(19) Евразийское патентное ведомство

(11) 038077 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.07.01

(21) Номер заявки
201892089

(22) Дата подачи заявки
2018.10.16

(51) Int. Cl. ***G06F 21/31*** (2006.01)
G06F 21/60 (2006.01)
G06F 17/40 (2006.01)

(54) СПОСОБ И СИСТЕМА МАРКИРОВКИ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ ДЛЯ ПОСЛЕДУЮЩЕГО АНАЛИЗА И НАКОПЛЕНИЯ

(31) **2018134909**
(32) **2018.10.03**
(33) **RU**
(43) **2020.04.30**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-A1-20020112048
US-B1-7340600
US-B2-10033716
US-B2-8321952

(57) Настоящее техническое решение, в общем, относится к обработке цифровых данных, а в частности, к способу и системе маркировки действий пользователя для последующего анализа и накопления. Предложен компьютерно-реализуемый способ маркировки действий пользователя для последующего анализа и накопления, в котором формируют по меньшей мере один открытый и закрытый ключ шифрования на определенный период действия; осуществляют шифрование уникального идентификатора пользователя открытым ключом шифрования при его обращении к веб-ресурсу или программному приложению с помощью компьютерного устройства; сохраняют зашифрованный на предыдущем шаге уникальный идентификатор пользователя в файлы служебного типа на упомянутом компьютерном устройстве, причем срок действия данных файлов служебного типа автоматически устанавливается по сроку действия открытого ключа; формируют по меньшей мере один код на странице веб-ресурса или программного приложения с встроенным зашифрованным уникальным идентификатором пользователя; осуществляют отслеживание действий пользователя с помощью упомянутого кода и последующую их запись в базу данных; передают в систему пассивной аутентификации записанные действия пользователя и сформированный ранее закрытый ключ шифрования; расшифровывают в системе пассивной аутентификации идентификатор пользователя посредством закрытого ключа шифрования, и связывают полученные действия с его профилем. Технический результат - обеспечение способа верифицированного сбора данных действий пользователя, связанных с его активностью, за счет применения шифрования уникального идентификатора пользователя, используемого при сеансе обращения пользователя к ресурсу в сети Интернет, для связывания результатов мониторинга с пользовательским профилем.

038077 B1

038077 B1

Область техники

Настоящее техническое решение, в общем, относится к обработке цифровых данных, а в частности, к способу и системе маркировки действий пользователя для последующего анализа и накопления.

Уровень техники

В настоящее время широко применяются решения для анализа активности пользователей в вычислительных информационных сетях, например сети Интернет, в целях определения наиболее выгодных предложений для пользователей, таргетированной рекламы и т.п.

В качестве примера таких решений можно рассматривать известные способы и системы, описанные в документах RU 2509362, US 20040019523, US 7685191. Как правило, такие решения опираются на захват информации, идентифицирующей информационный ресурс, на котором осуществляет те или иные действия пользователь, однако основным недостатком их воплощения является недостаточная степень анализа авторизованного клиента с привязкой конкретных действий к его профилю, что приводит к появлению зашумления и ложной информации, которой могут не быть присущи активности соответствующего пользователя.

Эти недостатки в свою очередь приводят к существенному увеличению объема нерелевантной информации, которая ложным образом индексируется для соответствующего профиля пользователя, что впоследствии затрудняет ее дальнейшее использование для обработки и вычисление на ее основании таргетированной информации для пользователей.

Сущность технического решения

Технической проблемой или задачей в данном техническом решении является необходимость создания способа сбора информации о действиях пользователя, а также верификации данной информации для текущего профиля пользователя в целях релевантного мониторинга его действий на соответствующем ресурсе в сети Интернет.

Техническим результатом является обеспечение способа верифицированного сбора данных действий пользователя, связанных с его активностью, за счет применения шифрования уникального идентификатора пользователя, используемого при сеансе обращения пользователя к ресурсу в сети Интернет, для связки результатов мониторинга с пользовательским профилем. Дополнительным техническим результатом является повышение защиты сбора данных пользовательских действий за счет применения процедуры криптографической защиты идентификатора пользователя.

Заявленный способ маркировки действий пользователя для последующего анализа и накопления включает выполнение этапов, на которых:

формируют по меньшей мере один открытый и закрытый ключ шифрования на определенный период действия;

осуществляют шифрование уникального идентификатора пользователя открытым ключом шифрования при его обращении к веб-ресурсу или программному приложению с помощью компьютерного устройства;

сохраняют зашифрованный на предыдущем шаге уникальный идентификатор пользователя в файлы служебного типа на упомянутом компьютерном устройстве, причем срок действия данных файлов служебного типа автоматически устанавливается по сроку действия открытого ключа;

формируют по меньшей мере один код на странице веб-ресурса или программного приложения с встроенным зашифрованным уникальным идентификатором пользователя;

осуществляют отслеживание действий пользователя с помощью упомянутого кода и последующую их запись в базу данных;

передают в систему аутентификации записанные действия пользователя и сформированный ранее закрытый ключ шифрования;

расшифровывают в системе пассивной аутентификации идентификатор пользователя посредством закрытого ключа шифрования и связывают полученные действия с его профилем.

