкам, которая может безошибочно считаться несанкционированной рассылкой. На практике существуют другие альтернативные способы, чтобы получать электронную почту, отправленную электронным приманкам, которая может безошибочно считаться несанкционированной рассылкой.

Поскольку электронные приманки - это хороший источник несанкционированной рассылки, но ужасный источник легитимной почты, данные из электронных приманок могут

быть объединены с данными от системы контура обратной связи (фиг.1), чтобы обучать новые фильтры несанкционированной рассылки. Почта из различных источников или различных классификаций может быть взвешена по-разному. Например, если имеется 10 электронных приманок и 10 пользователей, которые опрошены по 10% их почты около 10 раз, столько несанкционированной рассылки должно быть ожидаемо от электронных приманок, сколько из опроса. Поэтому легитимная почта из опроса может быть взвешена 10 или 11 раз столько, сколько несанкционированной рассылки, чтобы компенсировать эту разницу. Альтернативно, вес данных электронных приманок может быть выборочно понижен. Например, около 50% почты пользователя - это полезная почта, и около 50% ее - это несанкционированная рассылка. Тот же объем несанкционированной рассылки идет в электронные приманки. Поэтому похоже, что электронная приманка имеет 100% несанкционированной рассылки, и выбрана она вся, а не 10%. Чтобы обучать с корректными соотношениями несанкционированной рассылки и полезной почты в объединенной системе, вес данных электронной приманки понижается на 95%, и вес пользовательской несанкционированной рассылки понижается на 50%, чтобы привести к общему соотношению 1:1.

Другие источники отчетов о несанкционированной рассылке включают в себя пользователей, которые не включены в качестве участников в систему контура обратной связи. Например, может быть предусмотрена кнопка "Report Spam", доступная для всех пользователей для всей почты, чтобы сообщать о несанкционированной рассылке, которая прошла через фильтр. Эти данные могут быть объединены с данными из системы контура обратной связи. Кроме того, вес этого источника несанкционированной рассылки должен быть понижен или он должен быть взвешен иначе, поскольку он может быть необъективным или недоверенным в различных аспектах. Перевзвешивание должно также быть выполнено, чтобы отразить тот факт, что только почта, которая не была отфильтрована, подлежит сообщению посредством кнопки "Report-as-spam".

Помимо фильтра несанкционированной рассылки фильтр карантина может быть создан и использован системой контура обратной связи. Фильтр карантина использует и положительные, и отрицательные признаки почты. Например, почта от популярного онлайнового коммерсанта почти всегда полезна. Распространитель несанкционированной рассылки пользуется системой посредством имитации аспекта полезной коммерческой почты в своей несанкционированной рассылке. Другой пример состоит в том, что распространитель несанкционированной рассылки намеренно вводит в заблуждение систему обратной связи посредством отправки небольших объемов полезной почты через IP-адрес. Контур обратной связи учится классифицировать эту почту как полезную почту, когда в то же время распространитель несанкционированной рассылки начинает отправлять несанкционированную рассылку с того же IP-адреса.

Таким образом, фильтр карантина уведомляет о том, что принимается конкретный позитивный признак в гораздо больших объемах, чем используется системой, на основе данных за прошлые периоды. Это служит причиной для системы быть недоверчивой к сообщению и, следовательно, помещать его на карантин, пока не будут получены достаточные результаты опроса, перед выбором, чтобы доставить или пометить почту как несанкционированную рассылку. Фильтр карантина также может быть использован, когда почта принята с нового IP-адреса, для которого неизвестно или не бесспорно, является почта несанкционированной рассылкой или не несанкционированной рассылкой, и это не будет известно в течение какого-то времени. Помещение на карантин может быть осуществлено рядом способов, включая временную пометку почты как несанкционированной рассылки и ее перемещение в папку несанкционированной рассылки или недоставку ее пользователю, или сохранение ее где-либо, где ее не будет видно. Помещение на карантин может быть выполнено для сообщений, которые почти достигли порога фильтра несанкционированной рассылки: может быть предположено, что дополнительная информация из опроса поможет принять корректное решение. Помещение на карантин также может быть выполнено, когда принято множество аналогичных

сообщений: несколько сообщений может быть отправлено для опроса с помощью контура обратной связи, и переобученный фильтр может быть использован, чтобы корректно классифицировать сообщения.

Помимо создания фильтров система контура обратной связи, описанная в данном документе, может быть использована, чтобы также оценивать их. Т.е. параметры фильтров несанкционированной рассылки могут быть настроены как требуется. Например, фильтр обучен до полуночи прошлой ночи. После полуночи берутся данные, которые приходят в базу данных, чтобы определять частоты ошибок фильтра несанкционированной рассылки по сравнению с классификациями пользователей. Дополнительно, контур обратной связи может быть использован, чтобы определять частоту ошибочных положительных результатов и поимок фильтром несанкционированной рассылки. Например, голоса пользователя могут быть приняты, и почта может быть пропущена через потенциальный фильтр, чтобы определить частоту ошибочных положительных результатов и поимок. Эта информация затем может быть использована, чтобы настраивать и оптимизировать фильтр. Различные значения параметров или различные алгоритмы могут быть вручную или автоматически испробованы посредством создания нескольких фильтров, при этом использует отличающуюся от других настройку или алгоритм, чтобы получить наименьшие частоты ошибочных положительных каждый результатов и поимок. Таким образом, результаты могут быть сравнены, чтобы выбрать наилучшие или оптимальные параметры фильтра.

Контур обратной связи может быть использован для создания и заполнения списка IP-адресов или доменов URL-адресов, за которые всегда голосовали как за несанкционированную рассылку или всегда голосовали как за полезные, или голосовали по меньшей, мере, как за полезные на 90% и т.д. Эти списки могут быть использованы для фильтрации несанкционированной рассылки другими способами. Например, список IP-адресов, за который голосовали, по меньшей мере, на 90% как несанкционированную рассылку, может быть использован для создания списка черных дыр из адресов, от которых не принимать почту. Контур обратной связи также может быть использован, чтобы прекратить действие учетных записей распространителей несанкционированной рассылки. Например, если конкретный пользователь ISP, как предполагается, отправляет несанкционированную рассылку, ISP может быть автоматически уведомлен. Аналогично, если конкретный домен, как предполагается, несет ответственность за большой объем несанкционированной рассылки, поставщик электронной почты домена может быть автоматически уведомлен.

Существует ряд архитектур, которые могут быть использованы, чтобы реализовать систему контура обратной связи. Одна типичная процедура основана на сервере, как описано на фиг.7, с процессом выбора, происходящим, когда почта достигает сервера электронной почты. Альтернативная архитектура основана на клиенте, как описано на фиг.6. В основанном на клиенте контуре обратной связи информация по опросу может быть использована, чтобы повысить производительность персонализированного фильтра, или в проиллюстрированной здесь типичной реализации информация может быть отправлена в совместно используемое хранилище в качестве обучающих данных для совместно используемого фильтра (к примеру, корпоративное или глобальное). Следует принимать во внимание, что описанные ниже следующие архитектуры являются просто типичными и могут включать в себя дополнительные компоненты и признаки, не указанные в данном документе.

Обратимся теперь к фиг.6, где проиллюстрирована общая блок-схема методики контура обратной связи в основанной на клиенте архитектуре. Сеть 600 предоставлена, чтобы обеспечить передачу электронной почты к и от одного или более клиентов 602, 604 и 606 (также обозначены как КЛИЕНТ1, КЛИЕНТ2,..., КЛИЕНТN, где N - целое число, большее или равное одному). Сетью может быть сеть глобальной связи (GCN), например Интернет или глобальная сеть (WAN), локальная сеть (LAN), или любая другая подходящая сетевая конфигурация. В этой конкретной реализации шлюз 608 протокола SMTP взаимодействует

с сетью 600, чтобы предоставлять услуги SMTP для LAN 610. Сервер 612 электронной почты, при работе размещенный в LAN 610, взаимодействует с шлюзом 608, чтобы управлять и обрабатывать входящую и исходящую электронную почту клиентов 602, 604 и 606. Эти клиенты 602, 604 и 606 также размещены в LAN 610, чтобы осуществлять доступ, по меньшей мере, к почтовым услугам, предоставляемым ей.

Клиент 602 включает в себя центральный процессор (CPU) 614, который управляет процессами клиента. CPU 614 может содержать несколько процессоров. CPU 614 исполняет инструкции в связи с предоставлением любой из одной или более функций сбора данных/обратной связи, описанных выше. Инструкции включают в себя, но не только, закодированные инструкции, которые исполняют, по меньшей мере, одну вышеописанную базовую методику контура обратной связи, по меньшей мере, любые или все подходы, которые могут быть использованы в сочетании для адресации клиента и выбора сообщений, модификации сообщений для опроса, хранения данных, проверки надежности клиентов и классификации, перевзвешивания данных из нескольких источников, включая систему контура обратной связи, оптимизацию и настройку фильтра несанкционированной рассылки, фильтры карантина, создание списков несанкционированной рассылки и автоматическое уведомление о распространителях несанкционированной рассылки их соответствующим ISP и поставщикам услуг электронной почты. Пользовательский интерфейс 616 предоставлен, чтобы обеспечить обмен данными с CPU 614 и клиентской операционной системой, так чтобы клиенты могли взаимодействовать с целью осуществления доступа к электронной почте и голосования по сообщениям для опроса.

Выборка клиентских сообщений, извлеченных из сервера 612, может быть выбрана для опроса посредством селектора 620 сообщений. Сообщения выбираются и модифицируются для опроса, если намеченный получатель (клиент) ранее согласился принимать участие. Модификатор 622 сообщений модифицирует сообщение, чтобы оно стало сообщением для опроса. Например, сообщение(я) может быть модифицировано так, чтобы включать в себя инструкции по голосованию и кнопки и/или ссылки для голосования согласно описаниям модификации сообщений, предоставленным выше. Кнопки и/или ссылки для голосования реализованы посредством модификации пользовательского интерфейса 616 клиентского почтового программного обеспечения. Помимо этого, модификатор 622 сообщений может удалять любые вирусы в сообщениях (сообщениях для опроса и не для опроса) до того, как они открываются или загружаются для просмотра клиентом 602.

В одной реализации пользователь клиента 602 борьбы с несанкционированной рассылкой видит каждое сообщение только один раз, при этом некоторые сообщения специально помечены как сообщения для опроса и включают в себя кнопки для голосования и т.д. В представленной реализации пользователь клиента 602 борьбы с несанкционированной рассылкой может видеть некоторые сообщения дважды, при этом одно - это обычное сообщение, а другое - сообщение для опроса. Это может быть реализовано несколькими способами. Например, сообщение для опроса может быть возвращено серверу 612 и сохранено в хранилище опрошенных сообщений. Альтернативно, клиент 602 может сохранять дополнительное сообщение в сервере 612 электронной почты. Альтернативно, клиент 602 может показывать пользователю каждое сообщение дважды, один раз как обычное сообщение и один раз в модифицированной форме.

Результаты 626 опроса могут быть отправлены CPU 614 и затем в базу 630 данных, которая может быть сконфигурирована, чтобы сохранять данные от одного клиента или более чем одного клиента, в зависимости от конкретной организации архитектуры обратной связи с клиентом. Центральная база 630 данных сохраняет сообщения для опроса, результаты опроса, а также информацию о соответствующем клиенте-пользователе. Соответствующие компоненты могут быть использованы, чтобы анализировать эту информацию, например определять частоту опросов, степень доверия

клиенту-пользователю (к примеру, проверку 632 достоверности пользователя) и другую статистику по клиенту. Методики проверки достоверности могут быть использованы особенно в том случае, когда надежность голосования клиента вызывает вопросы. Подозрение может возникать из анализа числа противоречий, числа измененных решений и числа сообщений, опрошенных для конкретного пользователя или пользователей; альтернативно, методики проверки достоверности могут быть использованы для каждого пользователя. Любой подходящий объем данных, сохраненный в центральной базе данных, может быть использован в методиках 634 обучения машины, чтобы обеспечить обучение нового и/или усовершенствованного фильтра несанкционированной рассылки.

Клиенты 604 и 606 включают в себя аналогичные компоненты, описанные выше, чтобы получать и обучать фильтр, который персонализирован для конкретного клиента(ов). Помимо того, что было описано, очиститель 628 опрошенных сообщений может согласовывать CPU 614 и центральную базу 630 данных, так чтобы аспекты опрошенного сообщения могли быть удалены по множеству причин, например агрегирование данных, сжатие данных и т.д. Очиститель 628 опрошенных сообщений может устранять посторонние части опрошенного сообщения, а также любую нежелательную информацию, ассоциированную с ним.

