(19) Евразийское патентное ведомство

(21) 202293481 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2023.08.31

(22) Дата подачи заявки
2022.12.26

(51) Int. Cl. ***G06F 21/30*** (2013.01)
G06F 21/73 (2013.01)
G06Q 20/08 (2012.01)

(54) СПОСОБ И УСТРОЙСТВО ФОРМИРОВАНИЯ СТАТИЧНОГО ИДЕНТИФИКАТОРА МОБИЛЬНЫХ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОС ANDROID, СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ПОМОЩЬЮ СТАТИЧНОГО ИДЕНТИФИКАТОРА

(31) **2022102770**
(32) **2022.02.04**
(33) **RU**

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

(72) Изобретатель:
Оболенский Иван Александрович, Губанов Дмитрий Николаевич, Широков Артём Александрович, Денисенко Максим Геннадиевич, Якушев Владимир Владимирович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области компьютерной техники, в частности к методам формирования идентификаторов устройств для их применения в области защиты информации. Техническим результатом является повышение точности идентификации мобильных устройств, за счет формирования статичного идентификатора. Заявленное изобретение осуществляется с помощью способа формирования статичного идентификатора мобильных устройств под управлением ОС Android, содержащего этапы, на которых с помощью процессора мобильного устройства устанавливают платежное приложение в ОС мобильного устройства; осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля и, по меньшей мере, данные марки мобильного устройства; осуществляют хэширование полученного набора параметров с помощью алгоритма кусочного хэширования, инициированного контекстом, и алгоритма блочного восстановления, при это хэширование параметров каждым из алгоритмов выполняется параллельно; формируют статичный идентификатор мобильного устройства на основании выполненного хэширования; связывают полученный идентификатор с платежным приложением конкретного пользователя; передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

202293481 A1

202293481 A1

202293481 A1

202293481 A1

СПОСОБ И УСТРОЙСТВО ФОРМИРОВАНИЯ СТАТИЧНОГО ИДЕНТИФИКАТОРА МОБИЛЬНЫХ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОС ANDROID, СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ПОМОЩЬЮ СТАТИЧНОГО ИДЕНТИФИКАТОРА

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное решение относится к области компьютерной техники, в частности к методам формирования идентификаторов устройств для их применения в области защиты информации.

УРОВЕНЬ ТЕХНИКИ

[0002] В настоящее время применение мобильный приложений для получения финансовых услуг является широко используемым способом взаимодействия пользователей с банками. Однако с массовым распространением получения услуг в цифровом формате возросло также и количество мошеннической активности, направленной на хищение средств пользователей, что обуславливает необходимость разработки новых средств защиты пользователей от действий мошенников.

[0003] Особенно критичной данная проблема является для мобильных устройств под управлением ОСAndroid. Банковское мобильное приложение предоставляет возможность получать идентификатор мобильного устройства и передавать его в информационные системы банка. Данная возможность по умолчанию предоставляется всем приложениям, установленным на мобильном устройстве. На основе этого идентификатора банк осуществляет дополнительную верификацию клиента при совершении транзакций и при наличии расхождений в идентификаторах клиента, может приостановить, либо отклонить транзакцию, как подозрительную.

[0004] Операционная система (далее – ОС) Android начиная с 10 версии и выше, в целях повышения конфиденциальности пользователей мобильных устройств ограничила доступ к не сбрасываемым (статичным) идентификаторам устройств, в том числе для приложений, установленных и работающих на устройстве. При сбросе устройства до заводских настроек, идентификатор, доступный установленным на устройстве приложениям, изменяется. Таким образом, однозначная идентификация клиентского мобильного устройства на стороне банка не представляется возможной.

[0005] Злоумышленники, используя различные методики воздействия на клиентов банка, в том числе социальную инженерию, могут получить доступ к критическим данным клиентов, затем эти данные могут быть использованы для установки банковских

приложений на устройстве злоумышленника с дальнейшей регистрацией его в банке. Злоумышленник после регистрации такого приложения на своем устройстве от имени клиента получает доступ к денежным средствам клиента и далее предпринимает попытки хищения этих средств.

[0006] Существуют подходы в части формирования комплексных ID устройств (патентная заявка US 20140164178 A1, 12.06.2014), при которых ID формируется на основании существующей информации о регистрационных данных пользователя различных аккаунтов, позволяя тем самым сформировать более уникальный ID для применения в целях аутентификации.

