(19) Евразийское патентное ведомство

(11) 038265 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.07.30

(21) Номер заявки
201892715

(22) Дата подачи заявки
2018.12.21

(51) Int. Cl. ***G06Q 20/00*** (2006.01)
G06Q 40/00 (2006.01)

(54) СПОСОБ И СИСТЕМА ПОИСКА МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ

(31) **2018145342**
(32) **2018.12.20**
(33) **RU**
(43) **2020.06.30**

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

(72) Изобретатель:
Оболенский Иван Александрович, Сысоев Валентин Валерьевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-B2-7249094
EP-B1-2884418
WO-A1-2013158123
US-B2-7769682
US-B1-7562814
US-B1-8856923

(57) Данное техническое решение в общем относится к способам обработки данных с помощью компьютерных систем, а в частности к способу и системе поиска мошеннических транзакций в области кибербезопасности. Техническим результатом является повышение скорости обработки множества транзакционных операций для выявления реквизитов мошеннических транзакционных узлов. Заявленный результат достигается за счет компьютерно-реализуемого способа поиска мошеннических транзакций в котором осуществляют получение транзакционного потока, в котором по меньшей мере часть транзакций характеризует мошеннические действия; формируют на основании полученного потока графовую модель движения транзакций; определяют по меньшей мере два узла графовой модели, характеризующие мошеннические транзакции; определяют для каждого из упомянутых узлов список окрестностей; определяют набор пересечений списка окрестностей каждого из упомянутых узлов; определяют узлы графа, входящие в по меньшей мере одно пересечение списка окрестностей двух узлов; осуществляют построение кратчайшего маршрута на основе минимального количества узлов и ребер между упомянутыми узлами с учетом узлов графа.

038265 B1

038265 B1

Область техники

Данное техническое решение в общем относится к способам обработки данных с помощью компьютерных систем, а в частности, к способу и системе поиска мошеннических транзакций в области кибербезопасности.

Уровень техники

В настоящее время в рамках тенденции развития параллельных вычислений, как в области программирования, так и в области вычислительной техники, имеет смысл оптимизировать имеющиеся алгоритмы под новообразующие условия. Проблема анализа банковских транзакций на предмет выявления сомнительных и/или мошеннических операций заключаются в том, что для эффективной работы необходимо осуществлять большой объем вычислений данных транзакций за небольшой промежуток времени, что повышает вычислительную нагрузку на систему

Из уровня техники известно техническое решение для отображения и анализа транзакционных потоков, в котором для обработки данных применяется принцип построения графовой модели (US 20020156724, патентообладатель: PayPal Inc., дата публикации: 24.10.2002). В данном решении графовая модель применяется для анализа узлов совершения транзакций, чтобы отслеживать движение транзакционных потоков и визуально представлять маршрут их движения с помощью графовой модели. Принцип построения маршрута движения транзакционных потоков также может использоваться для выявления мошеннической активности или определения узлов графа, которые являются сомнительными и подлежат дополнительной проверке вне работы системы. Такой подход строится либо на анализе определенного шаблона поведения движения денежных потоков, либо при привлечении внешнего человеческого фактора для обработки узлов, идентифицированных системой как подозрительные, что является достаточно трудоемкой задачей, которая не позволяет быстро и в автоматизированном режиме выявлять и вносить в черный список для последующей блокировки транзакций мошеннические узлы.

Сущность технического решения

Технической проблемой или задачей, решаемой в данном техническом решении, является анализ данных о транзакциях с помощью графовой модели, что позволяет в кратчайший срок выявлять новые, ранее не промаркированные как "мошеннические" транзакции.

Техническим результатом, достигающимся при решении вышеуказанной технической проблемы, является повышение скорости обработки множества транзакций для выявления идентификаторов мошеннических транзакций.

Дополнительным техническим результатом является повышение точности нахождения идентификаторов мошеннических транзакций, за счет их обнаружения в маршруте выполнения транзакций между двумя и более идентификаторами мошеннических транзакций.