В одном из частных вариантов реализации заявленного способа действия пользователя включают в себя по меньшей мере одно из: траектория движения курсора, взаимодействие с элементом графического интерфейса, время нахождения курсора на элементе графического интерфейса, скроллинг страницы веб-ресурса, переход на веб-ресурс другого домена, данные транзакций. В другом частном варианте реализации заявленного способа каждое фиксируемое действие содержит уникальный идентификатор (УИД). Заявленное решение осуществляется также за счет системы маркировки действий пользователя для последующего анализа и накопления, которая содержит по меньшей мере один процессор и по меньшей мере одно средство памяти, содержащее машиночитаемые инструкции, которые при их исполнении процессором реализуют вышеуказанный способ.

Краткое описание чертежей

Признаки и преимущества настоящего технического решения станут очевидными из приводимого ниже подробного описания и прилагаемых чертежей, на которых:

фиг. 1 иллюстрирует блок-схему осуществления заявленного способа разметки и хранения данных;

фиг. 2 иллюстрирует пример системы для реализации способа;

фиг. 3 иллюстрирует блок-схему способа по подбору релевантных предложений;

фиг. 4 иллюстрирует пример обработки информации по интересам пользователя;

фиг. 5 иллюстрирует пример вычислительного устройства.

Подробное описание

Данное техническое решение может быть реализовано на компьютере, в виде автоматизированной информационной системы (АИС) или машиночитаемого носителя, содержащего инструкции для выполнения вышеупомянутого способа. Техническое решение может быть реализовано в виде распределенной компьютерной системы, которая может быть установлена на централизованном сервере (наборе серверов). Доступ пользователей к системе возможен как из сети Интернет, так и из внутренней сети предприятия/организации посредством мобильного устройства связи, на котором установлено программное обеспечение с соответствующим графическим интерфейсом пользователя, или персонального компьютера с доступом к веб-версии системы с соответствующим графическим интерфейсом пользователя.

Ниже будут описаны термины и понятия, необходимые для реализации настоящего технического решения.

В данном решении под системой подразумевается компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, чётко определённую последовательность вычислительных операций (действий, инструкций).

Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройства хранения данных. В роли устройства хранения данных могут выступать, но не ограничиваясь, жесткие диски (HDD), флеш-память, ПЗУ (постоянное запоминающее устройство), твердотельные накопители (SSD), оптические приводы.

Программа - последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

На фиг. 1 представлена общая схема реализации способа 100 маркировки действий пользователя для последующего анализа и накопления. На первом этапе 101 выполняется формирование по меньшей мере одного открытого и закрытого ключа шифрования на определенный период действия (день, неделя, месяц и т.п.). По истечении установленного периода действия ключей выполняется их деактивация.

Метод шифрования может выбираться из различных известных решений, например алгоритм RSA, выполняющий шифрование данных на открытом ключе, известным АИС. Под деактивацией ключей понимается удаление текущей версии ключей при истечении установленной даты их действия, т.к. они более не могут использоваться для идентификации пользователя в АИС при дешифрации информации. При деактивации ключей впоследствии выполняется формирование новых ключей. На этапе 102 при обращении пользователя в канал обслуживания через сеть Интернет с личного компьютерного устройства, в частности при обращении к веб-сайту (странице веб-сайта) или программному приложению, установленному на устройстве пользователя, выполняется процедура аутентификации. Для каждого пользователя подготавливается зашифрованный уникальный идентификатор (УИД) с помощью открытого ключа. Метод шифрования может выбираться из различных известных решений, например однонаправленный механизм шифрования с использованием соли (например, sha1 или sha2), который позволяет получить уникальный ключ, который не поддается обратной расшифровке. Созданный УИД записывается в файлы служебного типа, хранящиеся на компьютерном устройстве пользователя, например файлы Интернет-сессии или cookie-файлы (этап 103). При обновлении открытого ключа по истечении срока его действия данные в служебном файле обновляются.

УИД может быть постоянным или временным. Временный УИД создается при отсутствии информации пользовательского профиля в системе аутентификации, расположенной на сервере (будет раскрыта ниже). При наличии информации о пользовательском профиле, который ранее обращался к соответствующему ресурсу, соответствующий УИД хранится в системе аутентификации.

