

СПОСОБ И СИСТЕМА СОЗДАНИЯ СКОРИНГОВОЙ МОДЕЛИ

Область техники

Техническое решение относится к технологиям работы кредитных бюро, а более конкретно к системам и способам проверки данных онлайн пользователей на корректность и использования скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Уровень техники

Бурное развитие компьютерных технологий в последнее десятилетие, а также широкое распространение разнообразных вычислительных устройств (персональных компьютеров, ноутбуков, смартфонов и т.д.) стали мощным стимулом для использования упомянутых устройств в разнообразных сферах деятельности и для огромного количества задач (от интернет-сёрфинга до электронного документооборота и банковской деятельности). Параллельно с увеличением деятельности пользователей с использованием упомянутых вычислительных устройств через компьютерные сети росли и требования к такого рода деятельности – увеличения количества предоставляемых сервисов, увеличение скорости их работы, повышение уровня безопасности. Например, работа пользователя со своими финансами через банковский личный кабинет требует обеспечения безопасности и конфиденциальности данных, доступных из личного кабинета, быстрой авторизации пользователя в личном кабинете, а также быстрой реакции на действия, осуществляемые пользователем.

В современном мире использование недостаточно безопасных средств обмена данными между клиентами и удалёнными сервисами способно привести к огромным материальным и финансовым потерям. В финансовом секторе само использование персональных данных создаёт большие сложности по их защите – например, подмена персональных данных пользователей может обернуться потерей денег клиентов банков, в финансовом секторе неверная информация может привести к многомиллиардным убыткам и парализации работы фондовых бирж, в страховом секторе поддельная информация может стать причиной незаконных выплат и, как следствие, убытков страховых компаний. Поэтому, в настоящее время на первое место выходит оценка уровня риска от действий, осуществляемых пользователем, или данных, предоставляемых пользователем. Например, для разрешения некоторых финансовых операций пользователей (к примеру выдачу кредитов) предварительно производится оценка вероятности того, что предоставленные данные пользователя соответствуют именно этому пользователю и что упомянутый кредит будет выплачен пользователем.

Для решения описанных задач используются разнообразные скоринговые модели (англ. credit score), каждая из которых обладает своими плюсами и минусами – одни способны вычислить очень точные оценки, но работают очень долго или требуют большое количество ресурсов, другим для работы требуются персональные данные пользователей, которые могут быть скомпрометированы или к которым может быть осуществлён несанкционированный доступ (зачастую такие данные просто запрещено передавать и

хранить в рамках законодательства стран, в которых работают пользователи). При этом часто встречаемая проблема заключается в недоступности данных для эффективной работы упомянутых скоринговых моделей – например, наличие информативной кредитной истории по пользователям, запрашивающим кредит онлайн, составляет в среднем 70-85%, а наличие информативных данных в социальных сетях – 60-80%.

В публикации US8560436B2 описана технология компьютеризированной оценки кредитного риска заёмщика в условиях онлайн-кредитования. С этой целью упомянутый сервис собирает данные о заёмщике в социальных сетях и формирует на основании собранных данных оценку профиля заёмщика на основании заранее заданных правил и установленных перекрёстных связей, определённых по собранным данным.

Ещё в одной публикации US9684905 описана технология верификации пользовательских данных. С этой целью по запросу выполняют проверку актива потребителя для чего выполняют анализ конфиденциальных данных потребителя и связанных с ними косвенных данных. На основании параметров актива (тип, стоимость и т.д.) и проанализированных данных потребителя выносят решение о том, что пользовательские данные успешно прошли верификацию.

Описанные выше технологии хорошо справляются с задачами проверки пользователей, данных, предоставляемых пользователями и т.д., но при этом для своей работы требуют конфиденциальные или персональные данные пользователей, а также могут занимать значительное время.

Настоящее техническое решение позволяет решать задачу вынесения оценки (скоринг) кредитного риска или достоверности данных пользователя на основании его неперсональных данных, в том числе при онлайн кредитовании, при этом повысить доступность данных до уровня выше 99+%.

Раскрытие технического решения

Техническое решение предназначено для обеспечения работы кредитных бюро.

Технический результат настоящего технического решения заключается в проверке данных онлайн пользователей на корректность и использовании скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Дополнительный технический результат настоящего технического решения заключается в проверке прав пользователей на доступ к ресурсам.

Данные технические результаты достигаются с помощью использования системы специальной индексации онлайн пользователей и построения скоринговой модели для оценки риска с использованием неперсональных данных пользователей, которая содержит: средство сбора данных, предназначенное для сбора данных с клиентского устройства пользователя и передаче собранных данных средству индексации, при этом в качестве собираемых данных выступают по меньшей мере: данные онлайн сессии пользователя на онлайн ресурсе сервера, данные о клиентском устройстве пользователя, с которого осуществляется обмен данными с сервером, данные об активности пользователя на

упомянутом клиентском устройстве пользователя; средство индексации, предназначенное для вычисления индексов на основании собранных данных с использованием заранее заданных правил и передачи вычисленных индексов средству оценки риска; средство оценки риска, предназначенное для вычисления уровня риска доступа пользователя к ресурсам сервера на основании вычисленных индексов; средство формирования прав, предназначенное для формирования прав доступа пользователя на доступ к ресурсам, предоставляемых сервером, на основании вычисленного уровня риска.

В другом частном случае реализации системы упомянутая система представляет клиент-серверную архитектуру, в которой средство сбора данных функционирует на стороне клиента, средство индексации и средство оценки риска на стороне сервера сервис-провайдера, а средство формирования прав – на стороне сервера ресурса.

Дополнительно в одном частном случае реализации системы для сбора данных пользователя предварительно по запросу пользователя на клиентское устройство пользователя устанавливают средство сбора данных.

В другом частном случае реализации системы средство индексации дополнительно предназначено для оценки полноты полученных данных, в случае недостаточной полноты полученных данных формирования запроса к средству сбора данных на сбор дополнительных данных.