Заявленный результат достигается за счет компьютерно-реализуемого способа поиска мошеннических транзакций, выполняемый с помощью процессора, в котором:

a) осуществляют получение данных о транзакциях, в которых по меньшей мере часть данных относится к мошенническим транзакциям;

b) формируют на основании полученных данных граф, в котором узлами являются данные по транзакциям, а ребрами выполненные транзакции;

c) определяют по меньшей мере два узла графа, относящихся к по меньшей мере одной мошеннической транзакции, причем упомянутые узлы расположены на заданном удалении друг от друга;

d) определяют для каждого из узлов графа, выявленных на этапе c) список окрестностей, в котором каждая из окрестностей представляет собой множество узлов графа, соединенных ребрами и другими узлами с одним из упомянутых узлов, выбранных на этапе c);

e) определяют набор пересечений списка окрестностей каждого из определенных узлов на этапе c), где перечисление окрестностей для одного из двух узлов начинается с ближайшей окрестности к данному узлу, а для другого с самой дальней окрестности, в которую входит противоположный узел;

f) определяют узлы графа, входящие в, по меньшей мере, одно пересечение списка окрестностей двух узлов;

g) осуществляют определение и построение кратчайшего маршрута между упомянутыми узлами, определенными на этапе c), с учетом узлов графа, выявленных на этапе f);

h) идентифицируют узлы, входящие в определенный кратчайший маршрут, для которых в данных по транзакциям нет сведений об их принадлежности к мошенническим;

j) выполняют запись данных о транзакции, соответствующей узлам, определенным на этапе h) в базу данных.

В одном из частных вариантов осуществления способа данные транзакций выбираются из группы: идентификатор устройства, IP адрес, данные геолокации или их сочетания, номер счета, PAN платежной карты, номер телефона, данные плательщика или получателя платежа, или их сочетания.

Заявленное решение также осуществляется с помощью компьютерной системы, которая содержит процессор и память, в которой хранятся машиночитаемые инструкции, выполняемые процессором для осуществления вышеуказанного способа. Предлагаемый подход - является разновидностью двунаправленного поиска, который реализует тенденцию двух вычислительных узлов. Т.е. вычисления проводятся

параллельно, и централизованный вычислительный узел использует только результаты работы объектов двух вызываемых узлов. Как результат - находятся все кратчайшие пути за один цикл работы алгоритма.

Описание чертежей

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

фиг. 1 иллюстрирует блок-схему реализации представленного способа;

фиг. 2-8 иллюстрируют применение обработки данных на основании сформированного графа;

фиг. 9 иллюстрирует пример выполнения способа по реквизитам транзакций;

фиг. 10 иллюстрирует общий вид вычислительного устройства.

Осуществление изобретения

В контексте настоящего описания, если четко не указано иное, "вычислительное устройство" подразумевает под собой устройство, работающее на соответствующем оборудовании, которое способно получать запросы (например, от клиентских устройств) по сети и выполнять эти запросы или инициировать выполнение этих запросов. Оборудование может представлять собой один физический компьютер или одну физическую компьютерную систему, но ни то, ни другое не является обязательным для данной технологии. В контексте настоящей технологии использование выражения "вычислительное устройство" не означает, что каждая задача (например, полученные инструкции или запросы) или какая-либо конкретная задача будет получена, выполнена или инициирована к выполнению одним и тем же устройством (то есть одним и тем же программным обеспечением и/или аппаратным обеспечением); это означает, что любое количество элементов программного обеспечения или аппаратных устройств может быть вовлечено в прием/передачу, выполнение или инициирование выполнения любого запроса или последствия любого запроса, связанного с клиентским устройством, и все это программное и аппаратное обеспечение может являться одним вычислительным устройством или несколькими, оба варианта включены в выражение "по меньшей мере одно вычислительное устройство".