[0007] Существенной проблемой существующих подходов является ключевое использование цифровой информации и базовых аппаратных номеров мобильных устройств, например, IMEI, серийный номер и т.п. Эти данные достаточно уязвимы и не позволяет формировать на их основании статичный идентификатора, который не будет существенно изменяться при заводском сбросе устройств, также, начиная с 10й версии ОС Android, такого рода данные не доступны мобильным приложениям.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0008] Заявленное изобретение позволяет решить техническую проблему в части создания нового робастного и устойчивого идентификатора мобильного устройства для последующего его применения для отслеживания мошеннической активности.

[0009] Техническим результатом является повышение точности идентификации мобильных устройств, за счет формирования статичного идентификатора.

[0010] Заявленное решение осуществляется с помощью способа формирования статичного идентификатора мобильных устройств под управлением ОС Android, содержащего этапы, на которых с помощью процессора мобильного устройства:

устанавливают платежное приложение в ОС мобильного устройства;

осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства;

осуществляют хэширование полученного набора параметров с помощью алгоритма кусочного хэширования, инициированного контекстом, и алгоритма блочного восстановления, при это хэширование параметров каждым из алгоритмов выполняется параллельно;

формируют статичный идентификатор мобильного устройства на основании выполненного хэширования;

связывают полученный идентификатор с платежным приложением конкретного пользователя;

передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

[0011] В одном из частных примеров осуществления способа параметры процессора включают по меньшей мере одно из: количество ядер процессора, частота процессора, модель процессора, название ядра, архитектура ядра, поддерживаемая архитектура.

[0012] В другом частном примере осуществления способа параметры модуля камеры включают по меньшей мере одно из: размер сенсора камеры, фокальное расстояние камеры, горизонтальный угол отстройки камеры, вертикальный угол отстройки камеры, максимальная продолжительность кадра.

[0013] В другом частном примере осуществления способа параметры модуля памяти включают по меньшей мере одно из: общий объем физической оперативной памяти, общий объем доступного свопа, общий объем памяти от общего выделенного виртуального адресного пространства.

[0014] В другом частном примере осуществления способа параметры радиомодуля включают по меньшей мере одно из: идентификатор DRM-схемы, версия прошивки радиомодуля, данные базовой платы.

[0015] В другом частном примере осуществления способа параметры дополнительно включают по меньшей мере одно из: параметр проверки диапазона процессора, номер списка изменений, данные производителя, название мобильного устройства, название промышленного образца, разрешение экрана, строка идентификатора сборки.

[0016] Заявленное решение также осуществляется с помощью способа выявления мошеннических транзакций, осуществляемых с помощью мобильных устройств, при этом способ содержит этапы, на которых:

с помощью АСФМ:

фиксируют регистрацию платежного приложения на мобильном устройстве;

формируют статичный идентификатор мобильного устройства вышеуказанным способом;

связывают полученный идентификатор с регистрационными данными пользователя платежного приложения;

фиксируют выполнение транзакции посредством платежного приложения;

получают данные о совершении мошеннической транзакции посредством упомянутого платежного приложения;

вносят в черный список по меньшей мере полученный статичный идентификатор мобильного устройства;

блокируют работу платежного приложения на мобильном устройстве, содержащем идентификатор, внесенный в черный список.

[0017] В одном из частных примеров реализации способа фиксируют реквизиты счетов, на которые была осуществлена мошенническая транзакция.

[0018] В другом частном примере реализации способа выполняется внесение реквизитов счетов в черный список для последующих блокировок транзакций.

[0019] Заявленное решение также реализуется с помощью устройства формирования статичного идентификатора мобильных устройств под управлением ОС Android, которое содержит по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют вышеуказанный способ формирования статичного идентификатора.

[0020] Заявленное решение также реализуется с помощью системы выявления мошеннических транзакций, которая содержит по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют вышеописанный способ отслеживания мошеннических транзакций.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0021] Фиг. 1 иллюстрирует блок-схему способа формирования статичного идентификатора.

[0022] Фиг. 2 иллюстрирует блок-схему способа отслеживания мошеннических транзакций с помощью статичного идентификатора.

[0023] Фиг. 3 иллюстрирует схему вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0024] На Фиг. 1 представлена блок-схема выполнения этапов способа (100) формирования статичного идентификатора. Заявленное решение выполняется при установке платежного приложения на этапе (101) в ОС мобильного устройства. Под

термином «мобильное устройство» в рамках заявленного решения может пониматься смартфон, фаблет или планшет под управлением ОС Android.