Дополнительно в одном частном случае реализации системы уровень риска доступа пользователя к ресурсам сервера представляет собой численное значение в заранее заданном диапазоне, где минимальное значение из упомянутого диапазона соответствует наибольшей безопасности ресурсов сервера при работе с ними упомянутого пользователя, а максимальное значение - наименьшей безопасности.

В другом частном случае реализации системы безопасность ресурсов характеризует вероятность по меньшей мере того, что: произойдёт невозврат кредитных средств в течении первых 90 дней после ожидаемого возврата средств; произойдёт отсутствие платежа по заёмным средствам в течении первых 90 дней после ожидаемого первого платежа; упомянутые ресурсы будут скомпрометированы; упомянутые ресурсы будут модифицированы; к упомянутым ресурсам будет осуществлён несанкционированный доступ.

Дополнительно в одном частном случае реализации системы в качестве права доступа пользователя к ресурсам сервера выступает регистрация пользователя на упомянутом сервере.

В другом частном случае реализации системы упомянутая система дополнительно содержит средство авторизации, предназначенное для: вычисления индексов на основании собранных данных; при первом запросе пользователя к серверу на предоставление доступа к ресурсам, происходит вычисление индексации, и полученные результаты ставятся в соответствие сформированным правам пользователя на доступ к ресурсам, предоставляемых сервером; при каждом последующем запросе пользователя к серверу на предоставление доступа к ресурсам с ранее сформированными правами на доступ к ресурсам, предоставляемых сервером, происходит сопоставление результатов новой индексации и результатов индексации, полученных во время первого обращения.

Данные технические результаты достигаются с помощью способа работы системы специальной индексации онлайн пользователей и системы оценки риска (скоринговой модели) с использованием неперсональных данных пользователей, при этом способ

содержит этапы, которые реализуются с помощью средств из работы систем индексации и скоринговой модели с использованием неперсональных данных пользователей и на которых: собирают данные с клиентского устройства пользователя, при этом в качестве собираемых данных выступают по меньшей мере: данные онлайн сессии пользователя на онлайн ресурсе сервера, данные о клиентском устройстве пользователя, с которого осуществляется обмен данными с сервером, данные об активности пользователя на упомянутом клиентском устройстве пользователя; вычисляют индексы на основании собранных данных с использованием заранее заданных правил; вычисляют уровень риска доступа пользователя к ресурсам сервера на основании вычисленных индексов; на основании вычисленного уровня риска формируют права пользователя на доступ к ресурсам, предоставляемых сервером.

В другом частном случае реализации способа, для сбора данных пользователя, предварительно по запросу пользователя на клиентское устройство пользователя устанавливают средство сбора данных.

Дополнительно в одном частном случае реализации способа после этапа, на котором вычисляют индексы дополнительно оценивают полноту полученные данных, и в случае недостаточной полноты полученных данных формируют запрос к средству сбора данных на сбор дополнительных данных.

В другом частном случае реализации способа уровень риска доступа пользователя к ресурсам сервера представляет собой численное значение в заранее заданном диапазоне, где минимальное значение из упомянутого диапазона соответствует наибольшей безопасности ресурсов сервера при работе с ними упомянутого пользователя, а максимальное значение - наименьшей безопасностью.

Дополнительно в одном частном случае реализации способа безопасность ресурсов характеризует вероятность по меньшей мере того, что: произойдёт невозврат кредитных средств в течении первых 90 дней после ожидаемого возврата средств; произойдёт отсутствие платежа по заёмным средствам в течении первых 90 дней после ожидаемого первого платежа; упомянутые ресурсы будут скомпрометированы; упомянутые ресурсы будут модифицированы; к упомянутым ресурсам будет осуществлён несанкционированный доступ.

В другом частном случае реализации способа в качестве права доступа пользователя к ресурсам сервера выступает регистрация пользователя на упомянутом сервере

Дополнительно в одном частном случае реализации способа: вычисляют индексацию на основании собранных данных онлайн сессии; при первом запросе пользователя к серверу на предоставление доступа к ресурсам вычисленных индексов ставят в соответствие сформированные права пользователя на доступ к ресурсам, предоставляемых сервером; при каждом следующем запросе пользователя к серверу на предоставление доступа к ресурсам применяют ранее сформированные права пользователя на доступ к ресурсам, предоставляемых сервером, соответствующие вычисленной индексации.

Краткое описание чертежей

Фиг. 1 представляет пример-структурную схему системы проверки данных онлайн пользователей на корректность и использование скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Фиг. 2 представляет пример-структурную схему способа проверки данных онлайн пользователей на корректность и использование скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Фиг. 3 представляет пример-структурную схему системы работы кредитного бюро на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Фиг. 4 представляет пример-структурную схему способа работы кредитного бюро на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Фиг. 5 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер.

Хотя техническое решение 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 технического решения конкретным его воплощением. Наоборот, целью описания является охват всех изменений, модификаций, входящих в рамки данного технического решения, как это определено в приложенной формуле.

Описание вариантов осуществления технического решения

Объекты и признаки настоящего технического решения, способы для достижения этих объектов и признаков станут понятными посредством отсылки к практическим вариантам осуществления. Однако настоящее техническое решение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведённая в описании, является ничем иным, как конкретными деталями, необходимыми для помощи специалисту в области техники в исчерпывающем понимании технического решения, и настоящее техническое решение определяется в объёме приложенной формулы.

Введём ряд определений и понятий, которые будут использоваться при описании вариантов осуществления технического решения.

Кредитный скоринг (англ. credit score) — система оценки кредитоспособности (кредитных рисков) лица, основанная на численных статистических методах. Скоринг заключается в присвоении баллов и в оценке приемлемого общего числа баллов для заёмщика кредитными специалистами или автоматизированными системами.

Кредитное поведение — данные, характеризующие обслуживание своих кредитов пользователем. Кредитное поведение состоит из данных непосредственно о кредитах (величина кредита, условия его выдачи, погашения и т.д.) и истории обслуживания кредита (даты платежей, наличие просроченных задолженностей и т.д.).