Обратимся теперь к фиг.7, где проиллюстрирована типичная основанная на сервере система 700 контура обратной связи, которая обеспечивает многопользовательский вход в систему и которая получает данные опроса в соответствии с методиками контура обратной связи настоящего изобретения. Сеть 702 предусмотрена, чтобы облегчать передачу электронной почты к и от одного или более пользователей 704 (также отмеченных как ПОЛЬЗОВАТЕЛЬ1 7041, ПОЛЬЗОВАТЕЛЬ2 7042... и ПОЛЬЗОВАТЕЛЬN 704N, где N - целое число, большее или равное одному). Сетью 702 может быть сеть глобальной связи (GCN), например Интернет или глобальная сеть (WAN), локальная сеть (LAN) или любая другая подходящая сетевая конфигурация. В этой конкретной реализации шлюз 710 протокола SMTP взаимодействует с сетью 702, чтобы предоставлять услуги SMTP для LAN 712. Сервер 714 электронной почты, при работе размещенный в LAN 712, взаимодействует с шлюзом 710, чтобы управлять и обрабатывать входящую и исходящую электронную почту пользователей 704.

Система 700 предоставляет возможность многопользовательского входа в систему, так чтобы выбор 716 пользователей и сообщений, модификация 718 сообщений и опрос (720, 722, 724) сообщений осуществлялся для каждого отдельного пользователя, который входит в систему 700. Таким образом, предусмотрен пользовательский интерфейс 726, который представляет экран входа в систему в качестве части процесса загрузки операционной системы вычислительной машины или, при необходимости, чтобы захватывать ассоциированный профиль пользователя до того, как пользователь 704 сможет осуществлять доступ к своим входящим сообщениям. Таким образом, когда первый пользователь 704 (ПОЛЬЗОВАТЕЛЬ1) выбирает осуществить доступ к сообщениям, первый пользователь 704 входит в систему посредством экрана 728 входа в систему, вводя информацию доступа, в типичном случае в форме имени пользователя и пароля. CPU 730 обрабатывает информацию доступа, чтобы дать возможность доступа пользователю, посредством приложения обмена сообщениями (к примеру, почтового клиента) только для расположения 732 папки входящих сообщений первого пользователя.

Когда входящая почта принимается на сервере 714 сообщений, они случайно выбираются для опроса, что означает, что, по меньшей мере, одно из сообщений помечается для опроса. Намеченные получатели помеченных сообщений проверяются, чтобы определить, является ли кто-либо из этих получателей назначенным пользователем, борющимся с несанкционированной рассылкой. Свойства получателей, показывающие эту информацию, могут быть сохранены на сервере 714 сообщений или в любом другом компоненте системы 700 по необходимости. После того, как определено, какие намеченные получатели также являются борцами с несанкционированной рассылкой, копия их соответствующей почты, а также любая другая информация, касающаяся почтовой

транзакции, может быть отправлена в центральную базу 734 данных для хранения. Сообщения, помеченные для опроса, модифицируются модификатором 718 сообщений любым числом способов, описанных выше. Сообщения, выбранные для опроса, могут также быть специфическими для пользователя 704. Например, пользователь 704 может указать, что только определенные типы сообщений доступны для опроса. Поскольку это может привести к необъективной выборке данных, эти данные могут быть перевзвешены по отношению к данным по другим клиентам, чтобы уменьшить вероятность построения непропорциональных наборов обучающих данных.

Сканирование на вирусы сообщений для опроса может также быть выполнено в это время или в любое другое время до того, как сообщение для опроса будет загружено и/или открыто пользователем 704. После того, как сообщения были модифицированы надлежащим образом, они доставляются в папки входящих сообщений (INBOX) соответствующих пользователей, которые обозначены как INBOX1 732, INBOX2 736 и INBOXN 738, где они могут быть открыты для опроса. Чтобы обеспечить процесс опроса, каждое сообщение для опроса включает в себя две или более кнопки или ссылки для голосования, которые, будучи выбраны пользователем, генерируют информацию, относящуюся к сообщению для опроса и результату опроса. Текст каждого сообщения для опроса может быть модифицирован, чтобы включить в себя кнопки или ссылки для голосования.

Результаты опроса по сообщениям (обозначенные как MESSAGE POLL1 720, MESSAGE POLL2 722 и MESSAGE POLLN 724), которые включают в себя любую информацию, следующую из классификации (к примеру, сообщение для опроса или ассоциированный с ним идентификатор, свойства пользователя), отправляются в центральную базу 734 данных посредством сетевого интерфейса 740 в ЛВС 712. Центральная база 734 данных может сохранять информацию об опросе и пользователях (720, 722, 724) от соответствующих пользователей, чтобы применять к методикам обучения машины с целью создания или оптимизации нового и/или усовершенствованного фильтра 742 несанкционированной рассылки. Тем не менее, по соображениям конфиденциальности и/или безопасности конфиденциальная информация может быть удалена или вычищена из информации до того, как она отправляется в центральную базу 714 данных. Информация, сгенерированная пользователем(ями) 704 посредством опроса, также может быть агрегирована в статистические данные. Таким образом, используется меньшая пропускная способность, чтобы передавать информацию.

Вновь обученный фильтр 742 несанкционированной рассылки затем может быть распространен другим серверам (не показаны), а также клиентскому почтовому программному обеспечению (не показано), взаимодействующему с LAN 712 на текущей основе, например когда новый фильтр доступен, посредством конкретного запроса или автоматически. Например, новый фильтр несанкционированной рассылки может быть автоматически выдан и/или сделан доступным для загрузки посредством Web-сайта. Когда новые наборы обучающих данных сгенерированы, чтобы создать новые фильтры несанкционированной рассылки, более старые наборы данных (к примеру, информация, ранее полученная и/или используемая для обучения фильтра) могут быть отброшены или удалены в зависимости от возраста данных.

Рассмотрим теперь альтернативный сценарий, в котором организация, участвующая в борьбе с несанкционированной рассылкой, делает доступным фильтр, совместно используемый многими различными использующими фильтр организациями. В одном аспекте изобретения поставщик фильтра также является очень крупным поставщиком услуг электронной почты (к примеру, платных и/или бесплатных почтовых учетных записей). Вместо того, чтобы полагаться исключительно на электронную почту от собственной организации, поставщик фильтра выбирает также использовать некоторые данные от нескольких использующих фильтр организаций, с тем чтобы лучше фиксировать диапазон полезной почты и несанкционированной рассылки. Система контура обратной связи, описанная выше, может также быть использована в таком сценарии с несколькими

организациями, в основанной на сервере или клиенте архитектуре. Мы будем называть поставщика фильтра, который агрегирует данные от своих пользователей и других использующих фильтр организаций, "внутренней" организацией, а компоненты, постоянно размещенные в одной из участвующих использующих фильтр организаций, "внешними". В общем, межорганизационная система включает в себя сервер почтовых баз данных у поставщика фильтра (внутреннего), такого как, но не только, Hotmail, и один или более серверов сообщений (внешних), таких как те, которые могут быть размещены в одной или более отдельных компаниях. В этом случае внутренний сервер почтовых баз данных также сохраняет важную обратную связь по электронной почте от своих клиентов. Согласно этому аспекту представленного изобретения, наборы обучающих данных могут быть сгенерированы на основе информации, сохраненной во внутренней базе данных (к примеру, бесплатной электронной почте/обмену сообщениями на сервере Hotmail или MSN), а также информации, сохраненной в одной или более внешних базах данных, ассоциированных с соответствующими внешними серверами. Информация, хранящаяся во внешних базах данных, может быть передана внутреннему серверу по сети, такой как Интернет, например для использования в методиках обучения машины. В конечном счете данные из внешних баз данных могут быть использованы, чтобы обучать новые фильтры несанкционированной рассылки и/или совершенствовать используемые фильтры несанкционированной рассылки, расположенные внутри (к примеру, в соответствующей компании) или ассоциированные с внутренним почтовым сервером.

Данные из одной или более внешних баз данных должны включать в себя, по меньшей мере, одно из сообщений для опроса, результатов опроса (классификаций), информации/свойств пользователя и статистических данных о голосовании на каждого пользователя, группу пользователей или в среднем для каждой компании. Статистические данные о голосовании обеспечивают определение надежности информации, сгенерированной соответствующими компаниями, а также уменьшают необъективность внешних данных. Таким образом, данные из одной или более внешних баз данных (компаний) могут быть перевзвешены или взвешены отлично от одной или более других внешних баз данных. Более того, внешние объектные сущности могут быть протестированы на надежность и степень доверия с помощью аналогичных методик проверки достоверности, описанных выше.

Для безопасности, секретности и конфиденциальности компании информация или данные, передаваемые по Интернету для каждой компании, например, на сервер электронной почты, могут быть очищены, сокращены и/или выражены в сжатой форме по отношению к исходной форме. Исходная форма может быть сохранена в соответствующей внешней базе данных и/или иным образом интерпретирована согласно предпочтениям каждой компании. Таким образом, сервер электронной почты или любой другой внутренний почтовый сервер принимает только уместную информацию, необходимую для генерирования обучающих данных, таких как классификации несанкционированной рассылки, домен отправителя, имя отправителя, содержимое сообщений, классифицированных как несанкционированная рассылка и т.п.

Обратимся теперь к фиг.8, где проиллюстрирована типичная межорганизационная система 800 обратной связи, в которой внутренний сервер баз данных и внешний почтовый сервер могут передавать и обмениваться информацией из базы данных посредством сети, чтобы обеспечить генерирование наборов обучающих данных, используемых в методиках обучения машины, с целью создания усовершенствованных фильтров несанкционированной рассылки. Система 800 включает в себя, по меньшей мере, один внешний сервер 802 сообщений (к примеру, ассоциированный с, по меньшей мере, одной компанией) и внутренний сервер 804 баз данных. Вследствие сущности межорганизационной системы внешний сервер 802 и внутренний сервер 804 электронной почты, соответственно, хранят собственные базы данных. Т.е. сервер 804 электронной почты ассоциирован с внутренней базой 806 данных, которая также может быть использована, чтобы обучать новый фильтр 808 несанкционированной рассылки. Так же,

внешний сервер 802 ассоциирован с внешней базой 810 данных, которая может быть использована, чтобы обучать, по меньшей мере, один новый фильтр 812 несанкционированной рассылки, а также фильтр 808 несанкционированной рассылки, размещенный внутренним образом по отношению к серверу 804 электронной почты. Таким образом, информация, сохраненная во внешней базе 810 данных, может быть использована, чтобы обучать фильтр 808 несанкционированной рассылки, размещенный на сервере электронной почты.

GCN 814 предусмотрена, чтобы обеспечить передачу информации на и от внутреннего сервера 804 электронной почты и одного или более внешних серверов 802 сообщений. Компонент внутреннего сервера(ов) межорганизационной системы работает аналогично основанной на сервере системе контура обратной связи (к примеру, см. фиг.7 выше). Например, сервер 802 сообщений, внешняя база 810 данных и фильтр 812 могут быть размещены в LAN 815. Помимо этого, предусмотрен пользовательский интерфейс 816, который представляет экран 818 входа в систему в качестве части процесса загрузки операционной системы вычислительной машины или, при необходимости, чтобы захватывать ассоциированный профиль пользователя до того, как пользователь(и) сможет осуществлять доступ к своим входящим сообщениям.

В этой основанной на сервере системе один или более пользователей (обозначенных как ПОЛЬЗОВАТЕЛЬ1 820, ПОЛЬЗОВАТЕЛЬ2 822, ПОЛЬЗОВАТЕЛЬN 824) могут входить в систему одновременно, чтобы использовать доступные почтовые услуги. На практике, когда первый пользователь 820 (ПОЛЬЗОВАТЕЛЬ1) выбирает осуществить доступ к сообщениям, первый пользователь 820 входит в систему посредством экрана 818 входа в систему, вводя информацию доступа, в типичном случае в форме имени пользователя и пароля. CPU 826 обрабатывает информацию доступа, чтобы дать возможность доступа пользователю, посредством приложения обмена сообщениями (к примеру, почтового клиента) только для расположения 828 папки входящих сообщений первого пользователя.

Когда входящая почта принимается на сервере 802 сообщений, сообщения случайным или специальным образом предназначаются для опроса. Прежде чем сообщения могут быть выбраны для опроса, намеченные получатели этих целевых сообщений сравниваются со списком пользователей-борцов с несанкционированной рассылкой, чтобы определить, является ли какой-либо из получателей также назначенным пользователем, борющимся с несанкционированной рассылкой. Свойства получателей, показывающие эту информацию, могут быть сохранены на сервере 802 сообщений, в базе 810 данных или в любом другом компоненте системы 800 по необходимости. После того, как определено, какие намеченные получатели также являются борцами с несанкционированной рассылкой, сообщение(я) выбирается для опроса и копия сообщения(й) для опроса, а также любая другая информация, касающаяся почтовой транзакции, может быть отправлена в базу 810 данных.

Сообщения, выбранные для опроса, модифицируются модификатором 830 сообщений любым числом способов, описанных выше. На практике, уникальный идентификатор (ID) может быть назначен каждому сообщению для опроса, каждому борцу с несанкционированной рассылкой и/или каждому результату опроса и сохранен в базе 810 данных. Как упоминалось ранее, сообщения, выбранные для опроса, могут быть случайно выбраны или могут быть специальными для соответствующего пользователя(ей) (820, 822 и 824). Например, ПОЛЬЗОВАТЕЛЬ1 820 может указать, что только определенные типы сообщений доступны для опроса (к примеру, сообщения, отправленные из-за пределов компании). Данные, сгенерированные из этих специальных сообщений, перевзвешиваются и/или пропускаются, чтобы уменьшить получение необъективной выборки данных.