[0025] После установки платежного приложения, например, Сбербанк Онлайн, программная логика приложения запрашивает данные для последующей регистрации пользователя. Такими данными могут являться, ФИО, паспортные данные, номер платежной карты, номер телефона, логин/пароль для входа в приложение и т.п. Дополнительно может применяться биометрическая информация. После успешной регистрации для каждого пользователя создается уникальная запись под соответствующим идентификатором, которая сохраняется на сервере в единой базе данных.

[0026] После регистрации в приложении на этапе (102) осуществляется сбор данных мобильного устройства. Сбор осуществляется посредством программной логики платежного приложения, имеющего доступ к ОС мобильного устройства. В рамках осуществления настоящего этапа осуществляется сбор следующих параметров: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства.

[0027] Данные мобильного устройства собираются по основным аппаратным модулям (процессор, память, камера, радиомодуль), а также системные данные, идентифицирующие само устройство.

[0028] Параметры процессора могут выбираться из следующих данных, представленных в Таблице 1.

Таблица 1. Параметры процессора

CPU_CORES	Количество ядер процессора
CPU_MHZ	Частота процессора
MODEL_NAME	Модель процессора
CPU_FAMILY	Название семейства процессора
KERNEL_OS_NAME	Название ядра
KERNEL_OS_ARCH	Архитектура ядра
CPU_ABI	Поддерживаемая архитектура
CPU_ABI2	Поддерживаемая архитектура

[0029] Пример используемых параметров модуля камеры приведены в Таблице 2.

Таблица 2. Параметры камеры

CAMERA_SENSOR_SIZE	Размер сенсора камеры
CAMERA_0_FOCAL_LENGTH	Фокальное расстояние камеры

CAMERA_0_HORIZONTAL_ANGLE	Горизонтальный угол отстройки камеры
CAMERA_0_VERTICAL_ANGLE	Вертикальный угол отстройки камеры
MAX_FRAME_DURATION	Максимальная продолжительность кадра

[0030] Параметры модуля памяти могут включать в себя параметры, указанные в Таблице 3.

Таблица 3. Параметры модуля памяти

MEMTOTAL	Общий объем физической оперативной памяти
SWAPTOTAL	Общий объем доступного свопа («Своп» - файл\раздел подкачки операционной системы предназначенный для повышения быстродействия и оптимизации использования приложений на мобильном устройстве).
VMALLOCTOTAL	Общий объем памяти от общего выделенного виртуального адресного пространства

[0031] Пример используемых параметров радиомодуля приведен в Таблице 4.

Таблица 4. Параметры радиомодуля

WIDEVINE_UUID_SYSTEM_ID	Идентификатор DRM-схемы
RADIO_VERSION	Версия прошивки радио модуля
HARDWARE	Название оборудования (из командной строки ядра)
BOARD	Название базовой платы

[0032] Также дополнительно для формирования идентификатора используются системные параметры, приведенные в Таблице 5.

Таблица 5. Системные параметры

BOGOMIPS	Параметр проверки диапазона процессора
OUTPUT_SIZES	Разрешение экрана
MANUFACTURER	Название производителя

MODEL	Название мобильного устройства, видимое пользователю устройства
DEVICE	Название промышленного образца (заводское наименование марки и модельного ряда мобильных устройств)
ID	Номер списка изменений, либо метка типа «M4-rc20»
DISPLAY	Строка идентификатора сборки
BRAND	Название бренда производителя устройства

[0033] По факту сбора требуемого набора вышеуказанных параметров, на этапе (103) осуществляется их последующее хэширование. ОС Android позволяет получать данные параметры без дополнительных разрешений со стороны владельца мобильного устройства.

[0034] Данный список параметров позволяет добиться:

- уникальности получаемых идентификаторов, даже на одинаковых устройствах одного производителя;
- неизменности идентификатора на любом устройстве, даже при минорных и мажорных обновлениях ОС Android;
- воспроизводимости (повторяемость результатов) идентификатора при различных типах сбросов мобильного устройства до заводских и последующих восстановлений устройства.

[0035] В зависимости от типа решаемых задач идентификатор, получаемый на вышеописанных параметрах, может быть статическим и\или вероятностным, это достигается за счёт использования различных алгоритмов преобразования данных. В настоящем решении используется комбинация криптографических алгоритмов хэширования и методов нечеткого хэширования (хэш-функции с сохранением сходства). Это сделано для минимизации возможных дальнейших ограничений по сбору системных параметров со стороны ОС Android, а также любых других изменений, которые могут возникнуть с системными параметрами мобильного устройства во время эксплуатации (например, аппаратная замена камеры или процессора в устройстве).