В контексте настоящего описания, если четко не указано иное, термин "база данных" подразумевает под собой любой структурированный набор данных, не зависящий от конкретной структуры, программного обеспечения по управлению базой данных, аппаратного обеспечения компьютера, на котором данные хранятся, используются или иным образом оказываются доступны для использования. База данных может находиться на том же оборудовании, которое выполняет процесс, который сохраняет или использует информацию, хранящуюся в базе данных, или же она может находиться на отдельном оборудовании, например, выделенном сервере или множестве серверов. Дальнейшее описание примера осуществления заявленного технического решения будет представлено в соответствие с отсылками к представленным фигурам чертежей.

Согласно фиг. 1 заявленной способ поиска мошеннических транзакций (100) выполняется с помощью вычислительного устройства, например, сервера, который может быть, как локальным, так и облачным в различных вариантах реализации. Шаг 101: осуществляют получение данных о транзакциях, в которых по меньшей мере часть данных относится к мошенническим транзакциям. На первом шаге (101) осуществляется сбор множества данных по транзакциям. Транзакция - это банковская операция между двумя субъектами, например, между двумя клиентами банка. Данные по транзакциям могут поступать из различных источников информации, например, из внешних платежных систем, POS-терминалов, процессинговых систем и др., а также могут передаваться по любому протоколу передачи данных из стека TCP/IP. Транзакции аккумулируются и хранятся, как правило, в базе данных (БД) вычислительного устройства, например, сервера.

В качестве данных по транзакции могут выступать: идентификатор пользовательского устройства (например, смартфона), IP адрес, данные геолокации, номер счета, PAN платежной карты, номер телефона, данные плательщика или получателя платежа, или их сочетания. Данные по транзакции позволяют точно определить отправителя и получателя денежных средств и содержат в себе дополнительную информацию по маркировке, отражающей принадлежность ее к типам: мошенническая, легитимная.

В части реализации этапа (101) выбираются данные одной или нескольких транзакций, для которых заранее известно, что они содержат данные мошеннических отправителей и/или получателей.

В некоторых вариантах реализации информация о наличии мошеннической транзакции может быть помечена посредством числового или символьного идентификатора (например, 1 - легитимная, 0 - мошенническая). Набор таких транзакций может быть заранее автоматически или в ручном режиме размечен.

Шаг 102: формируют на основании полученных данных граф, в котором узлами являются данные по транзакциям, а ребрами выполненные транзакции.

Следующим шагом является создание графа по транзакциям (102). На фиг. 2 представлен пример построения первичного графа (200), в котором узлами (210) являются данные по транзакции, а ребрами (220) выполненные транзакции. Под выполненной транзакцией имеет в виду непосредственно факт осуществления транзакции (успешный), где ребро помечается заранее выбранным идентификатором.

Граф (200) представляет собой невзвешенный неориентированный граф G:=(V, E), где V - непустое множество узлов (210), а E - непустое множество неупорядоченных ребер (220). Граф (200) строится на

основании данных по транзакциям.

Каждому узлу графа известно множество Nbv={Nb1, Nb2...Nbn} его соседей.

Можно представить множество NB={Nbv1, NbV2..., NbVm} всех соседей каждого узла (210).

Шаг 103: определяют по меньшей мере два узла графа, относящихся к по меньшей мере одной мошеннической транзакции, причем упомянутые узлы расположены на заданном удалении друг от друга.

Как представлено на фиг. 3, далее выбираются по меньшей мере два узла V1 и V2, между которыми необходимо найти кратчайший путь (103) и выявить узлы графа, которые будут указывать на мошеннические одну или несколько транзакций. При выполнении алгоритма поиска (100) для каждого узла V1 и V2 известно, что они характеризуют мошенническую транзакцию или несколько транзакций (например, соответствующими идентификаторами), определенных на этапе (101). Узлы V1 и V2 могут выбираться случайным образом из узлов, для которых известна принадлежность идентифицирующих их данных к мошенническим транзакциям.

Шаг 104: определяют для каждого из узлов графа, выявленных на этапе (103), список окрестностей, в котором каждая из окрестностей представляет собой множество узлов графа, соединенных ребрами и другими узлами с одним из упомянутых узлов, выбранных на этапе (103).