Далее на этапе 104 на ресурсе, для которого необходимо осуществлять мониторинг активности пользователя, генерируется по меньшей мере один код (скрипт, программа), который содержит в себе зашифрованный УИД пользователя для его идентификации и выполнению соответствующего мониторинга. Для мониторинга действий пользователя может применяться скрипт, отвечающий за направление сообщений о действиях пользователя на ресурсе, например clickstream или click path, которые позволяют отследить цепочку переходов. Под ресурсом в данном случае понимается, например, страница веб-сайта или программного приложения. В другом случае код может представлять собой персональную страницу веб-сайта или интерфейса программного приложения. Анализ пользовательских действий на этапе 105 заключается в мониторинге происходящих событий на ресурсе, с которым выполняется пользовательское взаимодействие. Такими действиями могут быть, например, траектория движения курсора, взаимодействие с элементом графического интерфейса, время нахождения курсора на элементе графического интерфейса, скроллинг страницы веб-ресурса, переход на веб-ресурс другого домена, данные транзакций, скачивание файлов, переход с ресурса в социальные сети и т.п. Полученная информация о действи-

ях пользователя на этапе 106 сохраняется и передается вместе с закрытым ключом в систему аутентификации для последующей расшифровки УИД и сопоставления действий пользователем и его профилем (этап 107). Каждое действие также содержит УИД для хранения и анализа соответствующих типов выявленных действий.

УИД может быть связан с такой информацией как: номер телефона пользователя, адрес электронной почты, ФИО пользователя, номер платежной карты и т.п.

На фиг. 2 представлен общий вид системы взаимодействия элементов заявленного решения. Как указывалось выше, пользователь с помощью компьютерного устройства 200, например смартфона, персонального компьютера, планшета, игровой приставки, смарт-ТВ, носимого умного устройства и т.п., осуществляет взаимодействие с веб-ресурсом 250, например веб-сайтом или программным приложением (например, Сбербанк Онлайн).

Факт пользовательского взаимодействия на ресурсе 250 фиксируется на управляющем сервере 300. Сервер 300 содержит необходимые программно-аппаратные средства для организации работы необходимых функций по осуществлению заявленного способа 100. С помощью модуля 310 осуществляется автоматизированное генерирование кода для мониторинга действий пользователя на веб-ресурсе 250. С помощью системы аутентификации 320 выполняется создание УИД для пользователя, либо же выполняется его выбор из базы данных (БД) сервера 330, в случае если пользователь уже зарегистрирован в системе. Информация о действиях пользователя на веб-ресурсе также впоследствии сохраняется в БД 330. Данные о пользовательских действиях также передаются в модуль обработчика событий 340, который обеспечивает подбор релевантных предложений для пользователей на основе анализа их активности (действий) на веб-ресурсе 250 (Интернет ресурсе).

В качестве примера использования способа 100 маркировки действий пользователя для последующего анализа и накопления можно рассматривать его применение для целей получения релевантных предложений для пользователей, например финансовых предложений (кредитование, ипотека, вклады и т.п.). На фиг. 3 представлена общая схема реализации способа для подбора предложений 400 для пользователя на основании данных мониторинга его действий на веб-ресурсе 250. По получаемой информации о пользовательских действиях (этап 401) на веб-ресурсе 250 с помощью автоматизированной системы осуществляется анализ данных (этап 402) для определения релевантных предложений для соответствующего профиля пользователя.

Анализ пользовательских действий 401, как было указано выше, может осуществляться по различным критериям. Например, анализ может осуществляться по выполненным транзакциям пользователя (веб-сайт, POS-терминалы, банкомат, устройство самообслуживания и т.п.), совершенных как с помощью веб-ресурса 250 в сети Интернет (сайта или программного приложения), так и при оплате с помощью платежных средств (дебетовые, кредитные карты), которые впоследствии обрабатываются на сервере платежной системы и передаются в БД 330 при их сравнении с данными соответствующего пользователя. Анализ информации может происходить на основании данных, характеризующих тип продукта, или информации, соответствующей интересу пользователя, например, на основании получения данных, фиксирующих время нахождения пользователя на соответствующей вкладке веб-сайта или его взаимодействие с интерфейсом приложения (например, кредитный калькулятор, выпуск кредитной карты, открытие вклада). Фиксируемые действия пользователя используются для формирования атрибутов события или вектора обслуживания пользователя при последующих обращениях в канал.