Редкие события — это события, которые имеют низкую частоту появления (например, не превышающую 1% или 0.5% от общей популяции).

Проверка статистической стабильности редких событий для отдельного процесса или объекта — проверка характера и размера эффекта редкого события при различных временных рамках, сопутствующих условиях и тестовых установках процесса/объекта и при наличии статистической значимости (где это возможно, учитывая природу редких событий).

Склеивание статистических моделей f_1 и f_2 — композиция от данных моделей. Как правило, «склеивание» статистических моделей используется для различных типов статистических моделей для повышения показателей KS и/или Gini.

Фиг. 1 представляет пример-структурную схему системы работы скоринговой модели с использованием неперсональных данных пользователей.

Структурная схема системы работы скоринговой модели с использованием неперсональных данных пользователей состоит из клиента 100, сервера 101, сервера сервис-провайдера 102, сервера ресурса 103, средства сбора данных 110, правил сбора данных 111, правил индексации 112, средства индексации 120, средства оценки риска 130, средства формирования прав 140, средства авторизации 150.

Например, в качестве клиента 100 может выступать мобильное устройство пользователя (телефон, смартфон и т.п.), персональный компьютер, ноутбук и т.д., в качестве серверов 102 и 103 – распределённая система серверов.

В некоторых вариантах реализации сервер 102 представляет собой сервер сервис-провайдера, а сервер 103 представляет собой сервер онлайн-банка.

В некоторых частных вариантах реализации сервера 102 и 103 объединяют в один сервер или кластер серверов 101, который может представлять собой распределённую систему, в которой компонент #1 сервера 101 отвечает за взаимодействие с пользователем, а компонент #2 – за анализ полученных от пользователя данных, при этом компонент #1 содержит правила индексации 112, средство индексации 120, средство оценки риска 130 и является хранилищем средств сбора данных 110 для последующей установки на клиенте 100 и сбора неперсональных данных, а компонент #2 – средство формирования прав 140, средство авторизации 150.

Разделение сервера 101 на две составляющие – 103 (сервер ресурса или сервер банка) и 102 (сервер сервис-провайдера) обусловлено снижением риска аффилированности, т.е. когда анализирующий сервер 102 не связан с сервером 103 на уровне акционерных прав, интеллектуальных прав или специальных прав использования. Данное разделение позволяет повысить информативность и точность работы сервера 102, т.к. этот сервер сервис-провайдера сможет работать с серверами 103 различных неаффилированных компаний.

Например, пользователь оформляет кредит в банке через сайт упомянутого банка. Пользователь со своего мобильного телефона 100 с помощью браузера заходит на сайт банка 103. Сайт работает на сервере банка 103, неперсональные данные собираются сервером 102 сервис-провайдера – компании, занимающейся обработкой полученных

данных, индексаций и вычисления уровня риска. Неперсональные данные собираются на основе соглашения с владельцем сервера 103. Результаты анализа полученных данных передаются обратно на сервер банка 103 и в зависимости от полученных результатов на сервере банка 103 формируются права пользователя. Таким образом, работа системы проверки данных онлайн пользователей на корректность и использование скоринговых моделей для оценки риска с использованием неперсональных данных пользователей может включать в себя взаимодействие между собой клиента 100, выбирающего (данные) сервера 103 и анализирующего (данные) сервера 102, при этом как выбирающий сервер 103 может взаимодействовать с разными анализирующими серверами 102, так и один анализирующий сервер 102 может взаимодействовать с несколькими выбирающими серверами 103 (к примеру у одного банка может быть несколько компаний-партнёров, выполняющих анализ данных, полученных от клиентов, а у одной компании, выполняющих анализ данных, полученных с клиентов, может быть несколько банков-клиентов).

Средство сбора данных 110 предназначено для сбора с клиентского устройства пользователя (клиента) 100 данных и передачи их средству индексации 120, при этом в качестве данных выступают по меньшей мере:

- данных онлайн сессии пользователя на онлайн ресурсе сервера 103,
- данные о клиентском устройстве пользователя 100, с которого осуществляется обмен данными с сервером 103 и/или 102,
- данные об активности пользователя на упомянутом клиентском устройстве пользователя 100.

Например, в качестве данных онлайн сессии пользователя могут использоваться:

- маркер (идентификатор) онлайн сессии,
- характеристики онлайн соединения, включающие по меньшей мере:
 - источник и приёмник соединения (адреса) (включая IPV4 и IPV6),
- маска браузера и заголовок онлайн запроса и другие параметры без которых не может состояться стандартное онлайн соединение.

В некоторых вариантах реализации в качестве данных о клиентском устройстве 100 используются по меньшей мере:

- параметры физических элементов клиента 100 (процессор, разрешение экрана, плотность матрицы экрана и т.д.),
- параметры операционной системы, установленной на клиенте 100 и под управлением которой работает клиент 100,
- установленные и запущенные на клиенте 100 приложения, доступные в выбранном режиме безопасности (названия, версии, режимы работы и т.д.).

В некоторых вариантах реализации в качестве параметров операционной системы используются по меньшей мере:

- название операционной системы,
- версия и ревизия операционной системы,
- битность операционной системы,

Например, Microsoft Windows 7, 64bit.

В некоторых вариантах реализации в качестве данных об активности пользователя используются по меньшей мере:

- характеристики ввода данных, включающие в себя по меньшей мере:
 - специальные клавиши и специальные символы, вводимые пользователем,
 - временные интервалы между вводом данных (более широко – частотная характеристика ввода данных),
 - приложение, из которого пользователь вводит данные (включая параметры, описанные выше для работы приложений),
- графические элементы операционной системы или приложений, с которыми взаимодействует пользователь (например, на какие кнопки нажимает пользователь),
- характеристики активности пользователя в приложениях, включающие в себя по меньшей мере:
 - время работы пользователя (начало и завершение работы, время выполнения заранее заданных действий),
 - статистические данные о работе пользователя с приложениями (например, частота выполнения заранее заданных действий в приложениях и т.д.).