Сканирование на вирусы сообщений для опроса также может быть выполнено в это время или в любое другое время до того, как сообщение для опроса будет загружено и/или открыто пользователем. После того, как сообщения были модифицированы надлежащим образом, они доставляются в папки входящих сообщений соответствующих пользователей, которые обозначены как INBOX1 828, INBOX2 832 и INBOXN 834, где они могут быть открыты для опроса. Чтобы обеспечить процесс опроса, каждое сообщение для

опроса включает в себя две или более кнопки или ссылки для голосования, которые, будучи выбраны пользователем, генерируют информацию, относящуюся к сообщению для опроса и результату опроса. Текст каждого сообщения для опроса может быть модифицирован, чтобы включить в себя кнопки или ссылки для голосования.

Результаты опроса по сообщениям (обозначенные как MESSAGE POLL1 836, MESSAGE POLL2 838 и MESSAGE POLLN 840), которые включают в себя любую информацию, следующую из классификации (к примеру, сообщение для опроса или ассоциированный с ним идентификатор, свойства пользователя), отправляются в базу 810 данных посредством сетевого интерфейса 842, размещенную в LAN 815. База 810 данных сохраняет информацию об опросе и пользователях от соответствующих пользователей для дальнейшего использования в методиках обучения машины, которые используются, чтобы создавать и/или оптимизировать новые и/или усовершенствованные фильтры 912, 808 несанкционированной рассылки.

По соображениям конфиденциальности каждая компания может захотеть вычистить ключевую информацию перед отправкой опрошенного сообщения и/или информации о пользователе в собственную базу 810 данных и/или базу 806 данных электронной почты, к примеру, по GCN 814. Один подход - предоставлять обратную связь только в базу данных (806 и/или 810) по сообщениям несанкционированной рассылки, тем самым, исключая обратную связь по легитимной почте. Другой подход - предоставлять только частичный поднабор информации по легитимной почте, такой как отправитель и IP-адрес отправителя. Другой подход - для выбранных сообщений, например помеченных как полезные пользователем, которые будут помечены как вредные фильтром, или наоборот, явно запросить разрешение пользователя перед отправкой их фильтру. Любой из этих подходов или их сочетание облегчает поддержание секретности конфиденциальной информации для участвующих клиентов, одновременно непрерывно предоставляя данные, чтобы обучать фильтр(ы) несанкционированной рассылки (808 и/или 812).

Схемы проверки достоверности пользователей, такие как описанные выше, также могут быть применены для каждой компании, а также для каждого пользователя в компании. Например, пользователи могут быть отдельно методикам перекрестной проверки достоверности, при этом классификации вызывающего подозрение пользователя(ей) исключаются из обучения фильтра. Фильтр обучается с помощью данных от оставшегося пользователя(ей). Обученный фильтр затем работает в отношении сообщений от исключенного пользователя(ей), чтобы определить, как он бы классифицировал сообщения. Если число несовпадений превышает пороговый уровень, то вызывающий подозрение пользователь(и) считается недоверенным. Дальнейшие классификации сообщений от недоверенного пользователя(ей) могут быть проверены вручную до того, как они будут приняты базой данных и/или фильтром. В противном случае, пользователь(и) может быть удален из будущего опроса.

Согласно к фиг.9, типичная среда 910 для реализации различных аспектов изобретения включает в себя компьютер 912. Компьютер 912 включает в себя модуль 914 обработки данных, системную память 916 и системную шину 918. Системная шина 918 соединяет компоненты системы, в том числе (но не только) системную память 916, с модулем 914 обработки данных. Модуль 914 обработки данных может быть любым из различных доступных процессоров. Архитектуры с двумя микропроцессорами и другие многопроцессорные архитектуры также могут быть использованы в качестве модуля обработки данных 914.

Системная шина 918 может относиться к любому из нескольких типов структур(ы) шин, включая шину памяти или контроллер памяти, периферийную шину или внешнюю шину и/или локальную шину, используя любую из множества архитектур шин, в том числе (но не только) 11-битную шину, шину промышленного стандарта (ISA), шину микроканальной архитектуры (MCA), расширенную шину ISA (EISA), встроенный интерфейс накопителей (IDE), локальную шину Ассоциации по стандартам в области видеоэлектроники (VLB), шину межсоединения периферийных компонентов (PCI), универсальную последовательную шину

(USB), ускоренный графический порт (AGP), шину Международной ассоциации производителей плат памяти для персональных вычислительных машин (PCMCIA) и шину интерфейса малых вычислительных систем (SCSI).

Системная память 916 включает в себя энергозависимую память 920 и энергонезависимую память 922. Базовая система ввода-вывода (BIOS), содержащая основные процедуры, чтобы передавать информацию между элементами в вычислительной машине 912, например при загрузке, хранится в энергонезависимой памяти 922. В качестве иллюстрации, но не ограничения, энергонезависимая память 922 может включать в себя постоянное запоминающее устройство (ПЗУ), программируемое ПЗУ (ППЗУ), электрически программируемое ПЗУ (ЭППЗУ), электрически стираемое программируемое ПЗУ (ЭСППЗУ) или флэш-память. Энергозависимая память 920 включает в себя оперативную память (ОЗУ), которая действует как внешний кэш. В качестве иллюстрации, но не ограничения, ОЗУ доступно во многих формах, например синхронное ОЗУ (SRAM), динамическое ОЗУ (DRAM), синхронное DRAM (SDRAM), SDRAM с двойной скоростью передачи данных (DDR SDRAM), улучшенное SDRAM (ESDRAM), Synchlink DRAM (SLDRAM) и direct Rambus RAM (DRRAM).

Компьютер 912 также включает в себя съемные/несъемные, энергозависимые/энергонезависимые носители данных компьютера. Фиг.9 иллюстрирует, например, дисковое запоминающее устройство 924. Дисковое запоминающее устройство 924 включает в себя (но не только) такие устройства, как дисковод для магнитных дисков, дисковод для гибких дисков, ленточный накопитель, дисковод Jaz, дисковод Zip, дисковод LS-100, карту флэш-памяти или карту Memory Stick. Помимо этого, дисковое запоминающее устройство 924 может включать в себя носители данных независимо или в сочетании с другими носителями данных, включая (но не только) оптический дисковод, например, устройство чтения ПЗУ на компакт-диске (CD-ROM), дисковод для записываемых CD (CD-R), дисковод для перезаписываемых CD (CD-RW) или дисковод для ПЗУ на универсальном цифровом диске (DVD-ROM). Чтобы обеспечить подключение дисковых запоминающих устройств 924 к системной шине 918, в типичном случае используется интерфейс съемной или несъемной памяти, например интерфейс 926.

Необходимо принимать во внимание, что фиг.9 описывает программное обеспечение, которое выступает в качестве посредника между пользователями и базовыми ресурсами вычислительной машины, описанными в подходящей рабочей среде 910. Такое программное обеспечение включает в себя операционную систему 928. Операционная система 928, которая может быть сохранена на дисковом запоминающем устройстве 924, служит для того, чтобы контролировать и распределять ресурсы системы компьютера 912. Системные приложения 930 используют преимущества управления ресурсами операционной системой 928 посредством программных модулей 932 и программных данных 934, сохраненных либо в системной памяти 916, либо на дисковом запоминающем устройстве 924. Необходимо принимать во внимание, что настоящее изобретение может быть реализовано с различными операционными системами или сочетаниями операционных систем.

Пользователь вводит команды или информацию в вычислительную машину 912 посредством устройств(а) 936 ввода. Устройства 936 ввода включают в себя (но не только) координатно-указательное устройство, такое как мышь, шаровой манипулятор, перо, сенсорную панель, клавиатуру, микрофон, джойстик, игровую панель, спутниковую антенну, сканер, плату ТВ-тюнера, цифровую камеру, цифровую видеокамеру, Web-камеру и т.п. Эти и другие устройства ввода подключаются к процессору 914 через системную шину 918 посредством интерфейсного порта(ов) 938. Интерфейсные порты 938 включают в себя, например последовательный порт, параллельный порт, игровой порт и универсальную последовательную шину (USB). Устройство(а) 940 вывода использует те же типы портов, что и устройство(а) 936 ввода. Таким образом, например порт USB может быть использован, чтобы обеспечить ввод в вычислительную машину 912 и чтобы выводить информацию из вычислительной машины 912 на устройство 940 вывода. Адаптер

942 вывода предоставлен, чтобы проиллюстрировать, что существуют некоторые устройства 940 вывода, такие как мониторы, динамики и принтеры среди прочих устройств 940 вывода, которые требуют специальных адаптеров. Адаптеры 942 вывода включают в себя, в качестве иллюстрации, но не ограничения, видео- и звуковые платы, которые обеспечивают средство соединения между устройством 940 вывода и системной шиной 918. Следует заметить, что другие устройства и/или системы устройств предоставляют возможности как ввода, так и вывода, такие как удаленный компьютер(ы) 944.

Компьютер 912 может работать в сетевой среде, используя логические соединения с одной или более удаленными компьютерами, например удаленным компьютером(ами) 944. Удаленным компьютером(ами) 944 может быть персональный компьютер (ПК), сервер, маршрутизатор, сетевой ПК, рабочая станция, устройство на базе микропроцессора, одноранговое устройство или другой стандартный сетевой узел и т.п., и в типичном случае включает в себя большинство или все из элементов, описанных относительно компьютера 912. В целях краткости, только запоминающее устройство 946 проиллюстрировано с удаленным компьютером(ами) 944. Удаленные компьютеры 944 логически соединены с вычислительной машиной 912 посредством сетевого интерфейса 948 и затем физически соединены через коммуникационное соединение 950. Сетевой интерфейс 948 охватывает коммуникационные сети, такие как локальные сети (LAN) и глобальные сети (WAN). Технологии LAN включают в себя распределенный интерфейс передачи данных по волоконно-оптическим каналам (FDDI), распределенный проводной интерфейс передачи данных (CDDI), Ethernet/IEEE 1102.3, Token Ring/IEEE 1102.5 и т.п. Технологии WAN включают в себя, но не только, двухточечные каналы связи, сети с коммутацией каналов, такие как цифровые сети с комплексными услугами (ISDN) и их разновидности, сети с коммутацией пакетов и цифровые абонентские линии (DSL).

Коммуникационное соединение(я) 950 относится к аппаратным средствам/программному обеспечению, используемым, чтобы подсоединить сетевой интерфейс 948 к шине 918. Хотя коммуникационное соединение 950 показано в целях иллюстративной ясности внутри компьютера 912, оно также может быть внешним по отношению к компьютеру 912. Аппаратные средства/программное обеспечение, необходимые для подсоединения к сетевому интерфейсу 948, включают в себя, исключительно в целях иллюстрации, внутренние и внешние технологии, например, модемы, в том числе модемы на регулярных телефонных линиях, кабельные модемы и DSL-модемы, ISDN-адаптеры и платы Ethernet.

Фиг.10 - это блок-схема примера вычислительной среды 1000, с которой может взаимодействовать настоящее изобретение. Система 1000 включает в себя один или более клиентов 1010. Клиентом(ами) 1010 могут быть аппаратные средства и/или программное обеспечение (к примеру, потоки, процессы, вычислительные устройства). Система 1000 также включает в себя один или более серверов 1030. Сервером(ами) 1030 также могут быть аппаратные средства и/или программное обеспечение (к примеру, потоки, процессы, вычислительные устройства). Серверы 1030 могут вмещать потоки, чтобы выполнять преобразования, например посредством использования настоящего изобретения. Один возможный обмен данными между клиентом 1010 и сервером 1030 может быть в форме пакета данных, адаптированного к передаче между двумя или более процессами компьютера. Система 1000 включает в себя коммуникационную инфраструктуру 1050, которая может быть использована, чтобы обеспечивать обмен данными между клиентом(ами) 1010 и сервером(ами) 1030. Клиент(ы) 1010 в рабочем состоянии подсоединен к одному или более хранилищам 1060 данных клиента, которые могут быть использованы, чтобы сохранять информацию локально на клиенте(ах) 1010. Так же, сервер(ы) 1030 в рабочем состоянии подсоединены к одному или более хранилищам 1040 данных сервера, которые могут быть использованы, чтобы сохранять информацию локально на серверах 1030.

То, что было описано выше, включает в себя примеры настоящего изобретения. Конечно, невозможно описать каждое вероятное сочетание компонентов или методик в целях описания настоящего изобретения, но обычный специалист в данной области

техники может признать, что многие дополнительные сочетания и перестановки настоящего изобретения допустимы. Следовательно, настоящее изобретение предназначено, чтобы охватывать все подобные преобразования, модификации и разновидности, которые попадают под объем, определяемый прилагаемой формулой изобретения. Более того, в той степени, как термин "включает в себя" используется либо в подробном описании, либо в формуле, этот термин должен быть включающим аналогично термину "содержит", как "содержит" интерпретируется, при использовании в качестве промежуточного слова в пункте формулы изобретения.

