РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 790 330**(13) **C2**

(51) МПК
G06F 21/55 (2013.01)
G06N 20/20 (2019.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/554 (2022.02); G06N 20/20 (2022.02); H04L 63/1483 (2022.02)

(21)(22) Заявка: **2020131453, 24.09.2020**

(24) Дата начала отсчета срока действия патента:
24.09.2020

Дата регистрации:
16.02.2023

Приоритет(ы):
(22) Дата подачи заявки: **24.09.2020**

(43) Дата публикации заявки: **24.03.2022** Бюл. № 9

(45) Опубликовано: **16.02.2023** Бюл. № 5

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО "Лаборатория Касперского", Управление по интеллектуальной собственности, Московский Дмитрий Валерьевич

(72) Автор(ы):
Бенькович Никита Дмитриевич (RU),
Ковальчук Даниил Максимович (RU),
Голубев Дмитрий Сергеевич (RU),
Деденок Роман Андреевич (RU),
Слободянюк Юрий Геннадьевич (RU)

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

(56) Список документов, цитированных в отчете о поиске: **US 2020/0067861, 27.02.2020. US 2016/0344770 A1, 24.11.2016. US 2012/0158626 A1, 21.06.2012. US 2019/0199745 A1, 27.06.2019. US 2019/0238571 A1, 01.08.2019. RU 2011148263 A, 27.05.2013. RU 2710739 C1, 10.01.2020.**

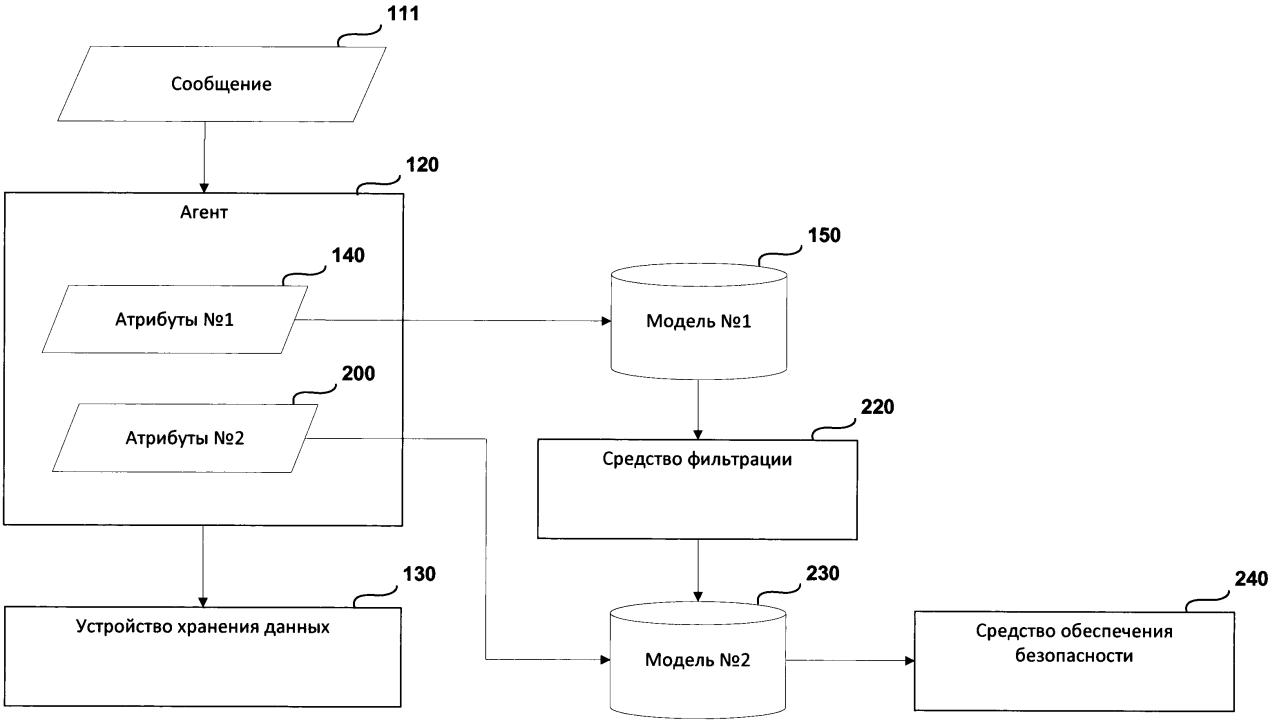
(54) Способ определения фишингового электронного сообщения

(57) Реферат:

Изобретение относится к области информационной безопасности. Технический результат заключается в повышении точности определении фишингового электронного сообщения, уменьшении количества ложных определений фишингового электронного сообщения, снижении временных и ресурсных затрат на применение ресурсоемкой второй модели машинного обучения путем предварительного определения электронного сообщения как подозрительного при помощи первой модели. Технический результат достигается при осуществлении способа определения фишингового электронного сообщения на основании использования по меньшей мере двух моделей машинного обучения, при этом с помощью первой модели определяют электронное сообщение как подозрительное на основании атрибутов первого типа перехваченного электронного сообщения, а с помощью второй модели определяют подозрительное электронное сообщение как фишинговое на основании атрибутов второго типа. 6 з.п. ф-лы, 4 ил.