В некоторых вариантах реализации средство сбора данных 110 предназначено для сбора данных с клиента 100 по запросу сервера 102.

В некоторых вариантах реализации запрос сервера 102 на сбор данных с помощью средства сбора данных 110 содержит информацию о том, какие данные требуется собрать.

Например, при первом запросе сервера 102 к клиенту 100 в запросе содержится информация на сбор параметров физических элементов клиента 100. В следующем запросе сервера 102 – информация на сбор данных по ритмичности ввода текста пользователем.

В некоторых вариантах реализации средство сбора данных 110 выполняет сбор данных с клиента 100 на основании заранее заданных правил сбора 111, при этом в запросе сервера 102 на сбор данных может содержаться информация о том, какие правила сбора данных 111 должны быть использованы.

В некоторых вариантах реализации правила сбора 111 формируются до использования их в описываемой системе специалистами, обслуживающими сервера сервис-провайдера 102, любым известным из уровня техники способом (например, на

основании статистического анализа данных, собранных ранее у других пользователей и обработанных с целью определения какие данные могут использоваться для вычисления уровня риска и какой вклад в вычисляемый уровень риска они могут внести).

В некоторых вариантах реализации для сбора данных пользователя предварительно по запросу пользователя на клиентское устройство **100** устанавливается средство сбора данных **110**.

В некоторых вариантах реализации средство сбора данных **110** представляет собой по меньшей мере:

- отдельное приложение, устанавливаемое на клиенте **100**, автоматически (т.е. без привлечения пользователя или в полуавтоматическом режиме, когда пользователю предоставляется установочный пакет средства **110**, а установку на клиенте **100** производит сам пользователь),
- специализированный драйвер, устанавливаемый в операционной системе клиента **100**.

При этом объём собираемых данных может определяться правами (в том числе административными правами), которые назначаются автоматически операционной системой или вручную пользователем.

Например, пользователь может зайти со своего смартфона (клиента **100**) на сайт кредитной организации (сервер **103**) с целью получить доступ к её ресурсам (сервера **103**) (к примеру, для оформления кредита) для чего пользователь запрашивает регистрацию. В результате упомянутых действий пользователя на клиенте **100** скачивается и устанавливается специализированное приложение (средство сбора данных **110**) с сервера **102**, которое после запуска начинает собирать данные, указанные выше при описании средства сбора данных **110**, при этом данные могут собираться

- из заранее заданного списка данных (например, название процессора, маркер сессии, список работающих на клиенте **100** приложений),
- на основании алгоритма, определяющего какие данные должны выбираться в зависимости от уже выбранных данных (например, собирает данные об оперативной памяти, если не удалось собрать данные о процессоре клиента **100**, собирает данные о работающем на клиенте **100** программном обеспечении, только если удалось собрать данные об операционной системе клиента **100**).

Средство индексации **120** предназначено для:

- вычисления индексов на основании собранных средством сбора данных **110** данных, на основании заранее заданных правил индексации **112**,
- и передачи вычисленных индексов средству оценки риска **130**.

В некоторых вариантах реализации средство индексации **120** дополнительно предназначено для:

- оценки полноты полученных данных,

- в случае недостаточной полноты полученных данных формирования запроса к средству сбора данных **110** на сбор дополнительных данных.

В некоторых вариантах реализации для оценки полноты собранных на клиенте **100** данных примеряют по меньшей мере следующие способы:

- определение собираемых у клиента **100** данных в зависимости от статистики оценки уровня риска:

Предварительно каждому типу данных, собираемых с клиента **100**, ставят в соответствие численную характеристику – вес. Чем выше вклад упомянутого типа данных в вычислении уровня риска, тем выше вес. Описанные веса могут вычисляться любым известным из уровня техники способом, в том числе статистически, на основании собранной ранее статистики собранных данных и вычисленных уровней риска. На основании весов подбираются такие типы данных, что их суммарный вклад в вычисляемый уровень риска достаточен для формирования прав доступа для заданного процента пользователей.

- определение собираемых у клиента **100** данных на основании заранее подготовленного списка с порядком данных, которые последовательно требуется собрать.

Например, для оценки риска, выполняемого средством оценки риска **130**, гарантированно достаточно всех данных, описанных выше, которые можно получить с клиента **100**. Но сбор и обработка такого объёма данных может занимать продолжительное время, а ресурсы, требуемые для обработки упомянутых данных, могут быть недоступны. Таким образом сбор всего объёма доступных данных может быть неприемлемым. Поэтому первоначально с клиента собирают минимально необходимый объём данных, требуемый для оценки риска для заранее заданной выборки пользователей, если полученных данных оказывается недостаточно, то с клиента **100** собирается следующая порция данных и т.д., до тех пор, пока объёма собранных данных не окажется достаточным для оценки риска.

Например, с клиента **100** собирается информация об онлайн-сессии (маркер онлайн-сессии, параметры соединения клиента **100** с сервером **103** и т.д.). После вычисления уровня риска оказывается, что вычисленный уровень риска находится в диапазоне значений, который не может однозначно характеризовать уровень риска. К примеру, вычисленный уровень риска равен 0.75, когда для формирования прав доступа к ресурсам сервера **100** необходим уровень риска в диапазоне [0.0, 0.2] (доступ к ресурсам разрешён) или диапазоне [0.8, 1.0] (доступ к ресурсам запрещён). В результате с клиента **100** собирается дополнительная информация об активности пользователя (какие приложения запущены на клиента **100**, какие данные упомянутые приложения обрабатывают и т.д.), в результате новых вычислений уровень риска становится равным 0.89 и выносится окончательное решение о запрещении доступа пользователю к ресурсам сервера **101**.