Формула изобретения

1. Система, которая обеспечивает выполнение классификации элементов в связи с предотвращением несанкционированной рассылки, причем система включает в себя:

компонент, который принимает набор элементов;

компонент, который идентифицирует намеченных получателей элементов и помечает поднабор элементов, по которым должен быть проведен опрос, при этом поднабор элементов соответствует поднабору получателей, которые являются известными пользователями, борющимися с несанкционированной рассылкой; и

компонент обратной связи, который принимает информацию, относящуюся к выполненной борцом с несанкционированной рассылкой классификации элементов по которым проведен опрос, и использует эту информацию в связи с обучением фильтра несанкционированной рассылки и заполнением списка несанкционированной рассылки.

2. Система по п.1, в которой элементы содержат, по меньшей мере, одно из электронной почты и сообщений.

3. Система по п.1, в которой компонентом, который принимает набор элементов, является одно из сервера электронной почты, сервера сообщений и клиентского программного обеспечения электронной почты.

4. Система по п.1, в которой поднабор элементов, по которым должен быть выполнен опрос, содержит все из принятых элементов.

5. Система по п.1, в которой поднабор получателей содержит всех получателей.

6. Система по п.1, в которой поднабор получателей выбирается случайно.

7. Система по п.1, в которой поднабор элементов, помеченных для опроса, ограничен, по меньшей мере, одним из следующего:

числом элементов, выбранных на каждого пользователя;

числом элементов, выбранных на каждого пользователя и на каждый период времени; и

вероятностью помечания элемента, соответствующего известному пользователю.

8. Система по п.1, в которой каждому из помеченных элементов назначается уникальный идентификатор, который соответствует любому одному из помеченного элемента и содержимого помеченного элемента.

9. Система по п.1, дополнительно содержащая компонент, который модифицирует элемент, помеченный для опроса, чтобы идентифицировать его как элемент для опроса.

10. Система по п.9, в которой модифицированный элемент содержит сводку по помеченному элементу, сводку, содержащую, по меньшей мере, одно из темы, даты, текста сообщения и первых нескольких строк текста.

11. Система по п.9, в которой модифицированный элемент содержит инструкции по голосованию и что-либо одно из, по меньшей мере, двух кнопок и ссылок для голосования, которые соответствуют, по меньшей мере, двум соответствующим классам элементов, чтобы обеспечить выполнение классификации элемента пользователем.

12. Система по п.1, дополнительно содержащая центральную базу данных, которая сохраняет информацию и данные, относящиеся к свойствам пользователя, содержимому элемента и свойствам, ассоциированным с помеченными элементами, выполненной пользователями классификации и статистическим данным о голосовании, данным анализа частоты опроса на каждого пользователя и опроса на каждого пользователя и на каждый период времени, списки несанкционированной рассылки, списки легитимной почты и списки

черных дыр.

13. Система по п.1, распределенная по более чем одной компании, борющейся с несанкционированной рассылкой, так, чтобы информация обратной связи от каждой компании отправлялась в центральную базу данных, при работе взаимодействующую с каждой компанией, при этом некоторая часть информации обратной связи удаляется по соображениям конфиденциальности.

14. Система по п.1, дополнительно содержащая компонент проверки достоверности выполненных пользователями классификаций, который тестирует надежность пользователей и степень доверия пользователям.

15. Система по п.14, в которой компонент проверки достоверности выполненных пользователями классификаций может быть применен к одному или более вызывающим подозрение пользователям.

16. Система по п.1, в которой компонент обратной связи принимает информацию, относящуюся к обратной связи от пользователей, обратной связи от электронных приманок и, в необязательном порядке, обратной связи от пользователя-получателя по принятым элементам.

17. Способ обеспечения классификации элементов в связи с предотвращением несанкционированной рассылки, содержащий этапы, на которых

принимают набор сообщений;

идентифицируют намеченных получателей сообщений;

помечают поднабор сообщений, по которым должен быть проведен опрос, при этом поднабор сообщений соответствует поднабору получателей, которые являются известными пользователями, борющимися с несанкционированной рассылкой;

принимают информацию, относящуюся к выполненной пользователем классификации сообщений для опроса; и

используют эту информацию в связи с обучением фильтра несанкционированной рассылки и заполняют список несанкционированной рассылки.

18. Способ по п.17, в котором поднабор получателей, которые являются известными пользователями, борющимися с несанкционированной рассылкой, определяется каждым получателем, выполняющим, по меньшей мере, один из следующих этапов, на которых

делают выбор предоставлять обратную связь по сообщениям, чтобы обеспечить обучение нового фильтра несанкционированной рассылки;

пассивно делают выбор предоставлять обратную связь по сообщениям посредством не отказа от участия;

оплачивают услуги электронной почты и сообщений, предоставленные принимающим участие сервером сообщений; и

открывают учетную запись электронной почты с помощью принимающего участие сервера сообщений.

19. Способ по п.17, в котором поднабор сообщений, помеченных для опроса, ограничен одним или более ограничениями опроса.

20. Способ по п.17, дополнительно содержащий этап, на котором модифицируют помеченные сообщения, чтобы отметить и идентифицировать их как сообщения для опроса.

21. Способ по п.20, в которой модифицирование помеченных сообщений содержит этапы, на которых выполняют, по меньшей мере, одно из следующего:

перемещают помеченное сообщение в отдельную папку для сообщений для опроса;

модифицируют адрес "От кого" помеченного сообщения;

модифицируют строку темы помеченного сообщения;

используют значок опроса на помеченном сообщении, чтобы идентифицировать его как сообщение для опроса; и

используют уникальный цвет, чтобы идентифицировать помеченное сообщение как сообщение для опроса.

22. Способ по п.17, дополнительно содержащий этапы, на которых сканируют

помеченные сообщения на вирусы перед тем, как они будут загружены для опроса.

23. Способ по п.17, дополнительно содержащий этапы, на которых делают копию каждого помеченного сообщения, как оно изначально принято, так, чтобы соответствующие пользователи принимали первую копию сообщения в его исходной форме и вторую копию сообщения в форме для опроса.

24. Способ по п.17, дополнительно содержащий этапы, на которых распространяют обученный фильтр несанкционированной рассылки на один или более серверов, причем распространение осуществляется автоматически и/или по запросу посредством, по меньшей мере, одного из сообщения электронной почты и размещения на Web-сайте для загрузки.

25. Способ по п.17, в котором обучение фильтра несанкционированной рассылки и заполнение списка несанкционированной рассылки выполняется посредством методик машинного обучения с помощью данных, основанных на обратной связи в форме выполненных пользователями классификаций и, в необязательном порядке, данных, сгенерированных одним или более дополнительными источниками, содержащими электронные приманки, обратную связь в форме классификации, выполненных не являющимися пользователями получателями, и методик активного обучения.

26. Способ по п.25, в котором данные, сгенерированные одним или более источниками, перевзвешиваются пропорционально по отношению к типу данных, сгенерированных источником, и относительно данных выполненной пользователями классификации, чтобы обеспечить получение объективной выборки данных.

27. Способ по п.17, дополнительно содержащий этапы, на которых

отслеживают входящие сообщения на предмет их соответствующих одного или более позитивных признаков;

определяют частоту принятых позитивных признаков;

определяют, превышает ли один или более позитивных признаков пороговую частоту, на основе, по меньшей мере, частично данных предыстории; и

помещают на карантин вызывающие подозрение сообщения, которые соответствуют упомянутым одному или более позитивным признакам, которые превышают пороговую частоту, до тех пор пока дополнительные данные классификации не станут доступными, чтобы определить, являются ли вызывающие подозрение сообщения несанкционированной рассылкой.

28. Способ по п.27, в котором используемый признак является информацией об отправителе, содержащей, по меньшей мере, одно из IP-адреса и домена отправителя.

29. Способ по п.27, в котором помещение на карантин вызывающих подозрение сообщений содержит этапы, на которых выполняют, по меньшей мере, одно из следующего:

временно помечают вызывающие подозрение сообщения как несанкционированную рассылку и перемещают их в папку несанкционированной рассылки;

задерживают доставку вызывающих подозрение сообщений пользователю(ям) до тех пор, пока дополнительные данные классификации не станут доступными; и

сохраняют вызывающие подозрение сообщения в папке, не видимой для пользователя(ей).

30. Способ по п.17, дополнительно содержащий этапы, на которых определяют частоту ошибочных положительных результатов и поимок, чтобы обеспечить оптимизацию фильтра несанкционированной рассылки, при этом определение частоты ошибочных положительных результатов и поимок содержит этапы, на которых

обучают фильтр несанкционированной рассылки с помощью набора обучающих данных, причем набор обучающих данных содержит первый набор результатов опроса;

классифицируют второй набор сообщений для опроса с помощью обратной связи от пользователей, чтобы получить второй набор результатов опроса;

прогоняют второй набор сообщений для опроса через обученный фильтр несанкционированной рассылки;

сравнивают второй набор результатов опроса с результатами обученного фильтра несанкционированной рассылки, чтобы определить частоту ошибочных положительных результатов и поимок фильтра и тем самым оценить и настроить параметры фильтра согласно оптимальным рабочим характеристикам фильтра.

31. Способ по п.30, в котором создают более чем один фильтр несанкционированной рассылки, при этом каждый фильтр имеет отличающиеся от других параметры и обучается на одном и том же наборе обучающих данных так, чтобы частоты ошибочных положительных результатов и поимок сравнивались с, по меньшей мере, одним другим фильтром несанкционированной рассылки, чтобы определить оптимальные параметры фильтрации несанкционированной рассылки.

32. Способ по п.17, дополнительно содержащий этапы, на которых создают усовершенствованный фильтр несанкционированной рассылки с помощью дополнительных наборов входящих сообщений, поднаборы которых подвергаются опросу, чтобы получить новую информацию в связи с обучением усовершенствованного фильтра несанкционированной рассылки, при этом ранее полученная информация перевзвешивается на основе, по меньшей мере, частично того, как давно она была получена.

33. Способ по п.17, дополнительно содержащий этап, на котором используют информацию, чтобы создать список легитимных отправителей.

34. Способ по п.17, дополнительно содержащий этап, на котором используют информацию, чтобы обеспечить прекращение действия учетных записей распространителей несанкционированной рассылки.

35. Способ по п.34, дополнительно содержащий этапы, на которых идентифицируют распространителя несанкционированной рассылки, который использует поставщика Интернет-услуг (ISP), и автоматически уведомляют ISP о распространении несанкционированной рассылки.

36. Способ по п.34, дополнительно содержащий этапы, на которых определяют домен, несущий ответственность за отправку несанкционированной рассылки, и автоматически уведомляют, по меньшей мере, одного поставщика услуг электронной почты домена и ISP домена о распространении несанкционированной рассылки.

37. Способ по п.17, дополнительно содержащий этапы, на которых распространяют, по меньшей мере, одно из фильтра несанкционированной рассылки и списка несанкционированной рассылки на любое одно из почтовых серверов, серверов электронной почты и клиентского программного обеспечения электронной почты, при этом распространение содержит, по меньшей мере, один из следующих этапов, на которых:

помещают уведомление на Web-сайте, уведомляющее о том, что фильтр несанкционированной рассылки и список несанкционированной рассылки доступны для загрузки;

автоматически выдают фильтр несанкционированной рассылки и список несанкционированной рассылки на почтовые серверы, серверы электронной почты и клиентское почтовое программное обеспечение электронной почты; и

вручную выдают фильтр несанкционированной рассылки и список несанкционированной рассылки на почтовые серверы, серверы электронной почты и клиентское программное обеспечение электронной почты.

38. Способ перекрестной проверки, который обеспечивает проверку надежности выполненных пользователями классификаций и степени доверия выполненным пользователями классификациям, при этом способ содержит этапы, на которых

исключают классификации, выполненные одним или более вызывающими подозрение пользователями, из данных, используемых, чтобы обучать фильтр несанкционированной рассылки;

обучают фильтр несанкционированной рассылки с помощью всех других доступных выполненных пользователями классификаций; и

пропускают сообщения для опроса вызывающих подозрения пользователей через

обученный фильтр несанкционированной рассылки, чтобы определить, как бы он классифицировал сообщения по сравнению с классификациями, выполненными вызывающими подозрения пользователями.

39. Способ по п.38, дополнительно содержащий выполнение, по меньшей мере, одного из следующих этапов, на которых:

не учитывают имеющиеся и будущие классификации, предоставленные пользователями, которые определены как недоверенные, до тех пор пока не будет определено, что эти пользователи являются доверенными;

отбрасывают имеющиеся классификации, предоставленные пользователями, определенными как недоверенные; и

удаляют недоверенных пользователей из будущего опроса.

40. Способ обеспечения проверки надежности выполненных пользователями классификаций и степени доверия выполненным пользователями классификациям для обучения фильтра несанкционированной рассылки посредством системы контура обратной связи, при этом способ содержит этапы, на которых

идентифицируют поднабор пользователей, борющихся с несанкционированной рассылкой, в качестве вызывающих подозрение пользователей;

представляют одно или более сообщений, имеющих известный результат, вызывающим подозрение пользователям для опроса; и

определяют, соответствует ли выполненная вызывающими подозрение пользователями классификация одного или более тестовых сообщений известной классификации, чтобы удостовериться в надежности выполненных пользователями классификаций.