RU 2790330 C2

RU 2790330 C2



Фиг. 2

RU 2790330 C2

RU 2790330 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 790 330**(13) **C2**

(51) Int. Cl.
G06F 21/55 (2013.01)
G06N 20/20 (2019.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/554 (2022.02); G06N 20/20 (2022.02); H04L 63/1483 (2022.02)

(21)(22) Application: **2020131453, 24.09.2020**

(24) Effective date for property rights:
24.09.2020

Registration date:
16.02.2023

Priority:
(22) Date of filing: **24.09.2020**

(43) Application published: **24.03.2022** Bull. № **9**

(45) Date of publication: **16.02.2023** Bull. № **5**

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO "Laboratoriya Kasperskogo", Upravlenie po intellektualnoj sobstvennosti, Moskovskij Dmitrij Valerevich

(72) Inventor(s):
Benkovich Nikita Dmitrievich (RU),
Kovalchuk Daniil Maksimovich (RU),
Golubev Dmitrij Sergeevich (RU),
Dedenok Roman Andreevich (RU),
Slobodyanyuk Yurij Gennadevich (RU)

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

(54) METHOD FOR DETERMINATION OF PHISHING ELECTRONIC MESSAGE

(57) Abstract:

FIELD: information security.

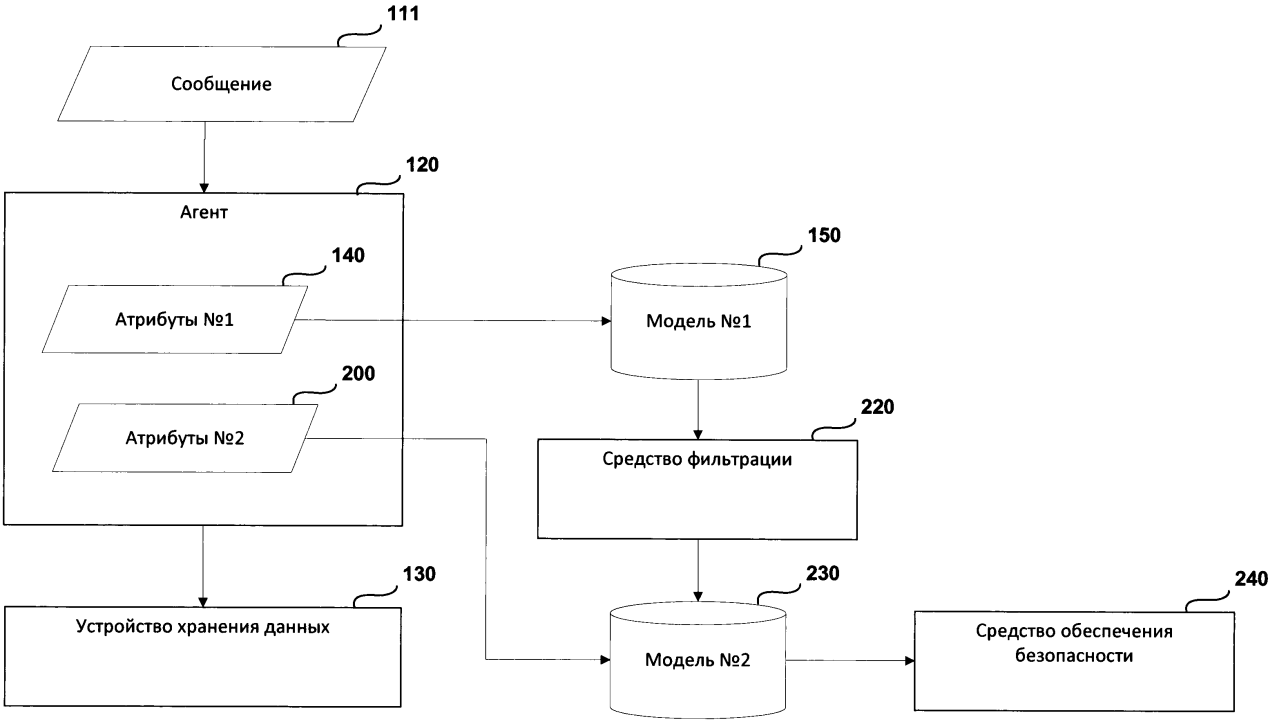
SUBSTANCE: method for determination of a phishing electronic message uses at least two machine learning models, while, using the first model, an electronic message is determined as suspicious based on the first type attributes of an intercepted electronic message, and, using the second model, a suspicious electronic message is determined as phishing based on the second type attributes.

EFFECT: increase in the accuracy of determination of a phishing electronic message, reduction in a number of false determinations of a phishing electronic message, reduction in time and resource costs for use of a resource-intensive second machine learning model by preliminary determination of an electronic message as suspicious, using the first model.

7 cl, 4 dwg

RU 2790330 C2

RU 2790330 C2



Фиг. 2

RU 2790330 C2

RU 2790330 C2

Область техники

Изобретение относится к области обеспечения информационной безопасности путем блокирования фишингового электронного сообщения.

Уровень техники

Фишинг (англ. phishing) представляет собой противоправные действия, совершаемые с целью вынудить жертву поделиться конфиденциальной информацией, например, паролем или номером кредитной карты. Чаще всего мошенники пытаются обманным путем добиться того, чтобы пользователь посетил фальшивый сайт и ввел на нем свои данные - регистрационное имя, пароль или PIN-код.

Для привлечения жертвы на сайт-ловушку злоумышленники используют массовую или адресную рассылку электронных сообщений, которые маскируются под сообщения, отправленные коллегой по работе, сотрудником банка или представителем государственного учреждения, но при этом содержат вредоносную ссылку. Текст требует от жертвы перейти по ссылке и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий. Другой вариант включает использование вложения в виде файла, где также содержатся вредоносные ссылки либо используются эксплойты для уязвимых приложений для дальнейшей компрометации компьютера пользователя.

Пройдя по ссылке, жертва попадает на фишинговый сайт, где ей предлагают «войти в систему», используя свою учетную запись (некоторые мошенники идут еще дальше, требуя отправить им копии документов или фото с удостоверением личности). Если жертва оказывается достаточно доверчивой и соглашается, то переданные данные попадают напрямую к злоумышленникам, которые используют их для кражи конфиденциальной информации или денежных средств.