В некоторых вариантах реализации средство индексации **120** запрашивает данные у средства сбора данных **110** по меньшей мере до тех пор, пока:

- результат оценки полноты полученных данных не будет положительной,
- объём полученных данных находится в заранее заданном диапазоне значений,

- количество переданных средству сбора данных **110** запросов превышает заранее заданное значение (например, заданное владельцем сервера ресурса при настройке системы).

Описанный выше «заранее заданный диапазон значений, полученных данных», «заранее заданное значение количества переданных данных» и т.д. представляют собой характеристики, определяемые или устанавливаемые по меньшей мере:

- разработчиками описываемой системы работы скоринговой модели с использованием неперсональных данных пользователей,
- владельцами сервера **103**,
- работниками кредитного бюро, обслуживающими технические средства упомянутого кредитного бюро,
- работниками сервис-провайдера **102**, обслуживающими технические средства упомянутого сервис-провайдера.

При этом, упомянутые характеристики определяются и устанавливаются любым известным из уровня техники способом.

Например, работники кредитного бюро, зная какие ресурсы они будут предоставлять пользователям, а значит и какие данные от пользователей нужны для оценки риска, а какие могут быть избыточными, заранее их определяют и задают в описываемой системе.

В некоторых вариантах реализации средство индексации **120** дополнительно предназначено для выполнения мер идентификации пользователя (но не индивидуума). В качестве идентификации пользователя выступает значение индекса пользователя (идентификатор пользователя), не связанный с персональными данными, но связанный с доступом к данному ресурсу (по аналогии с уже широко применяющимися инструментами – логин и пароль пользователя, выраженные в любом известном из уровня техники виде, сертификат пользователя, биометрические данные пользователя).

В некоторых вариантах реализации в качестве алгоритма вычисления уникального идентификатора выступают по меньшей мере:

- сгенерированный случайный набор символов заданного размера,
- хэш-сумма (в том числе контрольная сумма) от данных, собранных с устройства пользователя **100** (например, CRC32, MD5),
- значение счётчика, подсчитывающего количество пользователей в описываемой системе (для каждого нового пользователя счётчик увеличивает своё значение, таким образом значение идентификатора всегда уникально).

В некоторых вариантах реализации уникальный идентификатор выбирается таким образом, чтобы вероятность коллизии упомянутых идентификаторов была меньше заранее заданного значения. При этом на вероятность коллизии идентификаторов влияет по меньшей мере:

- размер идентификатора (чем больше размер идентификатора, тем меньше вероятность коллизии идентификаторов),
- алгоритм вычисления идентификатора.

Например, в качестве упомянутого идентификатора может выступать:

- сгенерированное случайным образом 17-значное число на основе счётчика новых пользователей, что сводит к 0 вероятность коллизии;
- контрольная сумма (например, MD5), вычисленная от данных, собранных с клиента пользователя **100**. При этом, использование MD5 обладает риском коллизии и требует существенных ресурсов для вычисления онлайн по большому числу параметров, превышающих 10 000 значений и не рекомендуется к практическому применению. Например, число характеристик звуковой карты может превышать 40 000 параметров для каждой отдельной звуковой карты и вычисление MD5 может занять более 100 миллисекунд, что в совокупности с другими показателями и вычислениями сильно ограничивает использование данного метода на практике.

Например, ID = 12345678901234567 или e214fb2120ed71e1c987233a54539987.

Средство оценки риска **130** предназначено для вычисления уровня риска доступа пользователя к ресурсам сервера **103** на основании индексов и собранной дополнительно информации, вычисленных средством индексации **120**, и передачи вычисленного уровня риска средству формирования прав **140**.

В некоторых вариантах реализации уровень оценки риска доступа пользователя к ресурсам сервера **103** представляет собой численное значение в заранее заданном диапазоне, где минимальное значение из упомянутого диапазона соответствует наибольшей безопасности ресурсов сервера **103** при работе с ними упомянутого пользователя, а максимальное значение – наименьшей безопасности.

Например, уровень риска может располагаться в диапазоне от 0 (минимальный риск) до 1 (максимальный риск).

В некоторых вариантах реализации уровень риска представляет собой дискретное численное значение.

Например, уровень риска может принимать одно из нескольких значений: «минимальный риск», «разумный риск», «средний риск», «неразумный риск», «максимальный риск», которым могут быть сопоставлены значения 0.0, 0.25, 0.50, 0.75, 1.0 из диапазона значений, описанного выше.

В некоторых вариантах реализации уровень риска вычисляется по следующему алгоритму:

1. среди собранных параметров с клиента **100** и из других источников выбираются наиболее значимые предикторы (маркеры) - A_i , где i от 0 до n ; где A_0 - является 1

2. каждому значимому предиктору определяется численный вес W_i - исходя из задачи максимизации показателя Gini или KS, где W_0 - является константой, а произведение $A_0 * W_0$ - константой линейной части регрессии;

3. далее для оценки вероятности наступления одного из событий, описанных выше может использоваться формула логической регрессии

$$Y = 1 / (1 + \text{EXP}(-1 * \text{SUM}(A_i * W_i)))$$

4. в результате будет получена оценка от 0 до 1, которую используют в зависимости от подхода выделения значимых предикторов и их весов;

5. вместо логистической регрессии могут использовать дерево принятия решений, нейронные сети или комбинации (склейки) различных аналитических инструментов, список возможных инструментов не ограничен данными частными примерами применения.

В некоторых вариантах реализации безопасность ресурсов характеризует вероятность по меньшей мере того, что:

- произойдёт невозврат кредитных средств в течении заранее заданного количества дней после ожидаемого возврата средств (например, первых 90 дней);
- произойдёт невозврат отсутствие платежа в течении заранее заданного количества дней после ожидаемого первого платежа по ранее выданным заёмным средствам (например, первых 90 дней);
- упомянутые ресурсы будут скомпрометированы;
- упомянутые ресурсы будет модифицированы;
- к упомянутым ресурсам будет осуществлён несанкционированный доступ.