На основе атрибутного состава событий, зафиксированных на веб-ресурсе 250 (Интернет-ресурсе), формируются бизнес-события и/или комплексные события, которые в автоматизированном режиме анализируются и обрабатываются бизнес-правилами, реализуемыми с помощью программной логики, взаимодействующей с сервером 300, в частности, с помощью модуля обработчика событий 340. По итогам обработки бизнес-правил происходит поиск конкретного продукта на этапе 403 и отправка сообщения пользователю с его описанием на этапе 404

Бизнес-событие представляет собой обработанное системой событие, сформированное пользователем ресурса 250 (например, совершенные операции по картам, переход на описание продукта на веб-сайте и т.п.). Бизнес-правила представляют собой последовательность анализа и обработки бизнес-событий пользователя.

Для обработки бизнес-правил модуль 340 может использовать следующие данные: контактная информация, возраст, пол, сегмент, регион и прочие атрибуты пользователя. Окончанием процесса обработки каждого бизнес-правила является наименование или ID конкретного продукта/вида продукта (предложения). Для этого может использоваться информация из БД 330 о текущих доступных предложениях, а также действующий продуктовый каталог. В модуле обработчика событий 340 может быть реализована аналитическая функция, которая позволяет рассчитывать аналитические значения по каждому пользователю в разрезе интервала времени, например, такими значениями могут выступать: количество событий, минимальное/среднее/максимальное/суммарное/среднее отклонение и др. значение одного из атрибутов события. Данная функция позволяет учитывать поступающие события по каждому профилю пользователя в заданный интервал времени, например, в секунду/минуту/час/сутки/неделя/месяц. Данные счетчика используются для настройки алгоритмов выявления комплексного бизнес-события пред-

ложений и отбор наиболее релевантной информации для соответствующих пользователей. Под комплексным бизнес-событием, как правило, понимается бизнес-событие, сформированное по результатам нескольких предшествующих событий, сформированных пользователем на ресурсе 250.

Каждому бизнес-событию и/или комплексному событию модуль 340 присваивает УИД. Модуль 340 может также реализовывать интерфейс для гибкой настройки алгоритмов для фильтрации операций, фиксируемых по действиям пользователей. Модуль 340 выполняет поиск и подбор предложений для пользователя на основании полученных атрибутов событий по действиям пользователя.

Сервер 300 выполняет расшифровку УИД пользователя, который содержится в атрибутах события, формируемого по его действиям на соответствующем ресурсе. По итогам обработки событий сервер 300 связывает сформированные атрибуты события с УИД пользователя для последующей передачи информации в модуль обработки событий 340 и подбора соответствующих предложений для упомянутого УИД пользователя. На этапе 402 анализ предложений имеет временный диапазон для накопления необходимой информации и подбора релевантных данных. Как представлено на фиг. 4, с помощью заявленного решения, в частности с помощью обработки поступающих данных, модулем 340 могут фиксироваться на этапе 401 повторяющиеся страницы или категории интереса пользователя по совершаемым действиям, например, при просмотре в течение дня или недели тематически схожих элементов веб-ресурса (тематик веб-страниц) 250. Тематика может относится к различным предложениям, например кредитные предложения, вклады, дебетовые/кредитные карты. Сервер 300 получает данные о событиях пользователя в заданный временной период и ранжирует их на предмет наличия доступных для данного пользователя предложений.

Временной период для отправки сообщения с предложением пользователю может выбираться также исходя из анализа общей активности пользователя как в заданный временной период, так и более длительный период, что определяется исходя из наличия релевантного предложения или активности действий пользователя и соответствующей программной логики, реализуемой на сервере 300. Дополнительно может учитываться история транзакций пользователя для учета данных атрибутов при подборе релевантных предложений. Ниже в таблице будет представлен пример хранения данных действий клиента для анализа соответствующих бизнес-событий.

Идентификатор бизнес-события	Предложение	[Дата 1]	[Дата 2]	[Дата 3]	…	Дата N
ID 1	Вклад	01.01.2018	02.01.2018			10.01.2018
ID 2	Карта	01.01.2018	02.01.2018			10.01.2018

Идентификатор бизнес-события - идентификатор бизнес-события, полученный в запросе на поиск предложения.

Предложение - наименование продаваемого(банковского)/маркетингового продукта из продуктового каталога, по идентификатору которого был получен запрос на поиск предложения.

Дата 1 - количество запросов по уникальной связке "бизнес-событие - продукт", полученных системой в первый день выбранного периода.

Дата 2 - количество запросов по уникальной связке "бизнес-событие - продукт", полученных системой во второй день выбранного периода.

Дата 3 - количество запросов по уникальной связке "бизнес-событие - продукт", полученных системой в третий день выбранного периода.

Дата N - количество запросов по уникальной связке "бизнес-событие - продукт", полученных системой в последний день выбранного периода.

Фильтрация записей может осуществляться следующим образом:

1) По полю "идентификатор бизнес-события" - в алфавитном порядке;

2) По полю "Продукт" - в алфавитном порядке.