Существуют два основных типа схем обнаружения мошенничества. Первый тип относится к схемам, которые обнаруживают фишинг на основе анализа содержимого целевых веб-страниц, то есть анализа веб-страниц, ссылки на которые находятся в электронном сообщении (или во вложенных документах). Второй тип - это схемы, которые работают непосредственно с содержимым электронных сообщений.

В патентной публикации US 20170085584 A1 описана технология обнаружения фишингового электронного сообщения. На основании сравнения адреса отправителя сообщения с адресом из базы данных легитимных известных отправителей определяют подозрительные письма. Если отправитель отсутствует в базе и степень схожести с легитимным отправителем выше заранее заданного значения, пользователя оповещают о подозрительном электронном сообщении.

Хотя описанный выше способ хорошо справляется с задачей распознавания адресных рассылок, имитирующих электронные сообщения от доверенных отправителей, он не позволяет распознать фишинговое сообщение от неизвестных отправителей. К тому же определение фишинга на основании степени схожести доменов может дискредитировать легального отправителя. Вместо этого необходимо применять многоуровневый подход, чтобы уменьшить количество атак и снизить количество ложных определений фишинговых сообщений.

Настоящее изобретение позволяет решать задачу обеспечения информационной безопасности путем блокирования фишингового электронного сообщения.

Раскрытие изобретения

Изобретение предназначено для обеспечения информационной безопасности путем блокирования фишингового электронного сообщения.

Технический результат настоящего изобретения заключается в определении

фишингового электронного сообщения. Другой технический результат настоящего изобретения заключается в уменьшении количества ложных определений фишингового электронного сообщения. Еще один технический результат заключается в обеспечении информационной безопасности путем блокирования фишингового электронного сообщения.

Данные результаты достигаются с помощью использования способа определения фишингового электронного сообщения на основании использования по меньшей мере двух моделей машинного обучения, при этом с помощью первой модели определяют электронное сообщение как подозрительное, а с помощью второй модели определяют подозрительное электронное сообщение как фишинговое.

В частном случае реализации способа первую модель заранее обучают на атрибутах электронных сообщений, к которым относят по меньшей мере: значение заголовка электронного сообщения Message_ID; значение заголовка электронного сообщения X-mailer; последовательность значений заголовков электронного сообщения.

Еще в одном частном случае реализации способа электронное сообщение, определенное как подозрительное, дополнительно помещают во временный карантин.

В другом частном случае реализации способа вторую модель заранее обучают на атрибутах электронных сообщений, к которым относят по меньшей мере: репутацию множества ссылок, которая характеризует вероятность того, что электронное сообщение содержит фишинговую ссылку; категорию электронного сообщения; флаг присутствия домена отправителя в заранее сформированной базе нежелательных отправителей; флаг присутствия домена отправителя в заранее сформированной базе известных отправителей; степень схожести домена отправителя с доменами в заранее сформированной базе известных отправителей; флаг наличия HTML-кода в теле электронного сообщения; флаг наличия скриптовых вставок в теле электронного сообщения.

Еще в одном частном случае реализации способа репутацию множества ссылок вычисляют с помощью рекуррентной нейронной сети.

В другом частном случае реализации способа в качестве категории электронного сообщения используют N-граммы текста электронного сообщения, определенные путем отбора наиболее важных признаков, сильнее всего влияющих на результат бинарной классификации фишингового электронного сообщения.

Еще в одном частном случае реализации способа классификацию фишингового электронного сообщения выполняют на основании алгоритма логистической регрессии с регуляризацией.

В другом частном случае реализации способа в качестве алгоритма машинного обучения второй модели выступает по меньшей мере: байесовские классификаторы; логистическая регрессия; модифицированный алгоритм обучения случайного леса; метод опорных векторов; методы ближайших соседей; дерево принятия решений.

Еще в одном частном случае реализации способа дополнительно обеспечивают информационную безопасность путем по меньшей мере: блокирования фишингового электронного сообщения; информирования получателя о фишинговом характере электронного сообщения; помещения идентификатора фишингового электронного сообщения в базу данных вредоносных сообщений.

Краткое описание чертежей

Фиг. 1 иллюстрирует пример системы, предназначенной для сбора и хранения атрибутов электронного сообщения.

Фиг. 2 иллюстрирует пример системы, реализующей способ определения фишингового

электронного сообщения.

Фиг. 3 иллюстрирует способ определения фишингового электронного сообщения.

Фиг. 4 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер.

Хотя изобретение может иметь различные модификации и альтернативные формы, характерные признаки, показанные в качестве примера на чертежах, будут описаны подробно. Следует понимать, однако, что цель описания заключается не в ограничении изобретения конкретным его воплощением. Наоборот, целью описания является охват всех изменений, модификаций, входящих в рамки данного изобретения, как это определено приложенной формуле.

Описание вариантов осуществления изобретения

Объекты и признаки настоящего изобретения, способы для достижения этих объектов и признаков станут очевидными посредством отсылки к примерным вариантам осуществления. Однако настоящее изобретение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведенная в описании, является ничем иным, как конкретными деталями, необходимыми для помощи специалисту в области техники в исчерпывающем понимании изобретения, и настоящее изобретение определяется в объеме приложенной формулы.

Фиг. 1 иллюстрирует пример системы, предназначенной для сбора и хранения атрибутов электронного сообщения.

Структурная схема примера системы, предназначенной для сбора и хранения атрибутов электронного сообщения, содержит коммуникационную сеть 100, устройство пользователя 110, электронное сообщение 111, атрибуты №1140, агент 120, устройство хранения данных 130, Модель №1150.