41. Способ по п.40, в котором поднабор пользователей, борющихся с несанкционированной рассылкой, идентифицированных в качестве вызывающих подозрение пользователей, содержит всех пользователей.

42. Способ по п.40, в котором сообщением является тестовое сообщение, про которое известно, что оно является, по меньшей мере, одним из несанкционированной рассылки и полезной почты, и которое добавляется в поток входящей почты системой контура обратной связи и доставляется вызывающим подозрение пользователям.

43. Способ по п.40, в котором сообщение, принятое вызывающими подозрение пользователями для опроса, классифицируется вручную системным администратором, чтобы обучить фильтр несанкционированной рассылки с помощью корректной классификации, чтобы идентифицировать недоверенных пользователей.

44. Способ по п.40, дополнительно содержащий, по меньшей мере, один из следующих этапов, на которых

не учитывают имеющиеся и будущие классификации, предоставленные пользователями, которые определены как недоверенные, до тех пор пока не будет определено, что эти пользователи являются доверенными;

отбрасывают имеющиеся классификации, предоставленные пользователями, определенными как недоверенные; и

удаляют недоверенных пользователей из будущего голосования.

45. Система, которая обеспечивает выполнение классификации сообщений в связи с предотвращением несанкционированной рассылки, при этом система содержит

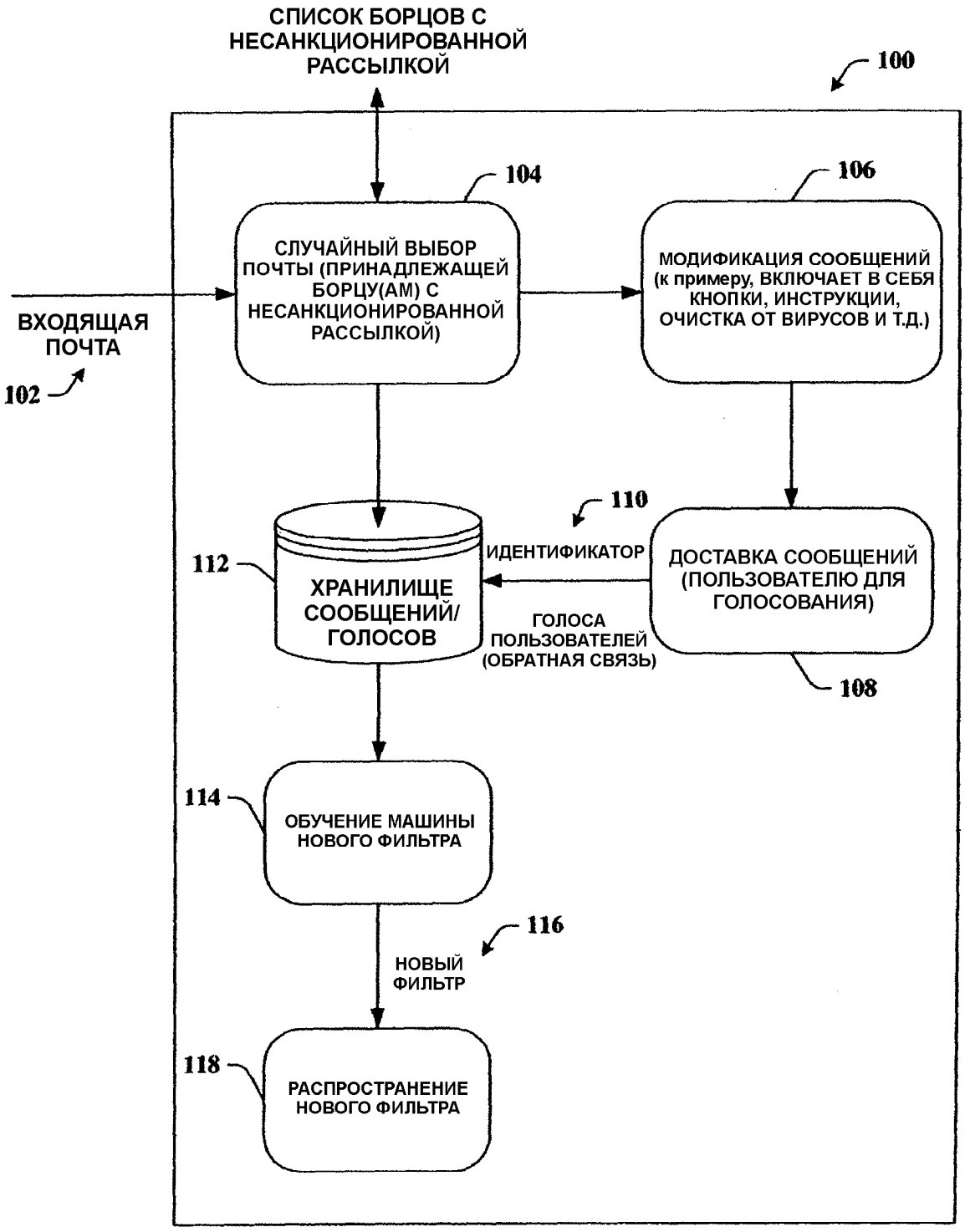
средство для приема набора сообщений;

средство для идентификации намеченных получателей сообщений;

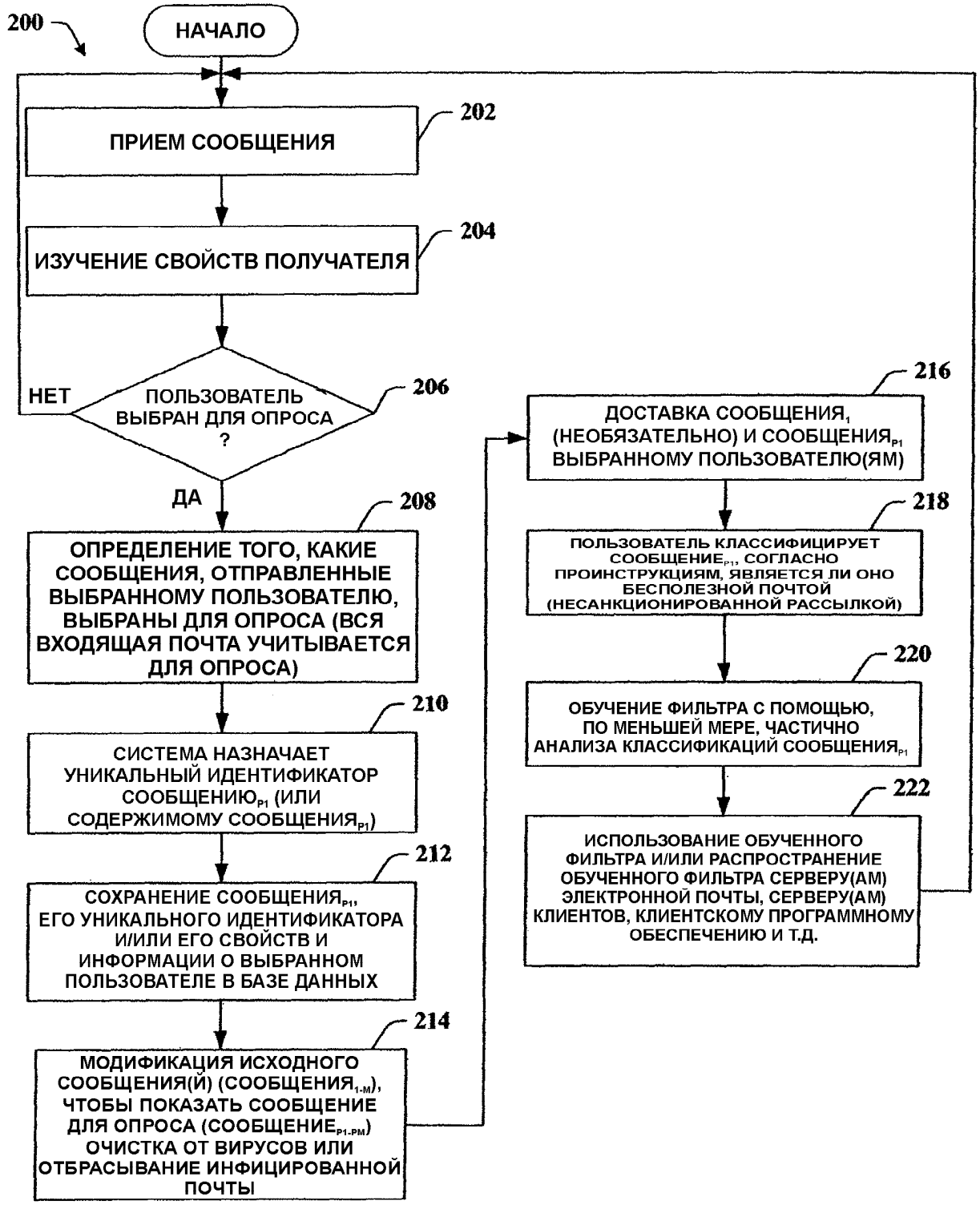
средство для помечания поднабора сообщений, по которым должен быть проведен опрос, при этом поднабор сообщений соответствует поднабору получателей, которые являются известными пользователями, борющимися с несанкционированной рассылкой;

средство для приема информации, относящейся к выполненной пользователем классификации сообщений для опроса; и

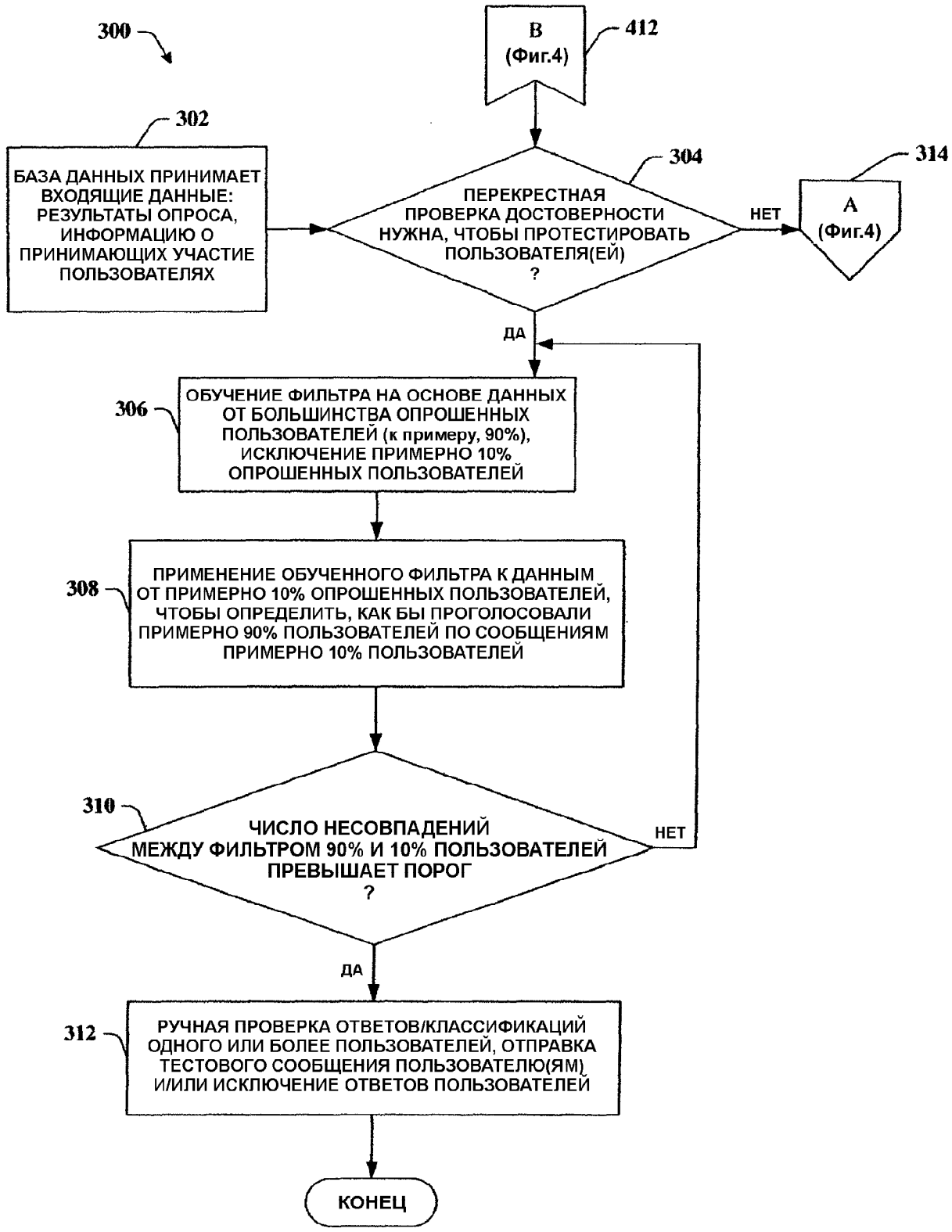
средство для использования этой информации в связи с обучением фильтра несанкционированной рассылки и заполнения списка несанкционированной рассылки.