В некоторых вариантах реализации для вычисления уровня риска используется по меньшей мере:

- система поиска и оценки стабильных маркеров редких событий, включая систему антифрод (англ. anti-fraud) скоринга (пример построения модели приведён выше);
- система бесшовной идентификации и индексации, привязанной к деталям клиентского устройства пользователя 100 и поведения пользователя онлайн;
- система выявления стабильных идентификационных маркеров устройств и поведения пользователя онлайн, составления маркеров в онлайн режиме, мониторинга стабильности маркеров и онлайн индексации устройств и пользователей с учётом ошибок 1 и 2 рода (пример приведены ниже в разделе);
- система учёта кредитного поведения пользователей за счёт обмена неперсональными данными с другими серверами 103, при этом механизм учёта обратной связи от различных серверов 103 в онлайн режиме - это

механизм обмена кредитным поведением на основе того или иного клиентского устройства пользователя **100** (определяется на основе индекса полученного от системы индексации **110**).

В некоторых вариантах реализации система поиска и оценки стабильных маркеров редких событий основана по меньшей мере на:

- укрупнение частоты редких событий за счёт локализации выборки (укрупнение выборки).

Вот один из практических примеров укрупнения выборки и выявления и оценки эффекта прокси соединения на уровень списания по кредитам: уровень прокси соединения в российском секторе Интернет составляет 0.2-1.5%. Невысокая частота не позволяет полностью проверить статистическую значимость данного фактора на уровень списания по кредитам. Для поиска и выделения данного эффекта проводится укрупнение выборки, например, за счёт наложения дополнительных условий:

- а) выделение соединений с нарушением временной зоны,
- б) выделение интернет соединений из ДатаЦентров.

В случае а) - доля прокси соединений вырастет до 6-7% от всей популяции при условии а).

Если применить одновременно а) и б) - то доля прокси соединений вырастет до 40-80%.

На укрупнённых выборках можно провести более детальную проверку значимости эффекта при наличии ограничений по укрупнению и разобрать процесс и эффект отдельно от нарушения временной зоны и ДатаЦентров, без наличия прокси соединения. Результатом будет то, что эффект от выявленного прокси соединения существенно выше по сравнению с а) и б) и по сравнению с их комбинацией. Далее, после анализа эффекта на укрупнённой выборке, необходимо провести детальный анализ устойчивости эффекта редкого события на исходной популяции.

- проверки характера и размера эффекта редкого события при различных временных рамках, сопутствующих условиях и тестовых установках процесса/объекта и при наличии статистической значимости (где это возможно);
- составления независимых правил принятия решений (например, аналитиками, обслуживающими работоспособность сервиса на основании полученных ранее данных, т.е. на основании собранной статистики) на основе выявленных редких событий и механизма «склеивания» системы принятия решений и стандартного антифрод скоринга, с оптимизацией показателей KS и/или Gini. В качестве примеров независимых правил может служить следующие: при оценке и предотвращении онлайн фрода для финансовых организаций проводится использование следующих правил, независимо от других показателей - блокировка соединения при наличии торрент соединения; отказ по кредитной заявке при наличии подтверждённого

фродилентного поведение по устройству в рамках последних 12 месяцев и т.д.

Например, важность использования бесшовной идентификации (механизмов бесшовной идентификации) обоснована по меньшей мере тремя факторами:

- наличие способов, обеспечивающих высокую эффективность поиска (англ. hit rate) – характеристику, определяющуюся отношением найденных маркеров к пользователям, на клиентах **100** которых производится поиск упомянутых маркеров, и времени, затраченного на описанный выше поиск;
- характера сбора данных – данные собираются в режиме, который не требует каких-либо действий со стороны пользователя;
- полученная информация может имеет самый широкий разрешающий спектр регулирования в мире, т.е. позволяет использовать данные механизмы в разных странах.

Например, эффективность поиска 0,995 означает, что были выявлены идентификационные маркеры для более чем 99.5% пользователей или были выявлены данные для 99.5% посетителей данного ресурса (сервер **103**). Как правило, для задач оценки риска и выявления онлайн-фрода достаточно иметь эффективность поиска в 0.995 по сравнению с предыдущими посетителями данного ресурса. При этом сбор биометрических данных для 99% населения может занять свыше 10 лет (исходя из опыта других стран) и потребует существенной поддержки регулятора. Более того само наличие биометрических данных не решит проблему онлайн-фрода (примером тому могут выступать проблемы с “вклейками”, панорамными фотографиями, макияжем пользователей и графическим изменением фотографий). Из практики, чем выше уровень и сложность системы идентификации на стороне сервера **103** и серверов **102** по сравнению с конкурентами, тем ниже уровень финансовых потерь, связанных с фродом.

Средство формирования прав **140** предназначено для формирования прав доступа пользователя на доступ к ресурсам, предоставляемых сервером **103**, на основании уровня риска, вычисленного средством оценки риска **130**.

В некоторых вариантах реализации в качестве права доступа пользователя к ресурсам сервера **103** выступает по меньшей мере:

- данные, необходимые для получения доступа пользователя к ресурсам сервера **103**, при этом упомянутые данные формируются в процессе регистрации пользователя на упомянутом сервере **103**,
- совокупность правил, регламентирующих порядок и условия доступа пользователя к ресурсам сервера **103**, при этом в качестве ресурсов выступают по меньшей мере:
 - материальные ресурсы, предоставляемые сервером **103**,
 - информационные ресурсы, расположенные на сервере **103**.

Например, в качестве данных, необходимых для получения доступа к ресурсам сервера 103, могут выступать:

- логин и пароль пользователя (выраженные в любом известном из уровня техники виде, например, в виде текста или графического изображения),
- сертификат пользователя,
- результаты индексации 120 и оценка риска 130,
- биометрические данные пользователя (полученные любым известным из уровня техники способом, например, путём снятия отпечатков пальцев, рисунка сетчатки глаза или образца голоса пользователя).