Коммуникационная сеть 100 представляет собой систему физических каналов связи, реализующую протокол передачи электронного сообщения 111 между терминальными устройствами, а также передачу атрибутов №1140 устройству хранения данных 130.

Электронное сообщение 111 имеет определенную структуру. Оно содержит тело (англ. body) и заголовки (англ. header) - служебную информацию о маршруте прохождения писем. К примеру, в заголовках представлены данные о том, когда, откуда и по какому маршруту пришло письмо, а также информация, добавляемая к письму различными служебными программами (почтовыми клиентами).

В качестве атрибутов №1140 выступают значения заголовков, относящихся к информации о маршруте прохождения электронного сообщения 111, а также служебная информация, сформированная почтовыми клиентами.

К примеру, в качестве атрибутов №1140 выступает по меньшей мере:

• Message_ID - уникальный идентификатор электронного сообщения 111, присваиваемый первым почтовым сервером, который встретится у него на пути;

• X-mailer (mailer_name) - значение поля заголовка, в котором почтовый клиент или сервис, с помощью которого было создано электронное сообщение 111, идентифицирует себя;

• последовательность значений заголовков электронного сообщения 111.

Устройство пользователя 110 содержит почтовый клиент и агент 120. С помощью почтового клиента устройство пользователя 110 формирует электронное сообщение 111 и передает его по коммуникационной сети 100, а также принимает электронное сообщение 111 от других устройств.

Агент 120 перехватывает электронное сообщение 111 по меньшей мере:

• отслеживая принимаемый и передаваемый по почтовым протоколам трафик (POP3, SMTP, IMAP, NNTP);

• отслеживая файлы в хранилищах почтовых серверов;

• отслеживая файлы в хранилищах почтовых клиентов.

Агент 120 определяет атрибуты №1140, содержащиеся в перехваченном электронном сообщении 111, и передает их устройству хранения данных 130 с помощью коммуникационной сети 100.

Устройство хранения данных 130 предназначено для сбора, хранения и обработки атрибутов №1140. К примеру, атрибуты №1140 используют для обучения Модели №1150.

В качестве устройства хранения данных 130 выступает облачное хранилище данных, обрабатывающее атрибуты №1140 в так называемом «облаке», где «облако» - модель хранилища, предусматривающая хранение данных в Интернете с помощью поставщика облачных вычислительных ресурсов, который предоставляет хранилище данных как сервис и обеспечивает управление им.

К примеру, в качестве устройства хранения данных 130 может выступать средство, содержащее систему Kaspersky Security Network (KSN) компании АО «Лаборатория Касперского».

Фиг. 2 иллюстрирует пример системы, реализующей способ определения фишингового электронного сообщения.

Структурная схема системы определения фишингового электронного сообщения содержит электронное сообщение 111, агент 120, устройство хранения данных 130, атрибуты №1140, атрибуты №2200, модель №1150, средство фильтрации 220, модель №2230, средство обеспечения безопасности 240.

Агент 120 предназначен для перехвата электронного сообщения 111, определения атрибутов №1140, атрибутов №2200, а также передачи атрибутов №1140 устройству хранения данных 130.

В качестве атрибутов №1140 выступает по меньшей мере:

• значение заголовка электронного сообщения 111 Message_ID;

• значение заголовка электронного сообщения 111 X-mailer (mailername);

• последовательность значений заголовков электронного сообщения 111.

Модель №1150 предназначена для классификации электронного сообщения 111 на основании атрибутов №1140. Модель №1150 классифицирует электронное сообщение 111 по меньшей мере как:

• подозрительное (к примеру, содержащее спам, вредоносное вложение, фишинговую ссылку);

• регулярное.

В одном из вариантов реализации системы Модель №1150 заранее обучают при помощи атрибутов №1140, переданных на устройство хранения данных 130, таким образом, что Модель №1150 определяет на основании указанных атрибутов признаки, при помощи которых классифицирует электронное сообщение 111 с некоторой вероятностью.

К примеру, Модель №1150 может быть основана на методах глубокого обучения (англ. deep learning). В частности, атрибуты №1140 представляют в виде матрицы, где каждый символ атрибута №1140 закодирован вектором чисел фиксированной длины, и подвергают преобразованию с помощью нейронной сети, которая вычисляет степень схожести указанных атрибутов с атрибутами подозрительных сообщений. В качестве признаков выступают преобразованные слоем нейронной сети атрибуты №1140.

Средство фильтрации 220 предназначено для помещения электронного сообщения 111, которое было классифицировано Моделью №1150 как подозрительное, во временный карантин.

В одном из вариантов реализации системы средство фильтрации 220 помещает во временный карантин электронное сообщение 111, степень схожести которого с подозрительным сообщением выше заранее заданного значения (к примеру, 0.7).

Модель №2230 предназначена для классификации подозрительного электронного сообщения на основании атрибутов №2200. Модель №2230 классифицирует подозрительное электронное сообщение по меньшей мере как:

- фишинговое;
- неизвестное.

В качестве атрибутов №2 200 выступает по меньшей мере:

- репутация множества ссылок, которая характеризует вероятность того, что электронное сообщение содержит фишинговую ссылку;
- категория электронного сообщения;
- флаг присутствия домена отправителя в заранее сформированной базе нежелательных отправителей;
- флаг присутствия домена отправителя в заранее сформированной базе известных отправителей;
- степень схожести домена отправителя с доменами в заранее сформированной базе известных отправителей;
- флаг наличия HTML-кода в теле электронного сообщения;
- флаг наличия скриптовых вставок в теле электронного сообщения.

В одном из вариантов реализации системы агент 120 вычисляет репутацию множества ссылок с помощью рекуррентной нейронной сети (англ. recurrent neural network, RNN).