Далее выполняется построение окрестностей для каждого из узлов V1, V2 (104), характеризующих мошеннические транзакции. На данном этапе для каждого из узлов V1 и V2 определяются все окрестности. Окрестность - OKRv представляет собой множество узлов, соединенных ребрами и расположенных на расстоянии N ребер от узла V, OKRv={OKR0, OKR1,... OKRN}, где N - целое число.

На фиг. 4 представлен пример отображения окрестности для узлов V1, V2 (области, пронумерованные от 0 до 5 для каждого из узлов V1, V2). Для каждого из узлов V1, V2 формируется список окрестностей, состоящий из N окрестностей для каждого узла (210), т.е. для каждого узла определяется N окрестностей с равноудалёнными узлами (210) для узлов V1, V2. Таким образом, для каждого из узлов V1 и V2 находятся списки окрестностей OKRV1 и OKRV2.

Шаг 105: определяют набор пересечений списка окрестностей каждого из определенных узлов на этапе (103), где перечисление окрестностей для одного из двух узлов начинается с ближайшей окрестности к данному узлу, а для другого с самой дальней окрестности, в которую входит противоположный узел.

По выявленному списку окрестностей для узлов V1, V2 выполняется поиск пересечений выявленных списков (105) для нахождения индексов вхождений - окрестности для одного узла, например V1, в которую входит противоположный узел - V2. Т.е. во множестве узлов (210) окрестности OKRV1[ItIdV2] существует узел V2, и, соответственно, во множестве узлов (210) окрестности OKRV2[ItIdV1] существует узел V1.

Индекс вхождения - целое число от 0 до n, где n - максимально возможное число окрестностей для данного узла. Индекс представляет собой расстояние, на котором удалено множество узлов (в частном случае один узел) от исследуемого узла. Таким образом, например, во множестве OKRV1[0] = V1, что означает, что узел V1 удален от узла V1 на 0 окрестностей. Индекс вхождения для узла V2 - это индекс, при котором во множестве узлов OKRV1[ItIdV2] существует узел V2. Таким образом, индекс вхождения для узла V1 во множестве OKRV1 равен 0.

Шаг 106: определяют узлы графа, входящие в по меньшей мере одно пересечение списка окрестностей двух узлов.

На следующем шаге определяются индексы вхождения ItIdV2 и ItIdV1 (т.е. узлы графа из пересечений) - индексы окрестностей в OKRV1 и OKRV2, в которые входят узлы V2 и V1 соответственно (106). Причем перечисление окрестностей для выявления индексов для одного из двух узлов идет с ближайшей окрестности к исследуемому узлу, например узлу V1, а для другого узла - V2 с дальней окрестности, в которую входит противоположный узел V1. Определение ближайшей и дальней окрестности выбранного узла (V1 или V2) производится исходя из подсчета количества ребер между исследуемым узлом и окрестностью.

Шаг 107: осуществляют определение и построение кратчайшего маршрута между упомянутыми узлами, определенными на этапе (103), с учетом узлов графа, выявленных на этапе (106).

Далее определяется цепочка путей графа (107). Для этого, например, может выбираться два индекса - один из полученных индексов вхождений ItIdV1 или ItIdV2 и нулевой индекс ZId:=0. Например, поиск цепочки узлов (210) графа (200) будет осуществляться по индексу вхождения ItIdV1. Исходя из этого, алгоритм (100) осуществляет поиск общих узлов OKRV1[ItIdV2] и OKRV2[ZId], постепенно увеличивая значение ItIdV2 и уменьшая ZId: W={{OKRV1[ItIdV2-i]∩OKRV2[ZId+i]}}, где i=0...ItIdV2.