Например, в качестве материальных ресурсов, предоставляемых сервером 103, могут выступать деньги (или другие материальные средства), предоставляемые пользователю (например, через денежный перевод на счёт пользователя) и оформленные в виде кредита, кредитной карты и т.д.

Например, в качестве информационных ресурсов, расположенных на сервере 103, могут выступать:

- данные, предоставляемые пользователю (например, файлы, базы данных и т.д.),
- банковские реквизиты, необходимые для получения материальных средств, описанных выше.

В некоторых вариантах реализации в качестве описанных выше правил выступают по меньшей мере разрешение или запрет на создание, модификацию или удаление данных, на основании которых выполняются действия над ресурсами, расположенными на сервере 103.

Например, пользователь может указать свои банковские реквизиты, на которые должны быть переведены запрашиваемые материальные средства.

В некоторых вариантах реализации информационные ресурсы представляют определённую технологию удовлетворения заявленной пользователем финансовой потребности. В этом случае информационный ресурс представляет собой упорядоченный комплекс взаимосвязанных организационных, технологических, информационных, финансовых, юридических и иных процедур, которые составляют целостный регламент взаимодействия банка в лице его сотрудников и подразделений с клиентом банка по поводу предоставления денежных средств.

Средство авторизации 150 предназначено для:

- при первом запросе пользователя к серверу 103 на предоставление доступа к ресурсам вычисленной индексации на сервер 102 и поставки в соответствие сформированных прав пользователя на доступ к ресурсам, предоставляемых сервером 103;

- при каждом следующем запросе пользователя к серверу 103 на предоставление доступа к ресурсам применения ранее сформированные права пользователя на доступ к ресурсам, предоставляемых сервером, соответствующие вычисленной индексации.

В некоторых вариантах реализации в качестве вычисляемой на основании собранных данных пользователя индексации выступает уникальный идентификатор, который не содержит персональных данных пользователя, но при этом может идентифицировать пользователя с заранее заданной вероятностью (например, вероятностью большей чем 99%) и при этом не может определить индивидуума, т.е. не сможет связать персональные данные пользователя с результатами индексации пользователя.

Процесс определения идентификатора состоит из двух этапов. Первый этап – индексация и поиск по существующим индексам пользователей или устройств и последующий выбор индекса/ идентификатора из найденных связанных пользователей или устройств. Второй этап – создание нового индекса/ идентификатора, в случае отсутствия связанных пользователей или устройств.

Фиг. 2 представляет пример-структурную схему способа проверки данных онлайн пользователей на корректность и использование скоринговых моделей для оценки риска на основе неперсональных данных пользователей.

Структурная схема способа проверки данных онлайн пользователей на корректность и использование скоринговых моделей для оценки риска на основе неперсональных данных пользователей содержит следующие этапы: этап 210, на котором собирают данные с клиентского устройства пользователя, этап 220, на котором вычисляют индексы, этап 221, на котором оценивают полноту данных, этап 230, на котором оценивают риск, этап 240, на котором формируют права пользователя на доступ к ресурсам, предоставляемых сервером, этап 250, на котором авторизуют пользователя.

На этапе 210 с помощью средства сбора данных 110 собирают данные с клиентского устройства пользователя (клиента) 100, при этом в качестве данных пользователя выступают по меньшей мере:

- данных онлайн сессии пользователя на онлайн ресурсе сервера 103,
- данные о клиентском устройстве пользователя 100, с которого осуществляется обмен данными с сервером 103,
- данные об активности пользователя на упомянутом клиентском устройстве пользователя 100.

На этапе 220 с помощью средства индексации 120 вычисляют индексы на основании собранных на этапе 210 данных.

Дополнительно на этапе 221 с помощью средства индексации 120 оценивают полноту полученных на этапе 210 данных, и в случае недостаточной полноты полученных данных формируют запрос к средству сбора данных 110 на сбор дополнительных данных.

На этапе 230 с помощью средства оценки риска 130 на основании вычисленных на этапе 220 индексов вычисляют уровень риска доступа пользователя к ресурсам сервера 103.

На этапе 240 с помощью средства формирования прав 140 на основании вычисленного на этапе 230 уровня риска формируют права пользователя на доступ к ресурсам, предоставляемых сервером 103.

На этапе 250 с помощью средства авторизации 150:

- запрашивают индексы средства индексации 120 на сервере сервис-провайдера 102;
- при первом запросе пользователя к серверу 103 на предоставление доступа к ресурсам вычисленных индексов ставят в соответствие сформированные права пользователя на доступ к ресурсам, предоставляемых сервером 103;
- при каждом следующем запросе пользователя к серверу 103 на предоставление доступа к ресурсам производят сверку полученных индексов при первом запросе и при текущем запросе и в случае соответствия и наличия приемлемого уровня риска этапа 230 и ранее сформированных прав пользователя на доступ к ресурсам, предоставляемых сервером 103, предоставляют доступ к ресурсам.

Фиг. 3 представляет пример-структурную схему системы работы кредитного бюро на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей

Структурная схема системы работы кредитного бюро с использованием скоринговой модели состоит из клиента 100, сервера сервис-провайдера 102, сервера ресурса 103, средства сбора данных 110, средства индексации 120, средства оценки риска 130, средства формирования прав 140, средства авторизации 150, кредитного бюро 304, средства запроса 310, средств формирования задач 320.1 и 320.2, средство авторизации сервера 330, средства уточнения риска 360.

Система работы кредитного бюро 304 на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей представляет собой клиент-серверную архитектуру в которой средство запроса 310, средство сбора данных 110 работают на стороне клиента 100, средство формирования прав 140, средство авторизации 150, средство формирования задач 320 – на стороне сервера ресурса 103, средство формирования задач 320, средство уточнения риска 360 – на стороне кредитного бюро 304, средство индексации 120, средство оценки риска 130, средство авторизации сервера 330 – на стороне сервис-провайдера 102.