К примеру, агент 120 кодирует строку URL-адреса ссылки как матрицу чисел (в частности, кодирует каждый символ URL-адреса вектором фиксированной длины), а затем передает закодированную строку в рекуррентную нейронную сеть. Сеть извлекает структурные и семантические признаки из URL-адреса, а затем использует функцию активации для вычисления степени схожести извлеченных признаков с аналогичными признаками фишинговых URL-адресов. В результате в качестве репутации ссылки выступает вероятность принадлежности URL-адреса ссылки к фишинговым URL-адресам.

Еще в одном из вариантов реализации системы в качестве репутации множества ссылок выступает мера центральной тенденции репутаций множества ссылок.

В одном из вариантов реализации системы в качестве категории электронного сообщения используют N-граммы текста сообщения, определенные путем отбора наиболее важных признаков, сильнее всего влияющих на результат бинарной классификации фишингового электронного сообщения.

К примеру, в фишинговых электронных сообщениях часто встречаются триграммы: «аккаунт будет заблокирован», «вы выиграли деньги», «срочно смените пароль», которые взывают к эмоциям получателя.

Еще в одном из вариантов реализации системы классификацию фишингового сообщения выполняют на основании алгоритма логистической регрессии с регуляризацией.

К примеру, текст сообщения из обучающей выборки разбивают на N-граммы заранее заданной длины. Указанные N-граммы используют в качестве признаков для обучения модели классификации фишингового электронного сообщения на основании алгоритма

логистической регрессии с L1-регуляризацией. Применение L1-регуляризации позволяет определить весовой коэффициент каждой N-граммы, который характеризует степень влияния указанной N-граммы на результат классификации. N-граммы, весовой коэффициент которых больше заранее заданного значения (например, больше 0), используют в качестве категории сообщения.

В одном из вариантов реализации системы предварительно собирают атрибуты электронных сообщений, относящихся к заранее известному классу сообщений (к примеру, фишинговые). На основании собранных данных обучают Модель №2230 таким образом, чтобы схожие по своим атрибутам электронные сообщения могли быть классифицированы упомянутой моделью с точностью выше заданной.

В качестве алгоритма классификации выступает по меньшей мере один из следующих алгоритмов (или их комбинация):

- байесовские классификаторы (англ. naive bayesian classifier);
- логистическая регрессия (англ. logistic regression);
- MRF-классификатор (англ. MRF classifier);
- метод опорных векторов (англ. SVM, support vector machine);
- методы ближайших соседей (англ. k-nearest neighbor);
- дерево принятия решений (англ. decision tree).

В одном из вариантов реализации система дополнительно содержит средство обеспечения безопасности 240, предназначенное для обеспечения информационной безопасности.

Обеспечение информационной безопасности включает в себя по меньшей мере:

- блокирование фишингового электронного сообщения;
- информирование получателя о фишинговом характере электронного сообщения;
- помещение идентификатора фишингового электронного сообщения в базу данных вредоносных сообщений.

К примеру, в качестве средства обеспечения безопасности 240 выступает модуль приложения безопасности компании АО «Лаборатория Касперского» (например, Kaspersky Internet Security).

Фиг. 3 иллюстрирует способ определения фишингового электронного сообщения.

Структурная схема способа передачи данных системе хранения данных содержит этап 310, на котором определяют электронное сообщение как подозрительное, этап 320, на котором помещают электронное сообщение, определенное как подозрительное, во временный карантин, этап 330, на котором определяют фишинговое электронное сообщение, этап 340, на котором обеспечивают информационную безопасность.

На этапе 310 с помощью Модели №1150 определяют электронное сообщение как подозрительное.

На этапе 320 с помощью средства фильтрации 220 помещают электронное сообщение, определенное как подозрительное, во временный карантин.

На этапе 330 с помощью Модели №2230 определяют подозрительное электронное сообщение как фишинговое.

На этапе 340 с помощью средства обеспечения безопасности 240 обеспечивают информационную безопасность.

Фиг. 4 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура,

содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) 26, содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

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

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

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35, а также дополнительные программные приложения 37, другие программные модули 38 и данные программ 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например, колонками, принтером и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг. 4. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 50 и глобальную вычислительную сеть (WAN). Такие сети применяются в корпоративных

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

В заключение следует отметить, что приведенные в описании сведения являются примерами, которые не ограничивают объем настоящего изобретения, определенного формулой.

(57) Формула изобретения

1. Способ определения фишингового электронного сообщения на основании использования по меньшей мере двух моделей машинного обучения, при этом с помощью первой модели определяют электронное сообщение как подозрительное на основании атрибутов первого типа перехваченного электронного сообщения, к которым относят по меньшей мере:

значение заголовка электронного сообщения Message_ID;

значение заголовка электронного сообщения X–mailer;

последовательность значений заголовков электронного сообщения,

а с помощью второй модели определяют подозрительное электронное сообщение как фишинговое на основании атрибутов второго типа, к которым относят по меньшей мере:

репутацию множества ссылок, которая характеризует вероятность того, что электронное сообщение содержит фишинговую ссылку;

категорию электронного сообщения;

флаг присутствия домена отправителя в заранее сформированной базе нежелательных отправителей;

флаг присутствия домена отправителя в заранее сформированной базе известных отправителей; степень схожести домена отправителя с доменами в заранее сформированной базе известных отправителей;

флаг наличия HTML–кода в теле электронного сообщения;

флаг наличия скриптовых вставок в теле электронного сообщения.

2. Способ по п. 1, по которому электронное сообщение, определенное как подозрительное, дополнительно помещают во временный карантин.

3. Способ по п. 1, по которому репутацию множества ссылок вычисляют с помощью рекуррентной нейронной сети.