Шаг 108: идентифицируют узлы, входящие в определенный кратчайший маршрут, для которых в данных по транзакциям нет сведений об их принадлежности к мошенническим. После выполнения этапа (107) в результате определяется список узлов W={{V1},{Va...Vb}...{V2}}, который при наложении соседей каждого узла в списке со следующей окрестностью даст наикратчайшие пути - множество транзакций Ways={W[1]∩NbV1,W[2]∩NbW[1]...,V2∩NbW[n-1]}, где n - размер множества узлов W.

Построение кратчайшего маршрута (пути) Ways выполняется на основе минимального количества узлов и ребер между упомянутыми узлами V1, V2 с учетом узлов (210) графа, выявленных при пересече-

нии списков окрестностей на этапе (106).

Шаг 109: выполняют запись данных о транзакции, соответствующей узлам, определенным на этапе (108) в базу данных.

Выявленные мошеннические транзакции в каждом кратчайшем маршруте Ways между минимум двумя узлами графа (200) заносятся в базу данных для последующего предотвращения создания транзакции между этими узлами.

Рассмотрим более детально работу данного способа поиска мошеннических транзакций. На фиг. 5 представлен первый шаг [i=1] работы способа, где созданы множества узлов OKRV1[ItIdV2] и OKRV2[ZId], где ZId:=0. Алгоритм осуществляет добавление узлов во множество узлов W, которые одновременно присутствуют как во множестве узлов OKRV1[ItIdV2], так и во множестве узлов OKRV2[ZId], иными словами W=+OKRV1[ItIdV2-i]∩OKRV2[ZId+i], где i - шаг алгоритма. В данном случае общим для двух множеств будет узел V1.

Далее на фиг. 6 представлен результат получения второй окрестности - полученной в результате декрементирования ItIdV1 и инкрементирования ZId, где получается два множества узлов OKRV1[ItIdV2-1] и OKRV2[ZId+1]. На фиг. 6 видно, что в список узлов анализируемого пути W (фиолетовые узлы на фиг. 6) от узла V1 до узла V2 попадают два узла - V1 и Va. Узел V1 попал в этот список по результату работы предыдущего шага, отображенного на фиг. 5. Узел Va одновременно входит в множество окрестностей как OKRV1[ItIdV2-1], так и OKRV2[ZId+1], то есть он является общим и соответственно добавляется в список W.

После этого осуществляется добавление в W узлов пересечения окрестностей, представленной на фиг. 7. В данном случае это узел Va. Вышеописанный алгоритм повторяется ItIdV2 раз, что позволяет получить узлы W, общие в каждой окрестности. При соединении соседей для каждого узла из W определяется кратчайший маршрут Ways из V1 в V2, представленный на фиг. 8, на основе минимального количества ребер в каждом из маршрутов.

В результате работы способа поиска мошеннических транзакций (100) определяются все кратчайшие пути в невзвешенном неориентированном графе транзакций, что позволяет выявлять мошеннические узлы между известными узлами (V1, V2), о которых ранее не было информации, путем перебора всех транзакций от одного мошеннического узла до другого, и любой транзитный узел в такой цепочке будет считаться мошенническим (этап 108), при условии, что по таким узлам ранее не было сведений о маркировке данных транзакций, соответствующих выявленным узлам (210) в кратчайшем маршруте, как относящихся к мошенническим.

Выявление мошеннических транзакций с помощью представленного способа (100) можно рассмотреть на следующем примере, представленном на фиг. 9. Выполняется получение данных по транзакциям между субъектами, характеризующимися реквизитами и атрибутами транзакций. Реквизиты и атрибуты транзакций представляют собой в частном случае идентификаторы транзакций, по которым можно определить отправителя и получателя транзакции, т.е. узлы, между которыми произошел денежный перевод. В рассматриваемом примере реквизиты выбираются из группы: номер счета, PAN платежной карты, номер телефона, данные плательщика или получателя платежа, или их сочетания, а атрибуты из группы: идентификатор устройства (например, смартфон), IP адрес, данные геолокации или их сочетания. Далее выполняется маркировка транзакций, для которых известно, что они являются мошенническими.

Реквизит #1 осуществил перевод Реквизит #2, с использованием Атрибут #1 - транзакция с типом мошенническая.