СПИСОК БОРЦОВ С НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКОЙ
100
104
106
СЛУЧАЙНЫЙ ВЫБОР ПОЧТЫ (ПРИНАДЛЕЖАЩЕЙ БОРЦУ(АМ) С НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКОЙ)
МОДИФИКАЦИЯ СООБЩЕНИЙ (к примеру, ВКЛЮЧАЕТ В СЕБЯ КНОПКИ, ИНСТРУКЦИИ, ОЧИСТКА ОТ ВИРУСОВ И Т.Д.)
ВХОДЯЩАЯ ПОЧТА
102
110
112
ИДЕНТИФИКАТОР
ДОСТАВКА СООБЩЕНИЙ (ПОЛЬЗОВАТЕЛЮ ДЛЯ ГОЛОСОВАНИЯ)
ХРАНИЛИЩЕ СООБЩЕНИЙ/ ГОЛОСОВ
ГОЛОСА ПОЛЬЗОВАТЕЛЕЙ (ОБРАТНАЯ СВЯЗЬ)
108
114
ОБУЧЕНИЕ МАШИНЫ НОВОГО ФИЛЬТРА
116
НОВЫЙ ФИЛЬТР
118
РАСПРОСТРАНЕНИЕ НОВОГО ФИЛЬТРА

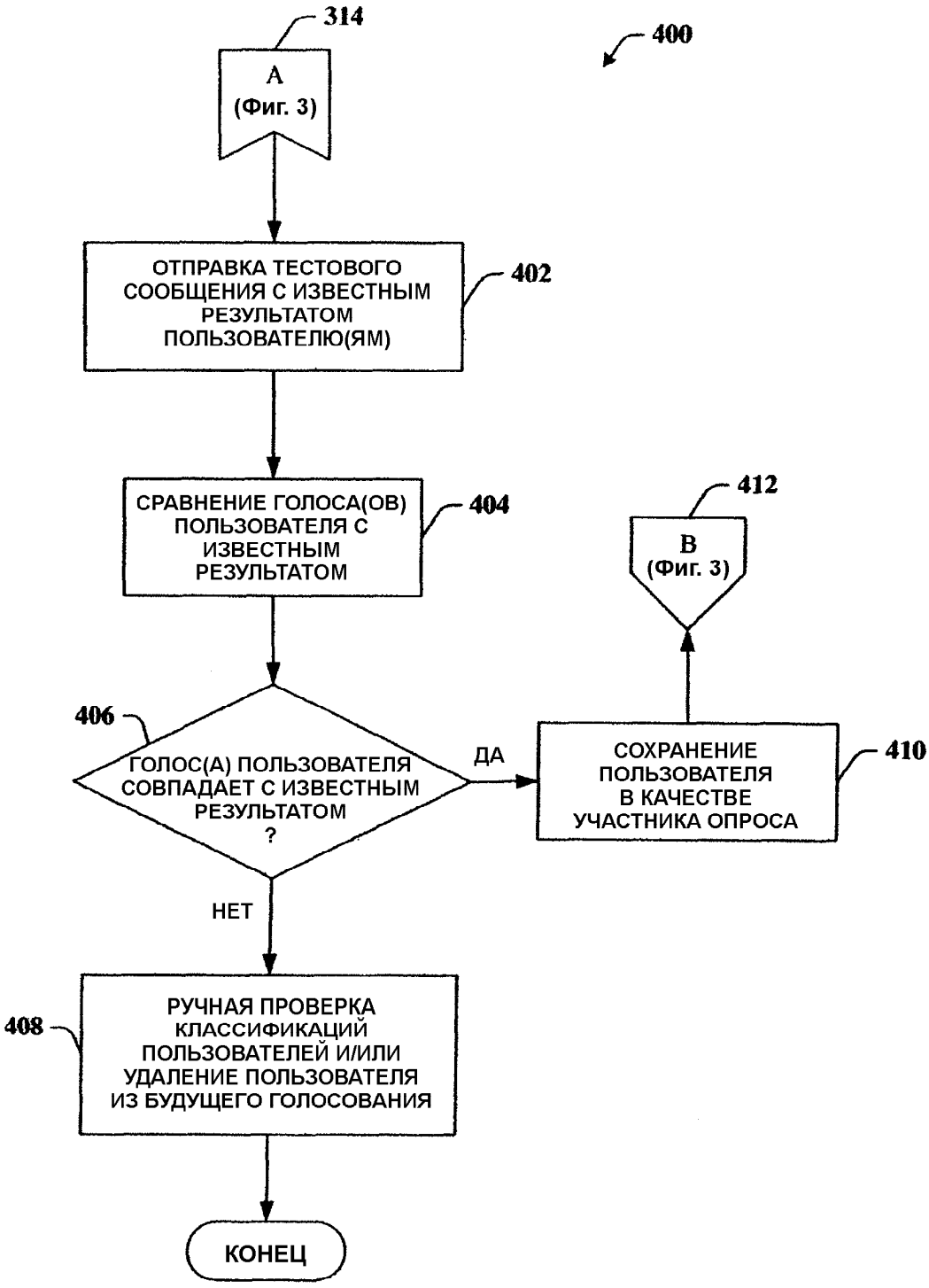
Фиг. 1B


200
НАЧАЛО
ПРИЕМ СООБЩЕНИЯ
202
ИЗУЧЕНИЕ СВОЙСТВ ПОЛУЧАТЕЛЯ
204
НЕТ
ПОЛЬЗОВАТЕЛЬ ВЫБРАН ДЛЯ ОПРОСА ?
206
ДА
ОПРЕДЕЛЕНИЕ ТОГО, КАКИЕ СООБЩЕНИЯ, ОТПРАВЛЕННЫЕ ВЫБРАННОМУ ПОЛЬЗОВАТЕЛЮ, ВЫБРАНЫ ДЛЯ ОПРОСА (ВСЯ ВХОДЯЩАЯ ПОЧТА УЧИТЫВАЕТСЯ ДЛЯ ОПРОСА)
208
СИСТЕМА НАЗНАЧАЕТ УНИКАЛЬНЫЙ ИДЕНТИФИКАТОР СООБЩЕНИЮ$_{P1}$ (ИЛИ СОДЕРЖИМОМУ СООБЩЕНИЯ$_{P1}$)
210
СОХРАНЕНИЕ СООБЩЕНИЯ$_{P1}$, ЕГО УНИКАЛЬНОГО ИДЕНТИФИКАТОРА И/ИЛИ ЕГО СВОЙСТВ И ИНФОРМАЦИИ О ВЫБРАННОМ ПОЛЬЗОВАТЕЛЕ В БАЗЕ ДАННЫХ
212
МОДИФИКАЦИЯ ИСХОДНОГО СООБЩЕНИЯ(Й) (СООБЩЕНИЯ$_{1-M}$), ЧТОБЫ ПОКАЗАТЬ СООБЩЕНИЕ ДЛЯ ОПРОСА (СООБЩЕНИЕ$_{P1-PM}$) ОЧИСТКА ОТ ВИРУСОВ ИЛИ ОТБРАСЫВАНИЕ ИНФИЦИРОВАННОЙ ПОЧТЫ
214
ДОСТАВКА СООБЩЕНИЯ$_1$ (НЕОБЯЗАТЕЛЬНО) И СООБЩЕНИЯ$_{P1}$ ВЫБРАННОМУ ПОЛЬЗОВАТЕЛЮ(ЯМ)
216
ПОЛЬЗОВАТЕЛЬ КЛАССИФИЦИРУЕТ СООБЩЕНИЕ$_{P1}$, СОГЛАСНО ПРОИНСТРУКЦИЯМ, ЯВЛЯЕТСЯ ЛИ ОНО БЕСПОЛЕЗНОЙ ПОЧТОЙ (НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКОЙ)
218
ОБУЧЕНИЕ ФИЛЬТРА С ПОМОЩЬЮ, ПО МЕНЬШЕЙ МЕРЕ, ЧАСТИЧНО АНАЛИЗА КЛАССИФИКАЦИЙ СООБЩЕНИЯ$_{P1}$
220
ИСПОЛЬЗОВАНИЕ ОБУЧЕННОГО ФИЛЬТРА И/ИЛИ РАСПРОСТРАНЕНИЕ ОБУЧЕННОГО ФИЛЬТРА СЕРВЕРУ(АМ) ЭЛЕКТРОННОЙ ПОЧТЫ, СЕРВЕРУ(АМ) КЛИЕНТОВ, КЛИЕНТСКОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ И Т.Д.
222

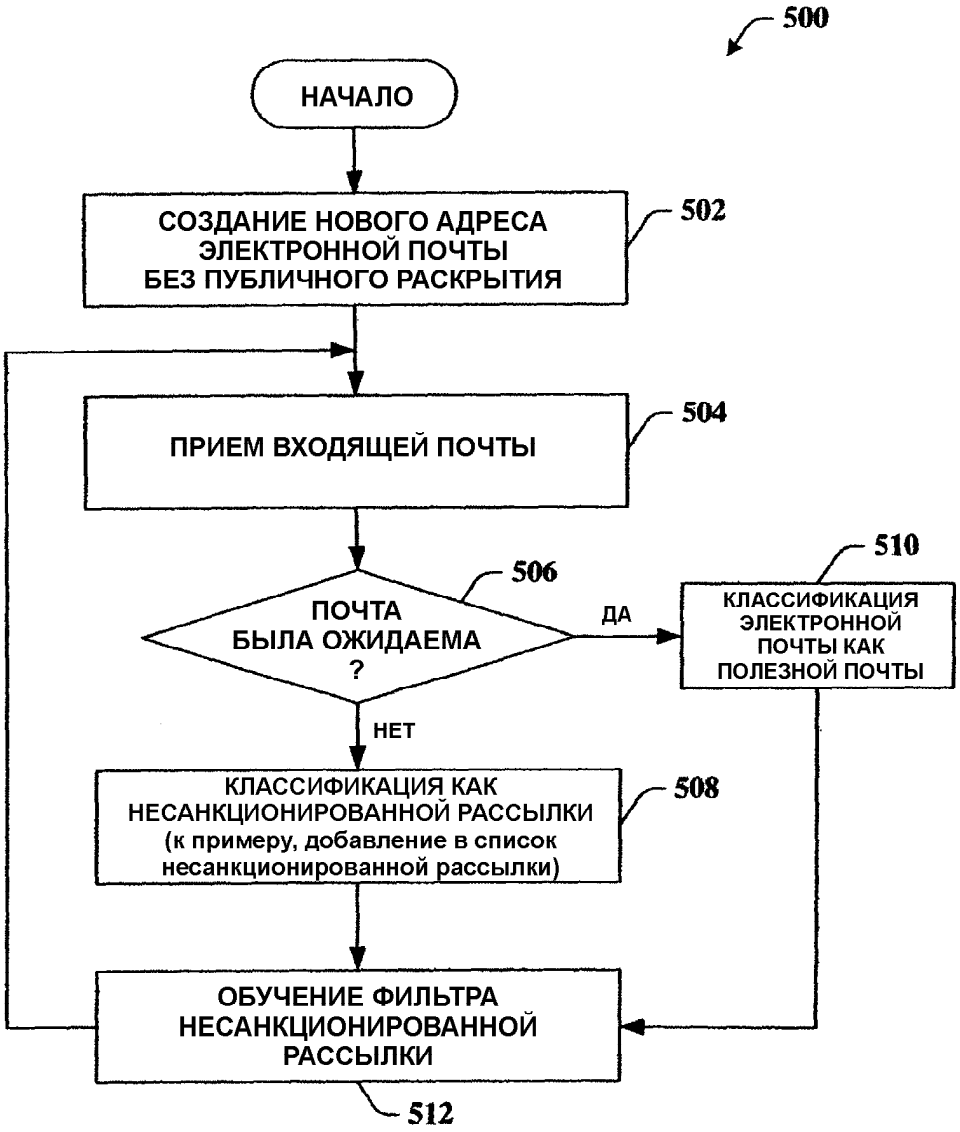
Фиг. 2


300
B
(Фиг.4)
412
302
БАЗА ДАННЫХ ПРИНИМАЕТ ВХОДЯЩИЕ ДАННЫЕ: РЕЗУЛЬТАТЫ ОПРОСА, ИНФОРМАЦИЮ О ПРИНИМАЮЩИХ УЧАСТИЕ ПОЛЬЗОВАТЕЛЯХ
304
ПЕРЕКРЕСТНАЯ ПРОВЕРКА ДОСТОВЕРНОСТИ НУЖНА, ЧТОБЫ ПРОТЕСТИРОВАТЬ ПОЛЬЗОВАТЕЛЯ(ЕЙ) ?
НЕТ
314
A
(Фиг.4)
ДА
306
ОБУЧЕНИЕ ФИЛЬТРА НА ОСНОВЕ ДАННЫХ ОТ БОЛЬШИНСТВА ОПРОШЕННЫХ ПОЛЬЗОВАТЕЛЕЙ (к примеру, 90%), ИСКЛЮЧЕНИЕ ПРИМЕРНО 10% ОПРОШЕННЫХ ПОЛЬЗОВАТЕЛЕЙ
308
ПРИМЕНЕНИЕ ОБУЧЕННОГО ФИЛЬТРА К ДАННЫМ ОТ ПРИМЕРНО 10% ОПРОШЕННЫХ ПОЛЬЗОВАТЕЛЕЙ, ЧТОБЫ ОПРЕДЕЛИТЬ, КАК БЫ ПРОГОЛОСОВАЛИ ПРИМЕРНО 90% ПОЛЬЗОВАТЕЛЕЙ ПО СООБЩЕНИЯМ ПРИМЕРНО 10% ПОЛЬЗОВАТЕЛЕЙ
310
ЧИСЛО НЕСОВПАДЕНИЙ МЕЖДУ ФИЛЬТРОМ 90% И 10% ПОЛЬЗОВАТЕЛЕЙ ПРЕВЫШАЕТ ПОРОГ ?
НЕТ
ДА
312
РУЧНАЯ ПРОВЕРКА ОТВЕТОВ/КЛАССИФИКАЦИЙ ОДНОГО ИЛИ БОЛЕЕ ПОЛЬЗОВАТЕЛЕЙ, ОТПРАВКА ТЕСТОВОГО СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ(ЯМ) И/ИЛИ ИСКЛЮЧЕНИЕ ОТВЕТОВ ПОЛЬЗОВАТЕЛЕЙ
КОНЕЦ