4. Способ по п. 1, по которому в качестве категории электронного сообщения используют N–граммы текста электронного сообщения, определенные путем отбора наиболее важных признаков, сильнее всего влияющих на результат бинарной классификации фишингового электронного сообщения.

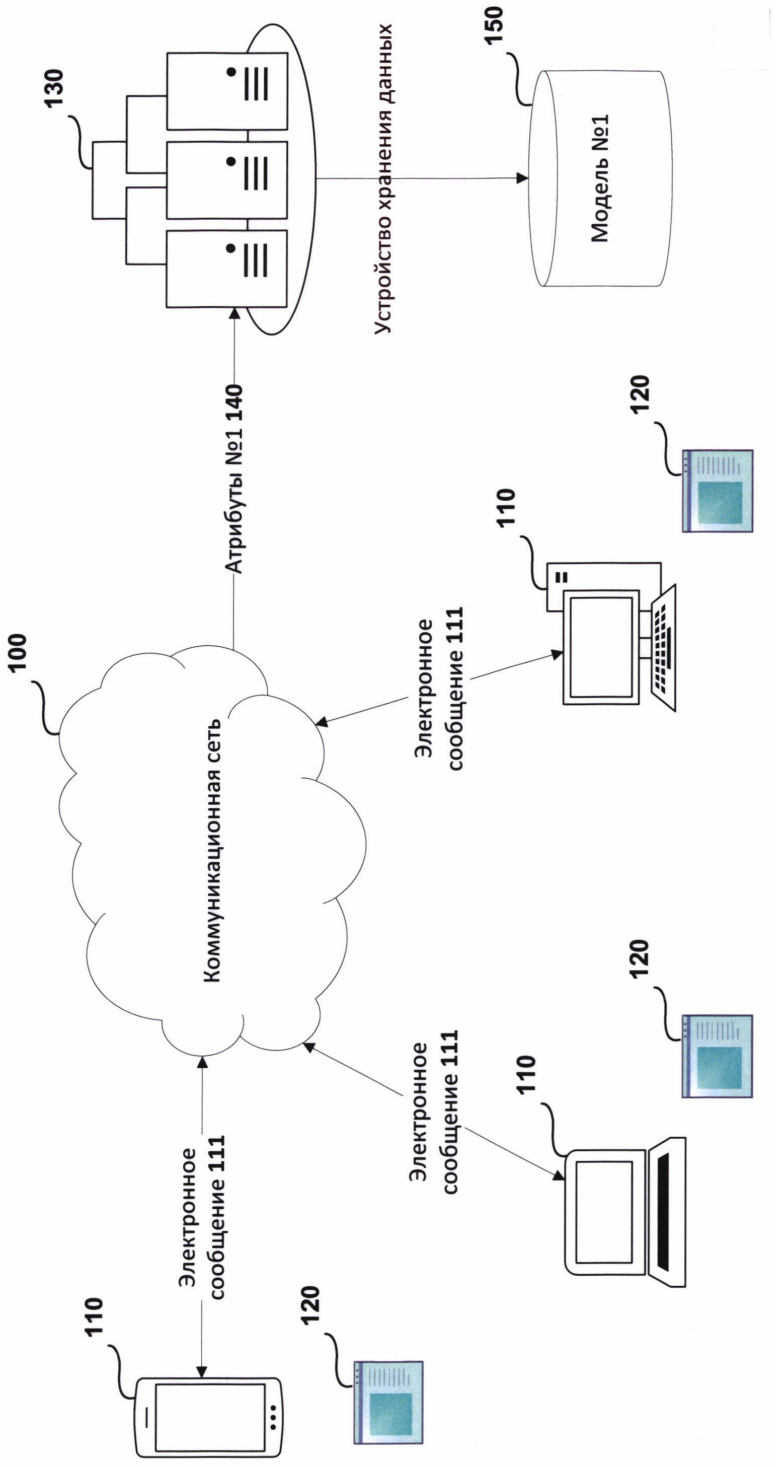
5. Способ по п. 4, по которому классификацию фишингового электронного сообщения выполняют на основании алгоритма логистической регрессии с регуляризацией.

6. Способ по п. 1, по которому в качестве алгоритма машинного обучения второй модели выступает по меньшей мере:

байесовские классификаторы;
логистическая регрессия;
модифицированный алгоритм обучения случайного леса;
метод опорных векторов;
методы ближайших соседей;
дерево принятия решений.