Реквизит #2 осуществил перевод Реквизит #3, с использованием Атрибут #23

Реквизит #3 осуществил перевод Реквизит #4, с использованием Атрибут #23

Реквизит #3 осуществил перевод Реквизит #5, с использованием Атрибут #23

Реквизит #5 осуществил перевод Реквизит #6 с использованием Атрибут #45 - транзакция с типом мошенническая.

Реквизит #1 и Реквизит #6 являются мошенническими, алгоритм на основе анализа кратчайших путей между этими узлами графа выделяет как транзитные мошеннические реквизиты: Реквизит #2, Реквизит #3, Реквизит #5, Атрибут #23, о которых ранее не было данных об их использовании в мошеннической схеме между данными узлами. Таким образом узлы с реквизитами: Реквизит #2, Реквизит #3, Реквизит #5, Атрибут #23, добавляются в базу данных как участвующие в мошеннической схеме.

Выявленные узлы графа (200) с соответствующими идентификаторами, которые попали в кратчайший маршрут между первично маркированными мошенническими узлами, заносятся в базу данных для дальнейшего использования для блокировки транзакций по выявленным мошенническим идентификаторам.

Как пример, идентификаторы транзакций, выявленные в ходе выполнения способа (100), могут заноситься в черный список или передаваться службам финансового контроля, подразделениям кибербезопасности и т.п., чтобы в случае определения платежной системой получения/отправки средств на идентификаторы узла, отправляющего/принимающего транзакцию и содержащего идентификационные данные, внесенные в черный список, происходила своевременная блокировка выполнения финансовых операций.

На фиг. 10 представлен пример общего вида вычислительного устройства (300), которое обеспечивает реализацию заявленного способа или является частью компьютерной системы, например, сервером, обрабатывающим необходимые данные для осуществления заявленного способа (100).

В общем случае, вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305), и устройство для сетевого взаимодействия (306).

Процессор (301) (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. Под процессором также необходимо учитывать графический процессор, например GPU NVIDIA или ATI, который также является пригодным для полного или частичного выполнения способа (100). При этом средством памяти может выступать доступный объем памяти графической карты или графического процессора. ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (303) 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 (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). 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 (300) применяются различные средства (305) 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 (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) 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 в составе устройства (300), 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 поиска мошеннических транзакций, выполняемый с помощью процессора, включающий следующие шаги:

a) осуществляют получение данных о транзакциях, в которых по меньшей мере часть данных относится к мошенническим транзакциям;

b) формируют на основании полученных данных граф, в котором узлами являются данные по транзакциям, а ребрами выполненные транзакции;

c) определяют случайным образом из узлов, для которых известна принадлежность идентифицирующих их данных к мошенническим транзакциям, по меньшей мере два узла графа, относящихся к по меньшей мере одной мошеннической транзакции, причем упомянутые узлы расположены на заданном удалении друг от друга;

d) определяют для каждого из узлов графа, выявленных на этапе c), список окрестностей, в котором каждая из окрестностей представляет собой множество узлов графа, соединенных ребрами и другими узлами с одним из упомянутых узлов, выбранных на этапе c);

e) определяют набор пересечений списка окрестностей каждого из определенных узлов на этапе c), на основе индекса вхождения, где индекс вхождения представляет собой, по меньшей мере, окрестности для одного узла, в которую входит противоположный узел, при этом перечисление окрестностей для одного из двух узлов начинается с ближайшей окрестности к данному узлу, а для другого с самой дальней окрестности, в которую входит противоположный узел;

f) определяют узлы графа, входящие в по меньшей мере одно пересечение списка окрестностей двух узлов;