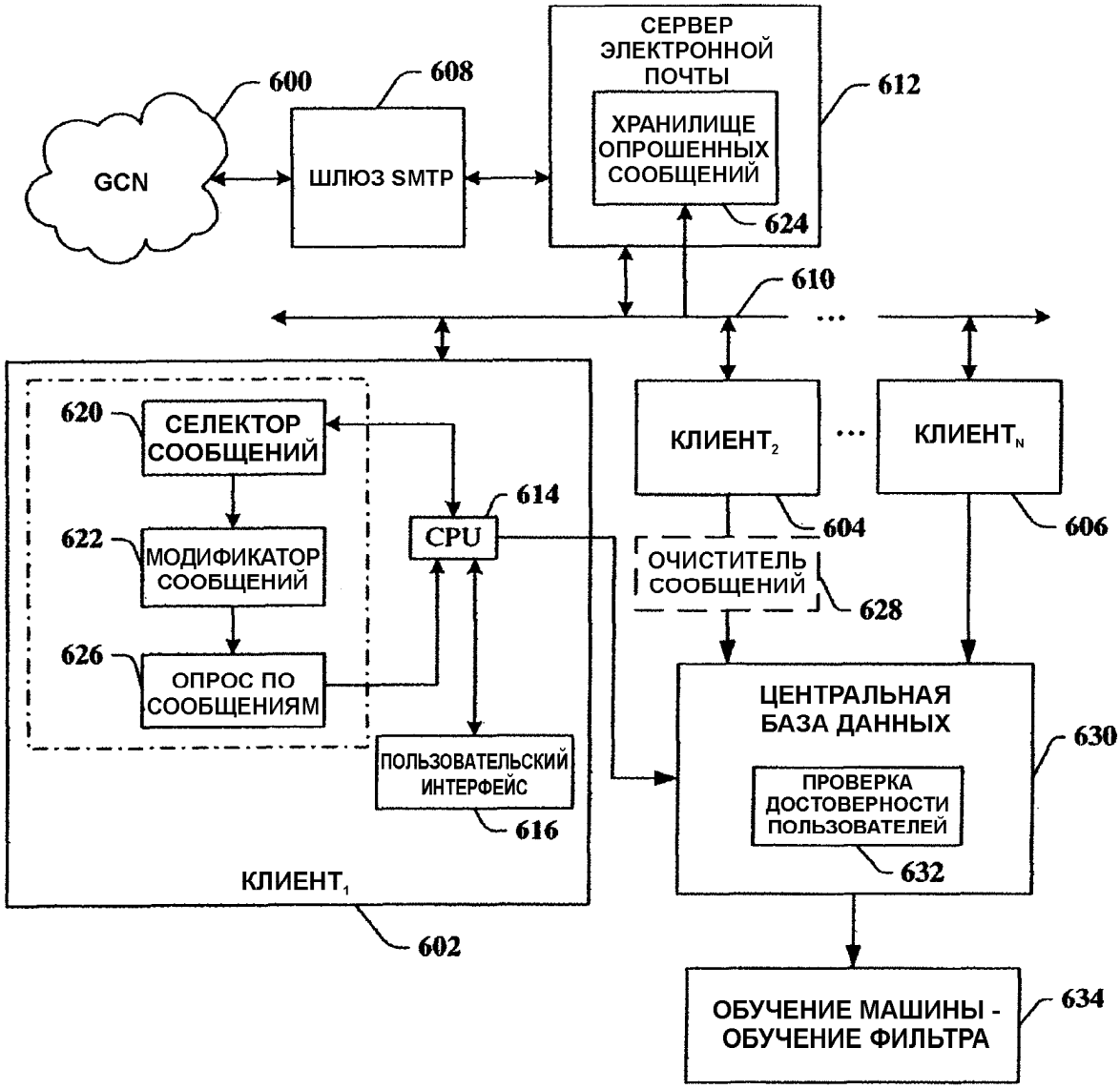
Фиг. 3


314
A
(Фиг. 3)
400
ОТПРАВКА ТЕСТОВОГО СООБЩЕНИЯ С ИЗВЕСТНЫМ РЕЗУЛЬТАТОМ ПОЛЬЗОВАТЕЛЮ(ЯМ)
402
СРАВНЕНИЕ ГОЛОСА(ОВ) ПОЛЬЗОВАТЕЛЯ С ИЗВЕСТНЫМ РЕЗУЛЬТАТОМ
404
412
B
(Фиг. 3)
406
ГОЛОС(А) ПОЛЬЗОВАТЕЛЯ СОВПАДАЕТ С ИЗВЕСТНЫМ РЕЗУЛЬТАТОМ ?
ДА
СОХРАНЕНИЕ ПОЛЬЗОВАТЕЛЯ В КАЧЕСТВЕ УЧАСТНИКА ОПРОСА
410
НЕТ
408
РУЧНАЯ ПРОВЕРКА КЛАССИФИКАЦИЙ ПОЛЬЗОВАТЕЛЕЙ И/ИЛИ УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ ИЗ БУДУЩЕГО ГОЛОСОВАНИЯ
КОНЕЦ

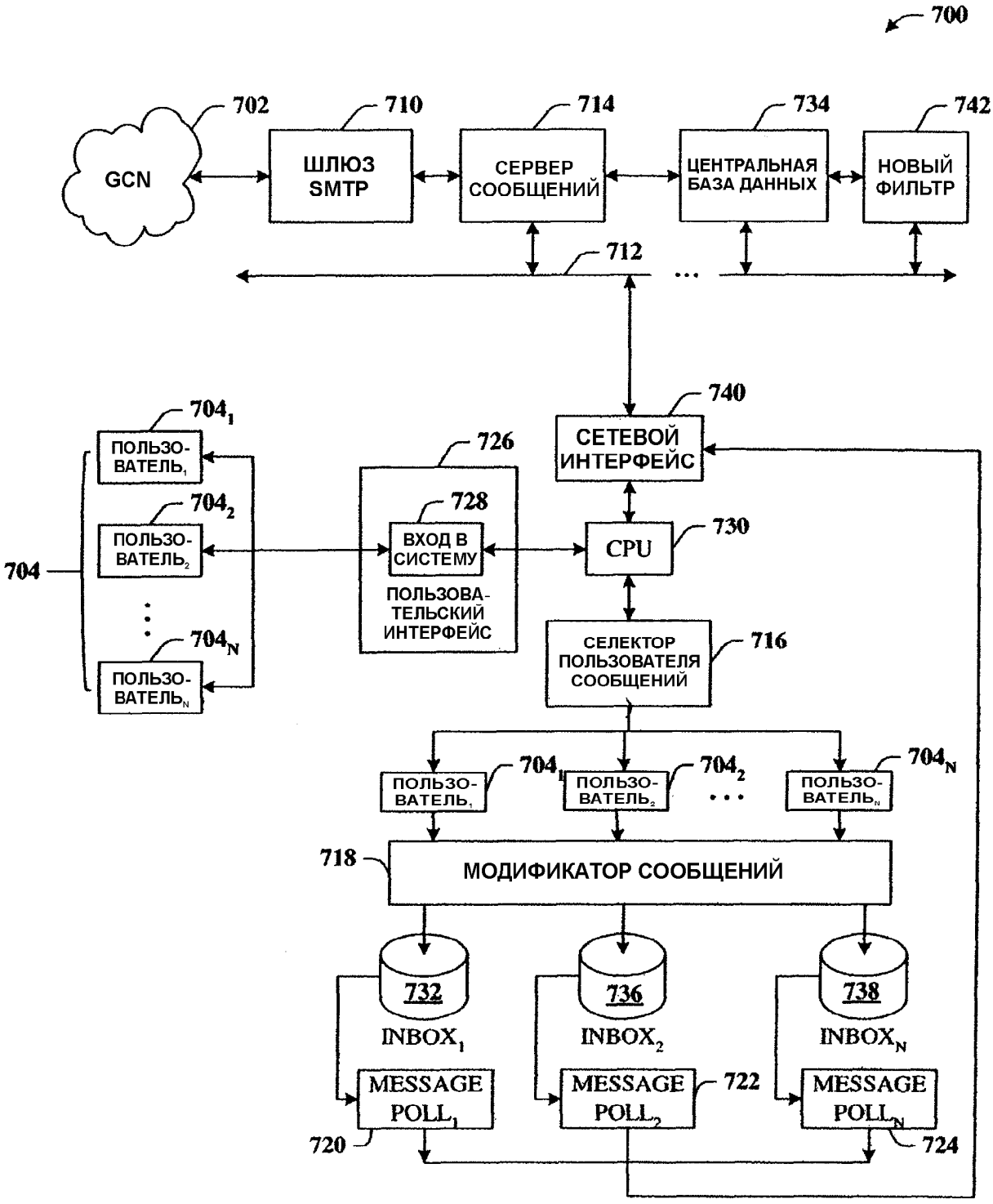
Фиг. 4


500
НАЧАЛО
СОЗДАНИЕ НОВОГО АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ БЕЗ ПУБЛИЧНОГО РАСКРЫТИЯ
502
ПРИЕМ ВХОДЯЩЕЙ ПОЧТЫ
504
ПОЧТА БЫЛА ОЖИДАЕМА ?
506
ДА
НЕТ
КЛАССИФИКАЦИЯ ЭЛЕКТРОННОЙ ПОЧТЫ КАК ПОЛЕЗНОЙ ПОЧТЫ
510
КЛАССИФИКАЦИЯ КАК НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКИ (к примеру, добавление в список несанкционированной рассылки)
508
ОБУЧЕНИЕ ФИЛЬТРА НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКИ
512