Применяемые фильтры:

1) "Дата с". Дата начала периода для формирования отчета, используется дата получения запроса на поиск предложения

2) "Дата по". Дата окончания периода для формирования отчета, используется дата получения запроса на поиск предложения

3) "Идентификатор бизнес-события". Список всех полученных идентификаторов бизнес-событий в запросах на поиск предложений.

4) "Продукт". Список всех продуктов, по которым были получены запросы на поиск предложений.

Поиск предложений для профиля пользователя может выполняться следующим образом:

Идентификатор клиента;

Идентификатор Вида продукта и/или продаваемого продукта или Идентификатор "Информационного" продукта;

Тип канала коммуникации.

Если список атрибутов состоит из двух идентификаторов пользователя, то вначале производится поиск по основному идентификатору. Если пользователь не найден, то производится поиск по дополнительному. В сообщении на поиск предложения помимо атрибутов для поиска передаются ID бизнес-события и/или комплексного события и ID бизнес-правил.

При отправке на этапе 404 сообщение о найденном релевантном предложении пользователю может быть предусмотрена функция формирования персонализированных обращений, например SMS-сообщений или писем, отсылаемых посредством электронной почты, PUSH-уведомлений или посредством звонка пользователю оператора колл-центра. Канал для передачи сообщений пользователю об уведомлении о наличии выявленных предложений выбирается, как правило, из следующих каналов передачи информации: SMS, PUSH уведомления, Интернет сеть, телефонная связь, программное приложение, мессенджер и т.п.

Отправляемое предложение пользователю может содержать информацию, описывающую конкретный продукт или условия приобретения продукта, срок действия предложения, стоимость и иной тип данных. Для каждой пары "бизнес-событие - продукт" может быть предусмотрен алгоритм формирования контрольной группы, которая используется для оценки эффективности. С помощью данного алгоритма фиксируется количество клиентов, для которых было найдено предложение, соответствующее паре "бизнес-событие - продукт".

Применение способа 100 маркировки и хранения данных о действиях пользователя позволяет улучшить поиск релевантного одного или нескольких предложений для пользователя за счет мониторинга его активности на веб-ресурсе с достоверной идентификацией профиля пользователя. На фиг. 5 представлен пример вычислительного устройства 500, которое может применяться для выполнения функций по логической обработке необходимых данных для реализации заявленного решения. Необходимо отметить, что указанные в материалах настоящей заявки компьютерное устройство пользователя 200 и сервер 300 могут представлять собой один из вариантов воплощения вычислительного устройства 500.

В общем случае вычислительное устройство 500 содержит объединенные общей шиной 510 один или несколько процессоров 501, средства памяти, такие как ОЗУ 502 и ПЗУ 503, интерфейсы ввода/вывода 504, средства ввода/вывода 505 и средство для сетевого взаимодействия 506. Процессор 501 (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п.

ОЗУ 502 представляет собой оперативную память и предназначено для хранения исполняемых процессором 501 машиночитаемых инструкций для выполнения необходимых операций по логической обработке данных. ОЗУ 502, как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ 503 представляет собой одно или более устройств постоянного хранения данных, например жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов устройства 500 и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В 504. Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

Для обеспечения взаимодействия пользователя с вычислительным устройством 500 применяются различные средства 505 В/В информации, например клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия 506 обеспечивает передачу данных устройством 500 посредством внутренней или внешней вычислительной сети, например Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств 506 может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации, например, GPS, ГЛОНАСС, BeiDou, Galileo.

Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Компьютерно-реализуемый способ маркировки действий пользователя для последующего анализа и накопления, включающий следующие шаги:

формируют по меньшей мере один открытый и закрытый ключ шифрования на определенный период действия;

осуществляют шифрование уникального идентификатора пользователя открытым ключом шифрования при его обращении к веб-ресурсу или программному приложению с помощью компьютерного устройства;

сохраняют зашифрованный на предыдущем шаге уникальный идентификатор пользователя в файлы служебного типа на упомянутом компьютерном устройстве, причем срок действия данных файлов служебного типа автоматически устанавливается по сроку действия открытого ключа;

формируют по меньшей мере один код на странице веб-ресурса или программного приложения с встроенным зашифрованным уникальным идентификатором пользователя;

осуществляют отслеживание действий пользователя с помощью упомянутого кода и последующую их запись в базу данных;