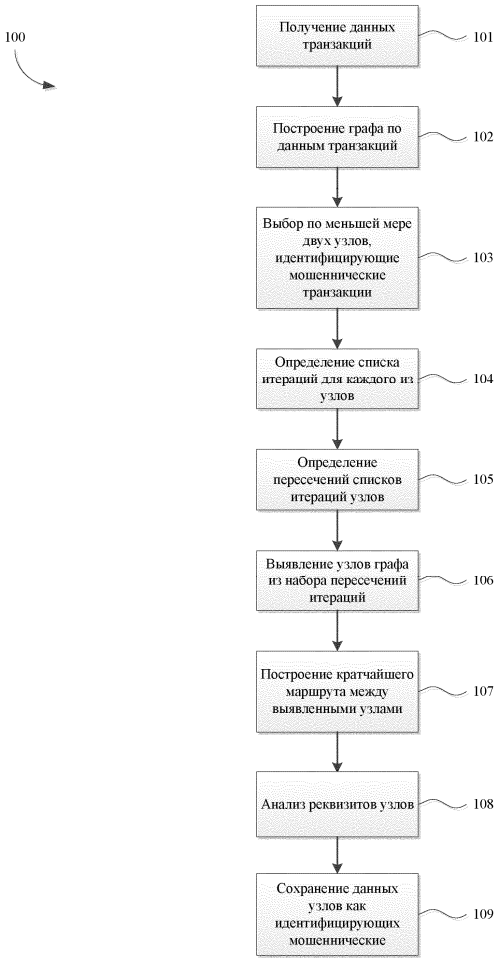
g) осуществляют определение и построение кратчайшего маршрута между упомянутыми узлами, определенными на этапе c), на основе минимального количества узлов и ребер между упомянутыми узлами с учетом узлов графа, выявленных на этапе f);

h) идентифицируют узлы, входящие в определенный кратчайший маршрут, для которых в данных по транзакциям нет сведений об их принадлежности к мошенническим;

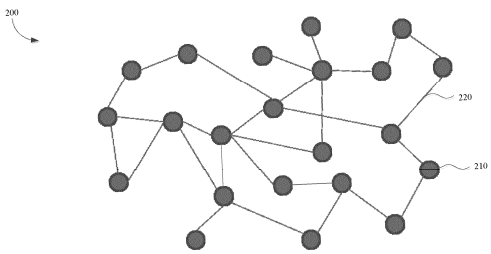
j) выполняют запись данных о транзакции, соответствующей узлам, определенным на этапе h), в базу данных.

2. Способ по п.1, характеризующийся тем, что данные по транзакции выбираются из группы: идентификатор устройства и/или IP адрес, и/или данные геолокации совершения транзакции, и/или номер счета, и/или PAN платежной карты, и/или номер телефона плательщика, и/или данные плательщика или получателя платежа, или их сочетания.

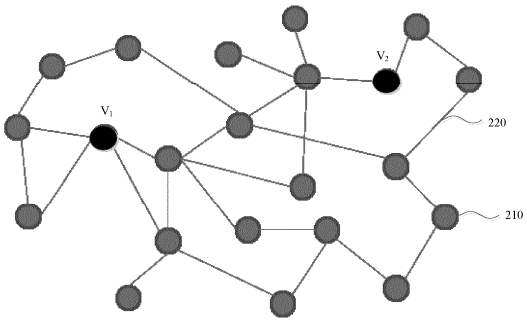
3. Система поиска мошеннических транзакций, содержащая по меньшей мере один процессор и по меньшей мере одну память, содержащую машиночитаемые инструкции, которые при их выполнении с помощью процессора осуществляют способ по любому из пп.1, 2.