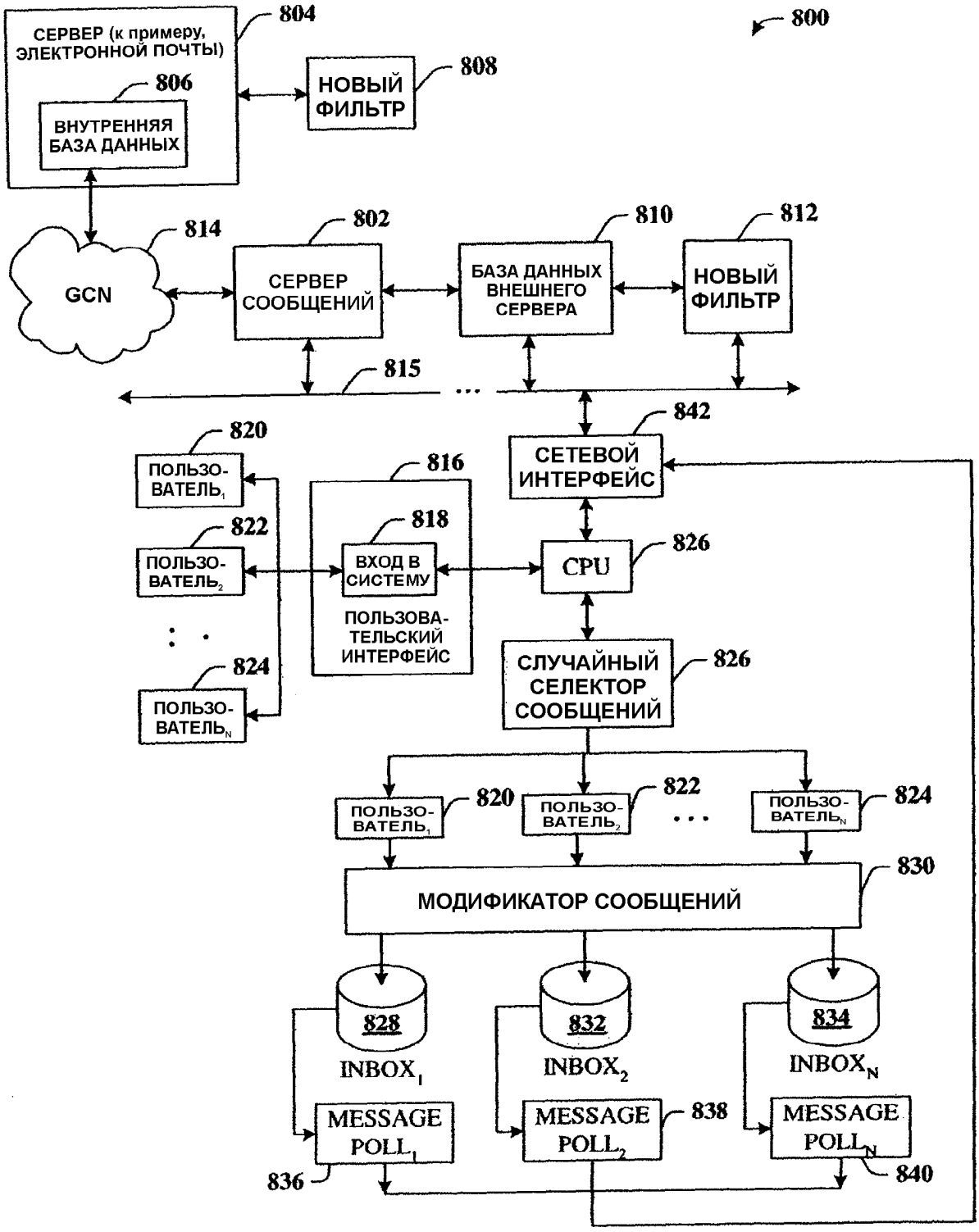
Фиг. 5


GCN
600
ШЛЮЗ SMTP
608
СЕРВЕР ЭЛЕКТРОННОЙ ПОЧТЫ
ХРАНИЛИЩЕ ОПРОШЕННЫХ СООБЩЕНИЙ
624
612
610
КЛИЕНТ2
КЛИЕНТN
604
606
620
СЕЛЕКТОР СООБЩЕНИЙ
622
МОДИФИКАТОР СООБЩЕНИЙ
626
ОПРОС ПО СООБЩЕНИЯМ
614
CPU
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС
616
КЛИЕНТ1
602
ОЧИСТИТЕЛЬ СООБЩЕНИЙ
628
ЦЕНТРАЛЬНАЯ БАЗА ДАННЫХ
ПРОВЕРКА ДОСТОВЕРНОСТИ ПОЛЬЗОВАТЕЛЕЙ
632
630
ОБУЧЕНИЕ МАШИНЫ - ОБУЧЕНИЕ ФИЛЬТРА
634

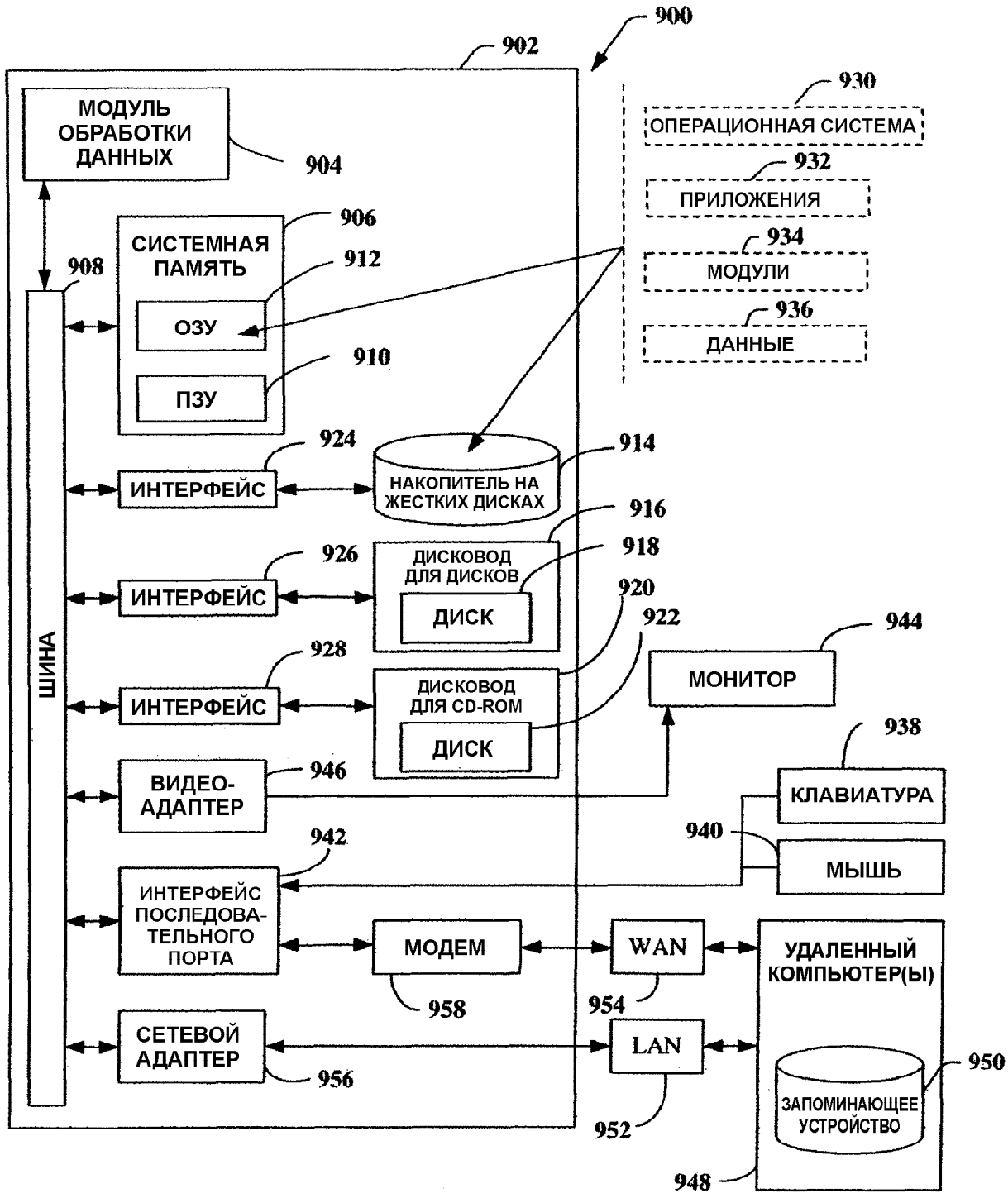
Фиг. 6


700
GCN
702
ШЛЮЗ SMTP
710
СЕРВЕР СООБЩЕНИЙ
714
ЦЕНТРАЛЬНАЯ БАЗА ДАННЫХ
734
НОВЫЙ ФИЛЬТР
742
712
...
СЕТЕВОЙ ИНТЕРФЕЙС
740
ПОЛЬЗОВАТЕЛЬ1
ПОЛЬЗОВАТЕЛЬ2
ПОЛЬЗОВАТЕЛЬN
704
704 1
704 2
704 N
726
ВХОД В СИСТЕМУ
728
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС
CPU
730
СЕЛЕКТОР ПОЛЬЗОВАТЕЛЯ СООБЩЕНИЙ
716
МОДИФИКАТОР СООБЩЕНИЙ
718
732
736
738
INBOX1
INBOX2
INBOXN
MESSAGE POLL1
MESSAGE POLL2
MESSAGE POLLN
722
720
724

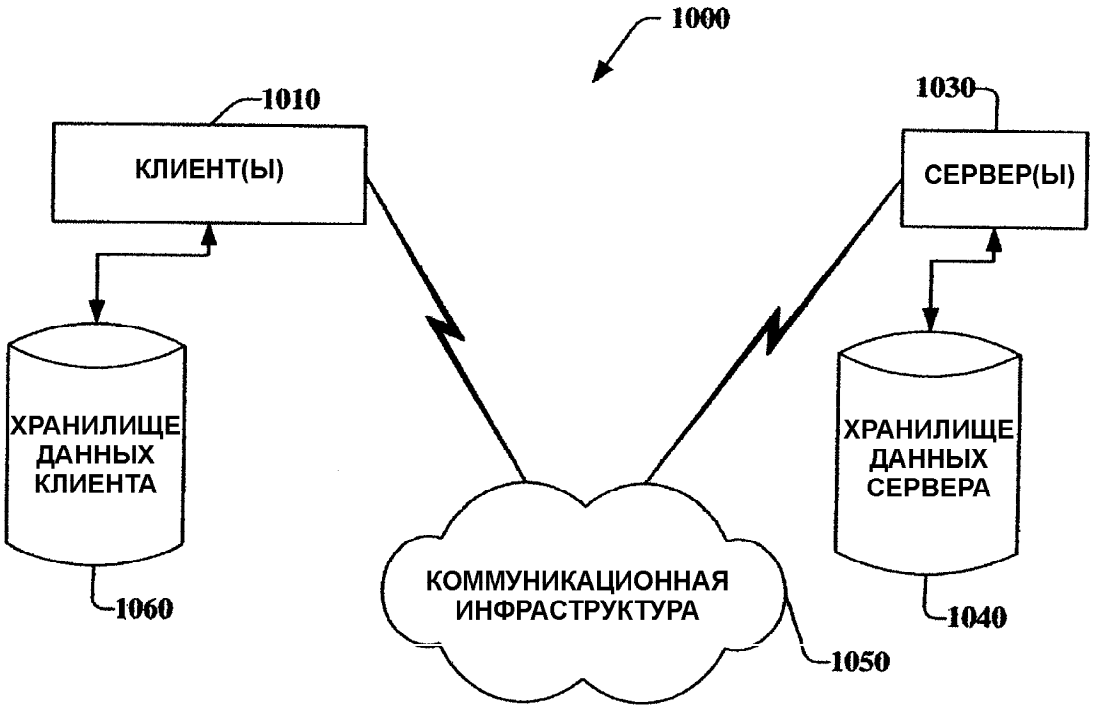
Фиг. 7


800
СЕРВЕР (к примеру, ЭЛЕКТРОННОЙ ПОЧТЫ)
804
ВНУТРЕННЯЯ БАЗА ДАННЫХ
806
НОВЫЙ ФИЛЬТР
808
GCN
814
СЕРВЕР СООБЩЕНИЙ
802
БАЗА ДАННЫХ ВНЕШНЕГО СЕРВЕРА
810
НОВЫЙ ФИЛЬТР
812
815
842
СЕТЕВОЙ ИНТЕРФЕЙС
ПОЛЬЗОВАТЕЛЬ1
820
ПОЛЬЗОВАТЕЛЬ2
822
ПОЛЬЗОВАТЕЛЬN
824
816
ВХОД В СИСТЕМУ
818
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС
CPU
826
СЛУЧАЙНЫЙ СЕЛЕКТОР СООБЩЕНИЙ
826
ПОЛЬЗОВАТЕЛЬ1
820
ПОЛЬЗОВАТЕЛЬ2
822
ПОЛЬЗОВАТЕЛЬN
824
МОДИФИКАТОР СООБЩЕНИЙ
830
828
INBOX1
832
INBOX2
834
INBOXN
MESSAGE POLL1
MESSAGE POLL2
838
MESSAGE POLLN
836
840

Фиг. 8


900
902
МОДУЛЬ ОБРАБОТКИ ДАННЫХ
904
930
ОПЕРАЦИОННАЯ СИСТЕМА
932
ПРИЛОЖЕНИЯ
934
МОДУЛИ
936
ДАННЫЕ
906
СИСТЕМНАЯ ПАМЯТЬ
908
912
ОЗУ
910
ПЗУ
924
ИНТЕРФЕЙС
914
НАКОПИТЕЛЬ НА ЖЕСТКИХ ДИСКАХ
916
926
ИНТЕРФЕЙС
ДИСКОВОД ДЛЯ ДИСКОВ
918
ДИСК
920
922
928
ИНТЕРФЕЙС
ДИСКОВОД ДЛЯ CD-ROM
ДИСК
ШИНА
944
МОНИТОР
938
946
ВИДЕО-АДАПТЕР
КЛАВИАТУРА
940
МЫШЬ
942
ИНТЕРФЕЙС ПОСЛЕДОВА-ТЕЛЬНОГО ПОРТА
МОДЕМ
WAN
УДАЛЕННЫЙ КОМПЬЮТЕР(Ы)
958
954
СЕТЕВОЙ АДАПТЕР
LAN
950
ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО
956
952
948

Фиг. 9


1000
1010
КЛИЕНТ(Ы)
1030
СЕРВЕР(Ы)
ХРАНИЛИЩЕ ДАННЫХ КЛИЕНТА
1060
КОММУНИКАЦИОННАЯ ИНФРАСТРУКТУРА
1050
ХРАНИЛИЩЕ ДАННЫХ СЕРВЕРА
1040

Фиг. 10