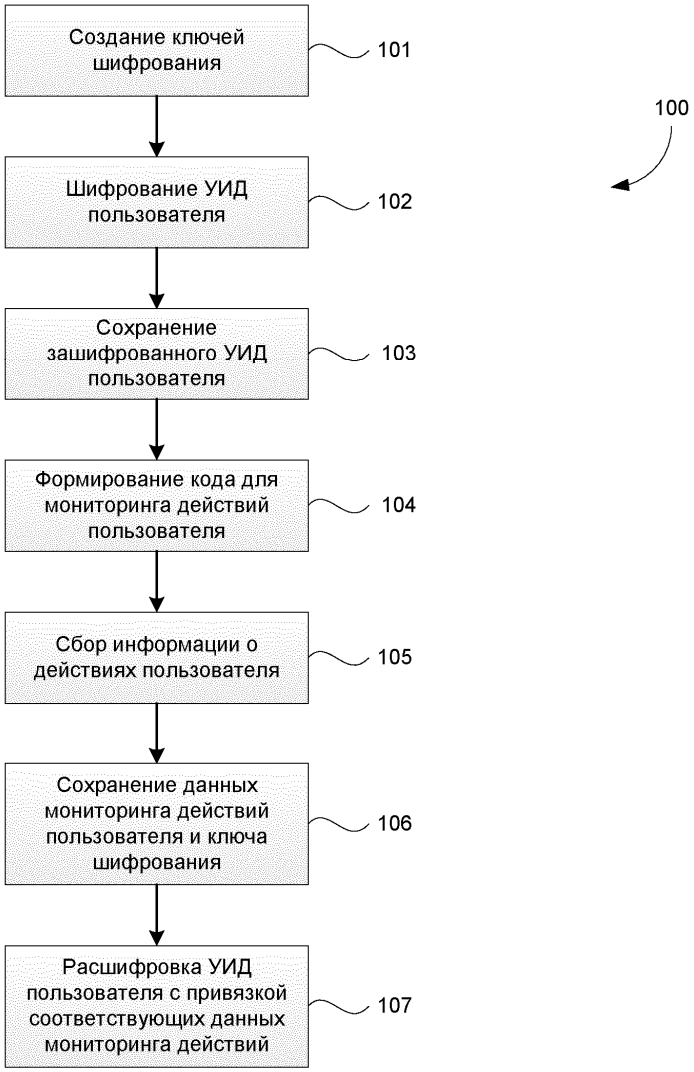
передают в систему пассивной аутентификации записанные действия пользователя и сформированный ранее закрытый ключ шифрования;

расшифровывают в системе пассивной аутентификации идентификатор пользователя посредством закрытого ключа шифрования и связывают полученные действия с его профилем.

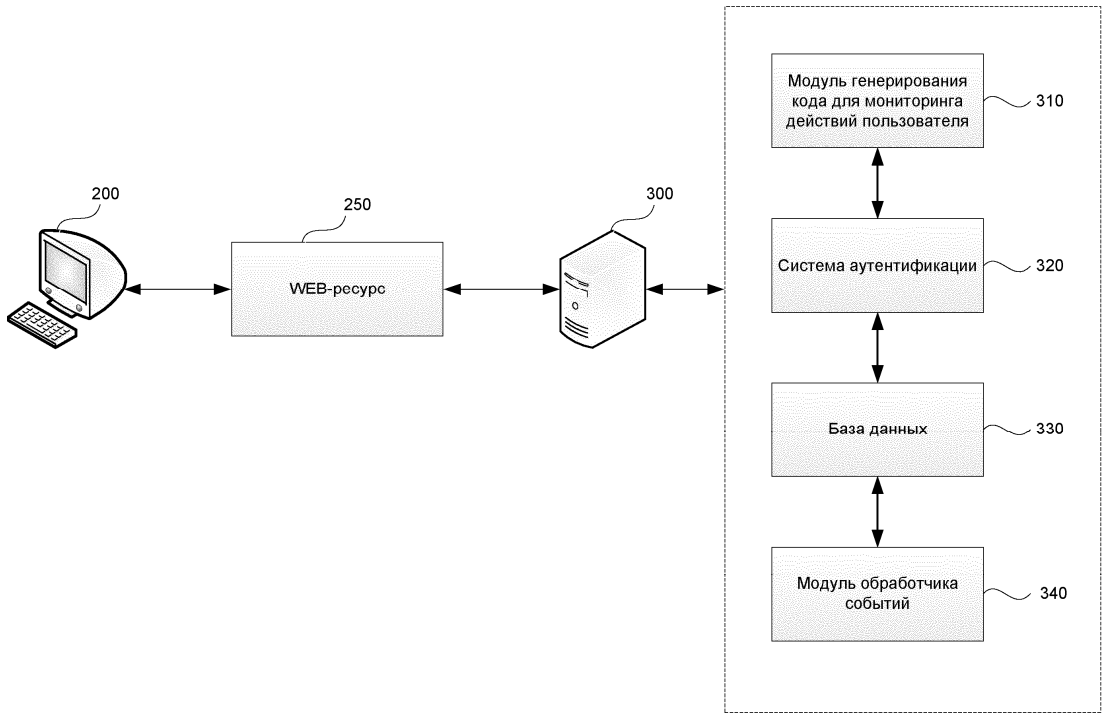
2. Способ по п.1, характеризующийся тем, что действия пользователя включают в себя по меньшей мере одно из: траектория движения курсора, взаимодействие с элементом графического интерфейса, время нахождения курсора на элементе графического интерфейса, скроллинг страницы веб-ресурса, переход на веб-ресурс другого домена, данные транзакций.