В некоторых вариантах реализации кредитное бюро 304, сервер сервис-провайдера 102, сервер ресурса 103 функционируют на сервере 101, представляющем собой распределённую систему серверов. Более подробно взаимодействие средств серверов 102 и 103 описаны на **Фиг.1**. При этом объединение серверов 102 и 103 в единую распределённую систему приводит к снижению эффективности данной системы, ввиду снижения информативности работы функционала системы сервис-провайдера 102.

Средство запроса **310** предназначено для формирования пользователем запроса на доступ к ресурсам сервера **103**, которое транслируется в кредитное бюро **304** через сервер **103** и передачи сформированного запроса средствам формирования задач **320.1** и **320.2**.

В некоторых вариантах реализации средство запроса **310** представляет собой по меньшей мере:

- отдельное приложение, работающее на клиенте **100**;
- сайт ресурса **103**, загруженный в браузере, работающем на клиенте **100**.

В некоторых вариантах реализации средство запроса **310** собирает информацию от пользователя на основании данных (например, представленных в виде электронной формы, требующей заполнения пользователем), передаваемых средствам формирования задач **320.1** и **320.2**.

Например, пользователь со своего компьютера **100** с помощью **310** заходит на сайт ресурса **103**. На сайте расположена форма с данными, которые требуются кредитному бюро **304** для выполнения запроса на авторизацию пользователя **100** на сервере **103**.

Средство формирования задач **320.1** предназначено для:

- формирования запроса для передачи сформированного запроса средству формирования задач кредитного бюро **320.2**;
- для последующей обработки и проверки прав и авторизации **140** и **150**.

Средство формирования задач **320.2** предназначено для:

- формирования запроса для передачи сформированного запроса средству авторизации сервиса **330** на различных серверах **102**;
- для последующей обработки и уточнения риска средством **360**.

В некоторых вариантах реализации первоначально до того, как кредитное бюро **304** сможет обрабатывать запросы от пользователей производится регистрация кредитного бюро **304** у сервис-провайдера **102**, для чего формируется запрос на доступ к серверу сервис-провайдера **102**. С этой целью средство формирования задач настраивает учётную запись в сервис-провайдере **102**, определяет показатели уровня риска для проверки пользователя.

В некоторых вариантах реализации после регистрации у сервис-провайдера **102** кредитное бюро **304** получает от него данные (исполнимый код, ключ API, сценарии и т.д.), встраиваемый в средства кредитного бюро **304** для обеспечения взаимодействия с сервис-провайдером **102**.

Средство авторизации сервера **330** предназначено для:

- регистрации новых кредитных бюро на предоставления услуг сервис-провайдера **102**;
- передачи данных и/или деталей запроса, полученных от зарегистрированного кредитного бюро **304** средству индексации **120**.

Фиг. 4 представляет пример-структурную схему способа работы кредитного бюро на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей

Структурная схема способа работы кредитного бюро на основе проверки данных онлайн пользователей на корректность и с использованием скоринговых моделей для оценки риска на основе неперсональных данных пользователей включает следующие этапы: этап **410**, на котором выполняют регистрацию кредитного бюро **304** у сервис-провайдера **102**, этап **420**, на котором выполняют настройку работы кредитного бюро **304**, этап **430**, на котором анализируют запрос от пользователя к кредитному бюро **304**, этап **431**, на котором устанавливают средство сбора данных **110**, этап **440**, на котором предоставляют пользователю доступ к ресурсам сервера ресурсов **103**, этап **450** на котором уточняют риск, этап **210**, на котором собирают данные с клиентского устройства пользователя **100**, этап **220**, на котором вычисляют индексы, этап **230**, на котором оценивают риск, этап **240**, на котором формируют права пользователя на доступ к ресурсам, предоставляемых сервером **103**, этап **250**, на котором авторизуют пользователя.

В некоторых вариантах реализации этапы, выполняемые средствами кредитного бюро **304**, и этапы, выполняемые сервис-провайдером **102**, фактически выполняются на сервере **103**, представляющем собой распределённую систему, в которой одна составляющая - **103** (сервер банка), на которой выполняются этапы средства кредитного бюро **304**, и **102** (сервис-провайдер), на котором выполняются этапы средства сервис-провайдера **102**. Более подробно взаимодействие средств сервера **103** и сервис-провайдера **102** описаны на **Фиг.1**, а этапы, выполняемые средствами сервера **103** и сервис-провайдером **102** описаны на **Фиг.2**. При этом объединение серверов **102** и **103** в единую распределённую систему приводит к снижению эффективности данной системы, ввиду снижения информативности работы функционала системы сервис-провайдера **102**.

На этапе **410** с помощью средства формирования задач **320.2** выполняют регистрацию кредитного бюро **304**, для чего формируют запрос на доступ к сервису оценки риска и последующей передаче сформированных запросов средству авторизации сервера **330**.

На этапе **420** с помощью средства авторизации сервера **330** выполняют настройку работы кредитного бюро **304** по запросу кредитное бюро **304** на предоставления услуг сервис-провайдера **102**.

На этапе **430** с помощью средства формирования задач **320.1** анализируют запрос от пользователя к кредитному бюро **304**.

На этапе **431** с помощью средства формирования задач **320.1** устанавливают средство сбора данных **110**.

На этапе **440** с помощью средства формирования прав **140** предоставляют пользователю доступ к ресурсам сервера ресурсов **103**.

На этапе **450** с помощью средства уточнения риска **360** уточняют риск.

На этапе **250** авторизуют пользователя, при этом на этапе **250** выполняют последовательно этап **240**, на котором формируют права пользователя на доступ к

ресурсам, предоставляемых сервером 103, и этап 440, на котором предоставляют пользователю доступ к ресурсам сервера ресурсов 103.

Фиг. 5 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 жёсткий 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. Жёсткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жёсткого 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 жёсткий 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 подсоединён 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 подсоединён к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащён 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 удалёнными компьютерами **49**. Удалённый 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. 5**. 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** подключён 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, подключён 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 приведённые в описании сведения являются примерами, которые не ограничивают объём настоящего изобретения, определённого формулой.