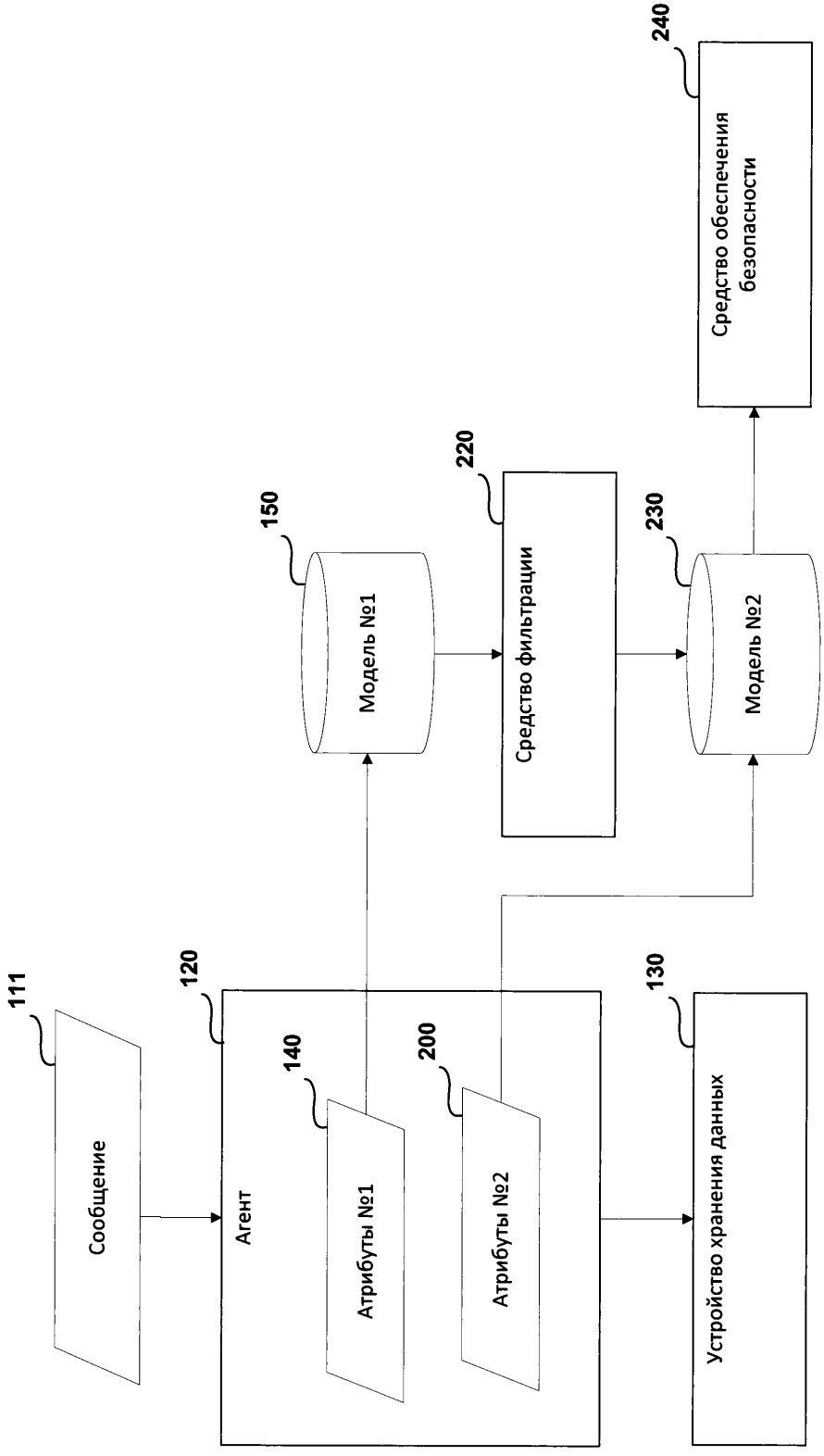
7. Способ по п. 1, по которому дополнительно обеспечивают информационную безопасность путем по меньшей мере:
блокирования фишингового электронного сообщения;
информирования получателя о фишинговом характере электронного сообщения;
помещения идентификатора фишингового электронного сообщения в базу данных вредоносных сообщений.

1


130
150
Устройство хранения данных
Модель №1
Атрибуты №1 140
120
110
100
Коммуникационная сеть
Электронное сообщение 111
Электронное сообщение 111
120
110
Электронное сообщение 111
110
120