3. Способ по п.1, характеризующийся тем, что каждое фиксируемое действие содержит уникальный идентификатор (УИД).

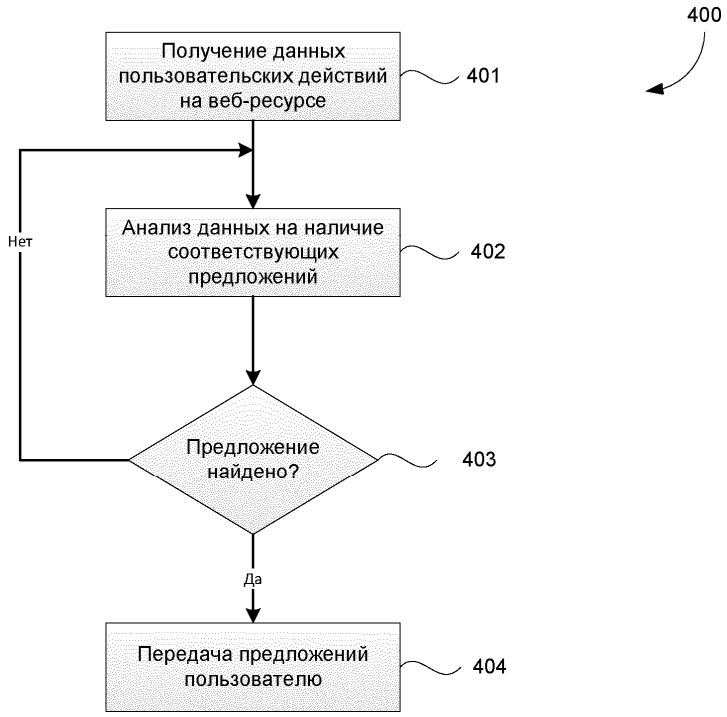
4. Система маркировки действий пользователя для последующего анализа и накопления, содержащая по меньшей мере один процессор и по меньшей мере одно средство памяти, содержащее машиночитаемые инструкции, которые при их исполнении процессором реализую способ по любому из пп.1-3.


Создание ключей шифрования
101
100
Шифрование УИД пользователя
102
Сохранение зашифрованного УИД пользователя
103
Формирование кода для мониторинга действий пользователя
104
Сбор информации о действиях пользователя
105
Сохранение данных мониторинга действий пользователя и ключа шифрования
106
Расшифровка УИД пользователя с привязкой соответствующих данных мониторинга действий
107