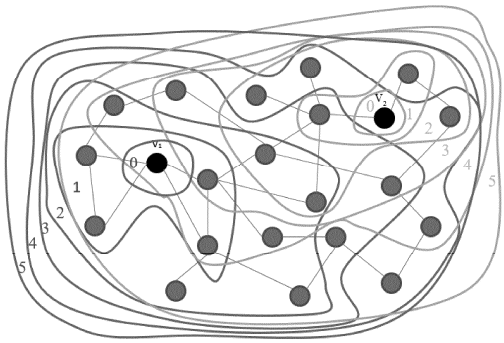
Фиг. 1



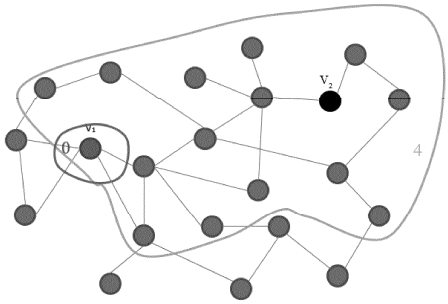
Фиг. 2



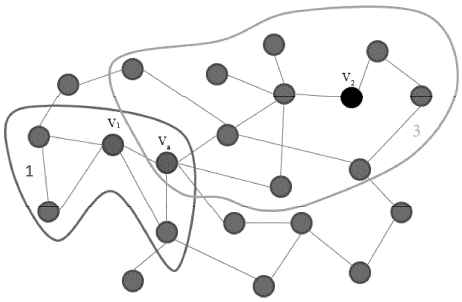
Фиг. 3



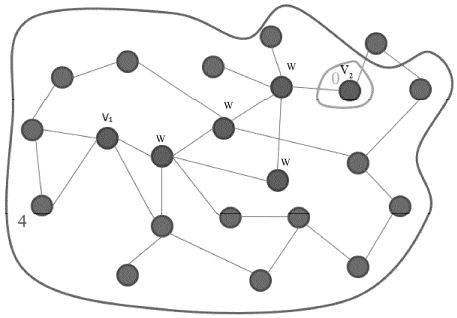
Фиг. 4



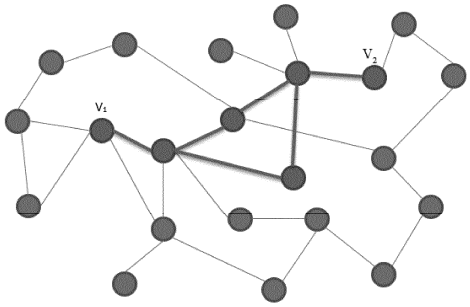
Фиг. 5



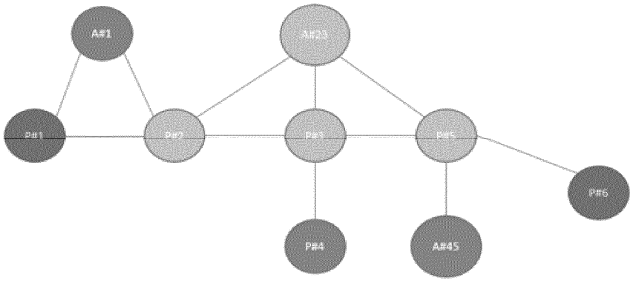
Фиг. 6



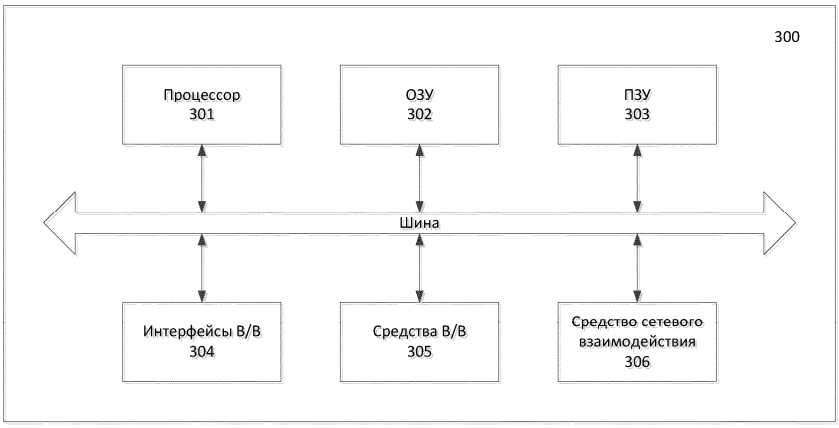
Фиг. 7



Фиг. 8



Фиг. 9



Фиг. 10