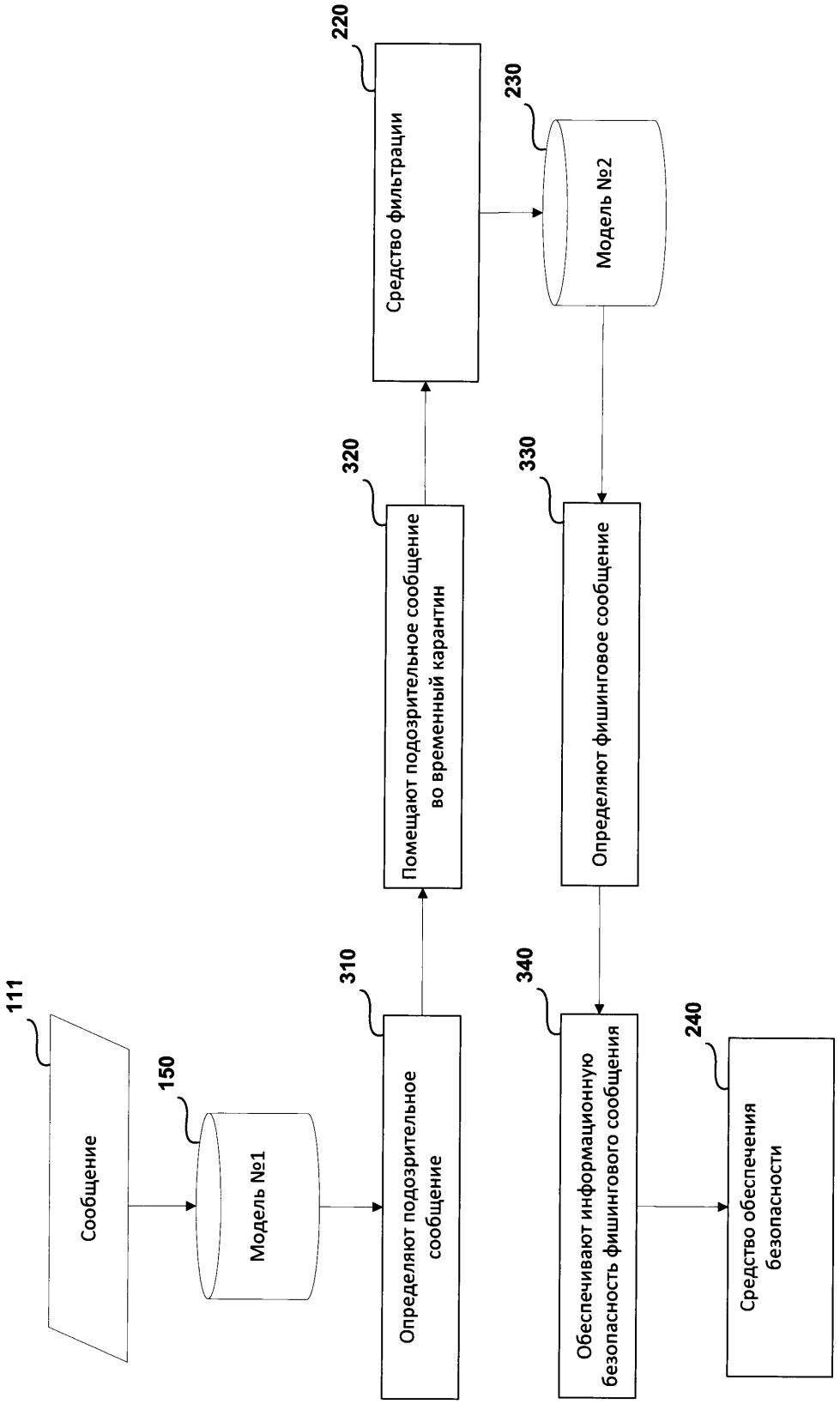
Фиг. 1

2


111
Сообщение
120
Агент
140
Атрибуты №1
200
Атрибуты №2
130
Устройство хранения данных
150
Модель №1
220
Средство фильтрации
230
Модель №2
240
Средство обеспечения безопасности

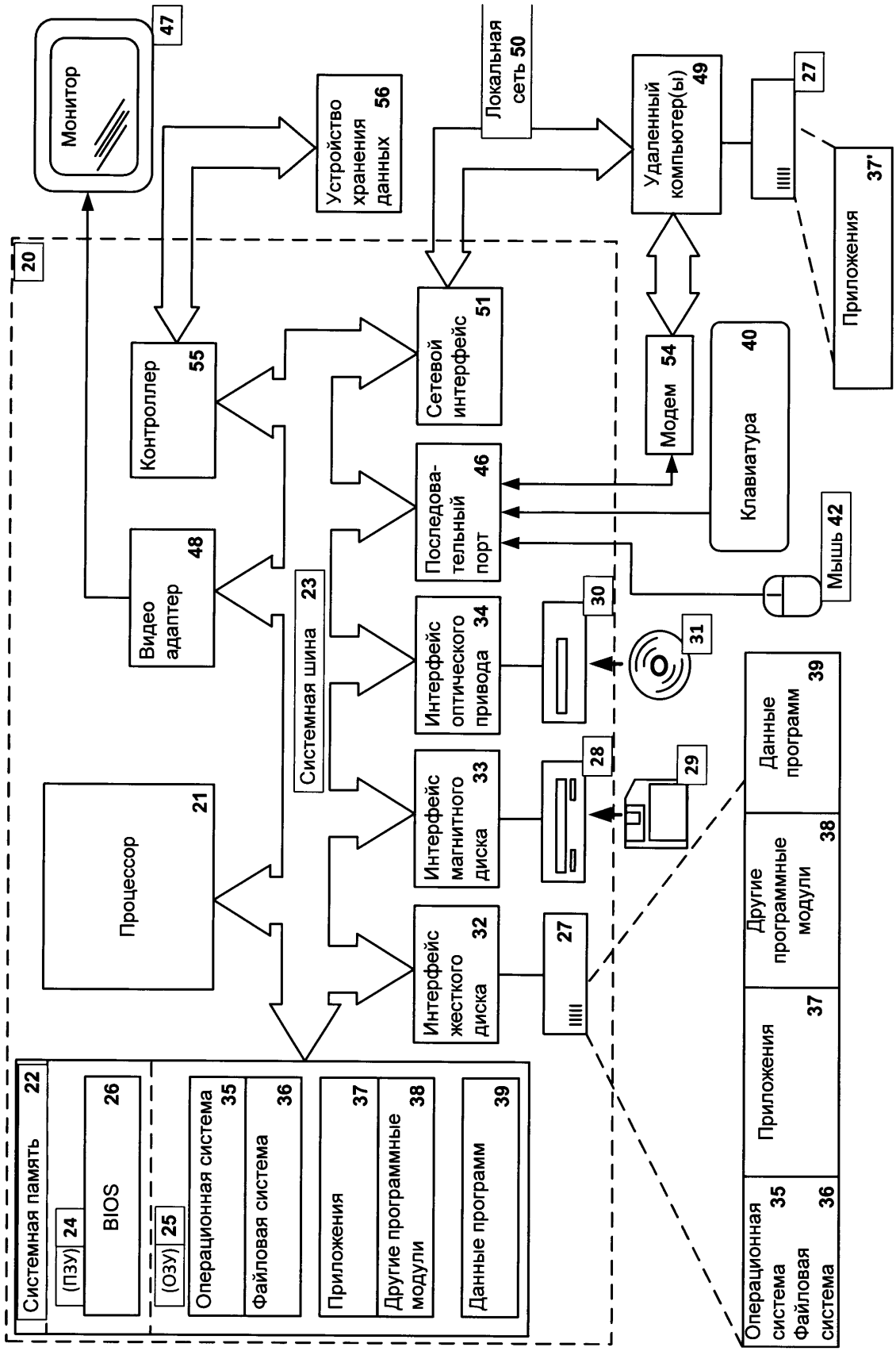
Фиг. 2

3


111
Сообщение
150
Модель №1
310
Определяют подозрительное сообщение
320
Помещают подозрительное сообщение во временный карантин
220
Средство фильтрации
230
Модель №2
330
Определяют фишинговое сообщение
340
Обеспечивают информационную безопасность фишингового сообщения
240
Средство обеспечения безопасности

Фиг. 3

4


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

Фиг. 4