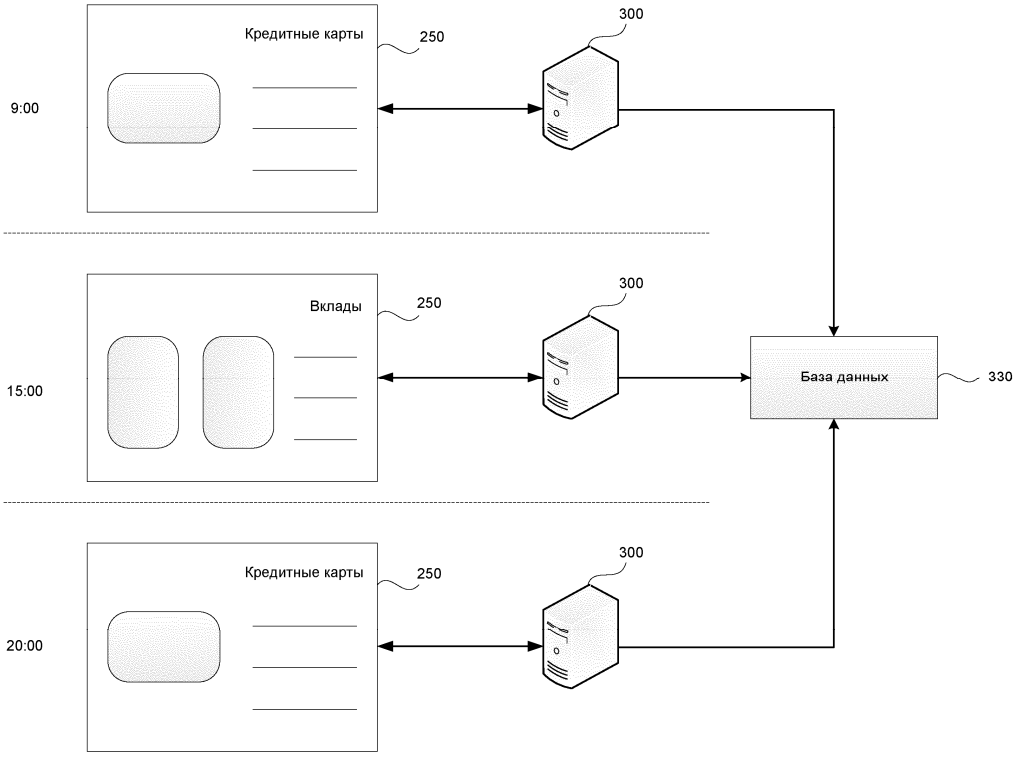
Фиг. 1


200
250
WEB-ресурс
300
Модуль генерирования кода для мониторинга действий пользователя
310
Система аутентификации
320
База данных
330
Модуль обработчика событий
340

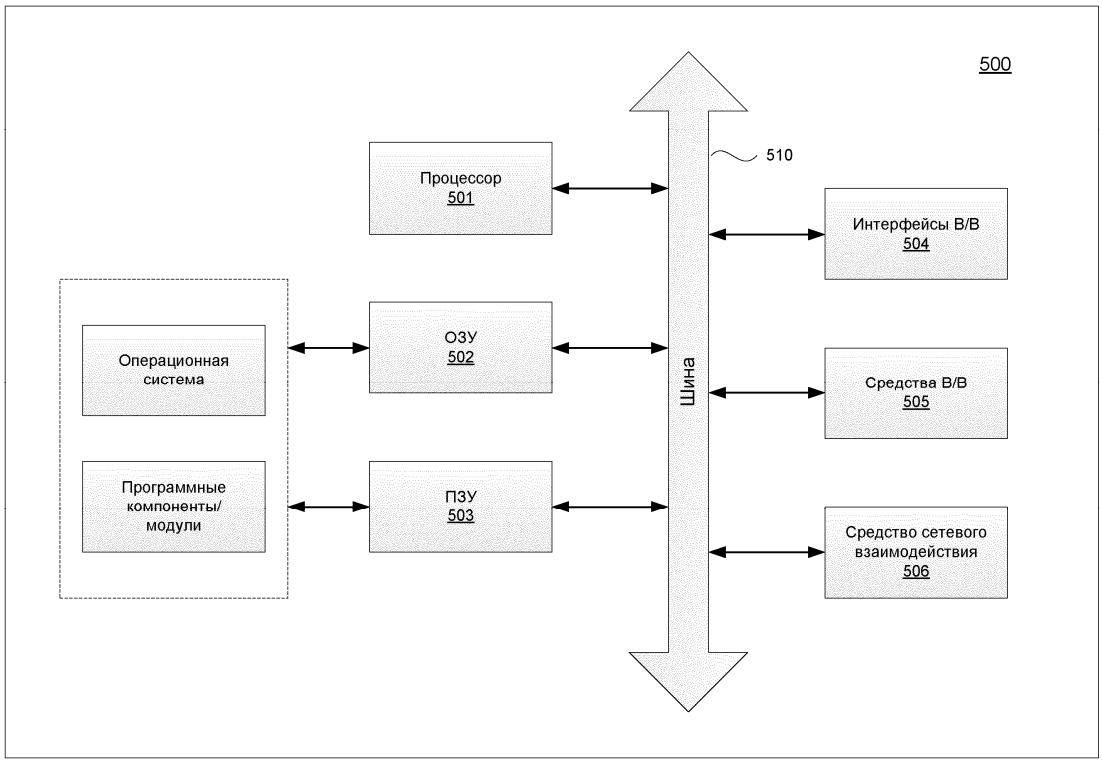
Фиг. 2


400
Получение данных пользовательских действий на веб-ресурсе
401
Анализ данных на наличие соответствующих предложений
402
Нет
Предложение найдено?
403
Да
Передача предложений пользователю
404

Фиг. 3


9:00
Кредитные карты
250
300
15:00
Вклады
250
300
База данных
330
20:00
Кредитные карты
250
300

Фиг. 4


500
510
Процессор
501
Интерфейсы В/В
504
Операционная система
ОЗУ
502
Шина
Средства В/В
505
Программные компоненты/ модули
ПЗУ
503
Средство сетевого взаимодействия
506

Фиг. 5