[0036] На этапе (103) применяются две модифицированные хэш-функции с сохранением сходства (подобия): ssdeep [1] и SimHash [2]. Исходно данные алгоритмы были разработаны для задач компьютерной криминалистики, а именно: ускорение и

автоматизация аналитики содержимого конкретного электронного документа, а также формализация и представление полученных доказательств в суде. Ssdeep относится к алгоритмам кусочного хэширования, инициированного контекстом, то есть во время хэширования создается хэш для нескольких дискретных сегментов данных, размер и количество которых определяются алгоритмически на основе контекста хэшируемых данных. SimHash является алгоритмом блочного восстановления и позволяет определить разницу расстояний между идентификаторами, вычислив расстояние Хэмминга, либо расстояние Дамерау-Левенштейна, либо XOR вектор. Путем дополнительного сравнения полученных числовых характеристик расстояний, можно выбирать как минимальное значение, что будет означать, что полученные идентификаторы могут относиться к одному устройству, так и максимальные значения, что будет говорить, о том, что это идентификаторы разных устройств.

[0037] Суть модификации алгоритмов, используемых в заявленном решении, заключается в фиксированных положениях дискретизации (сегментации) получаемой последовательности параметров на пять блоков, которые характеризуют основные системные модули мобильного устройства (процессор, камера, память, радиомодуль, системные данные), что позволяет алгоритмам ssdeep и SimHash производить расчет независимо от размеров и наличия строк каждого из системных параметров. Например, при замене камеры на устройстве, изменится идентификатор мобильного устройства, но благодаря алгоритмам хэширования с сохранением подобия можно определить наиболее вероятный (близкий) идентификатор, который был у устройства ранее, а также из-за фиксированных положений дискретизации определить модуль, в котором произошли изменения, аналогично при возможных ограничениях по сбору системных параметров со стороны ОС Android. Применение сразу двух алгоритмов хэширования независимо друг от друга также обусловлено повышением точности выявления вероятных идентификаторов и снижением ложноположительных срабатываний при целенаправленных атаках злоумышленников на алгоритмы [3].

[0038] На этапе (104) по итогу применения функций хэширования формируется статичный идентификатор мобильного устройства. Идентификатор может иметь следующий вид:
Wj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wMwAxSx0Wn:C3+zD3sl0XsjJOc:C3FzD3sl0XsjJOcWj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wlCY0Sx0Wn:C1fpwOcWj68LioBPZCiqyrGGJn1fVxv.

[0039] Сформированный статичный идентификатор связывается с регистрационными данными пользователя, введенными в платежное приложение, и на этапе (105) передаются

в базу данных на сервер. Периодичность формирования и передачи идентификаторов мобильных устройств на сервер может варьироваться в зависимости от целей и задач организации (единоразово, событийно, либо по расписанию). Полученные идентификаторы аккумулируются в автоматизированных системах организации и позволяют проводить идентификацию клиентских мобильных устройств при работе с приложением.

[0040] При выявлении аномалий (изменений) в идентификаторах клиента, банк может приостановить, либо отклонить транзакцию, как подозрительную, тем самым предотвратив возможное мошенничество (хищение денежных средств, либо имущества) в отношении клиента банка.

[0041] Уникальность заявленного подхода заключается в формировании идентификатора, одновременно сочетающего в себе несколько свойств:

- Статичность – устойчивый к изменениям в ОС на мобильных устройствах и не требующих дополнительных разрешений для мобильного платежного приложения.
- Вероятностная устойчивость - в случае изменения подхода разработчиков ОС для мобильных устройств остаются доступные характеристики, необходимые для формирования идентификатора.

[0042] Сформированная на этапе (105) информация, записанная на сервере банка, передается на этапе (106) на сервер автоматизированной системы фрод-мониторинга (АСФМ). Автоматизированная система фрод-мониторинга банка анализирует и выявляет аномалии в транзакционном потоке клиентов, помещая идентификаторы мобильных устройств злоумышленников в «чёрные» списки, тем самым предотвращая дальнейшие установки и регистрации платежных приложений на устройствах злоумышленников.

[0043] На Фиг. 2 представлен пример работы способа (200) отслеживания мошеннических транзакций с помощью вышеописанного метода формирования статичного идентификатора. На первом этапе (201) АСФМ фиксирует получение сведений об осуществлении первой транзакции с помощью мобильного устройства с установленным платежным приложением, для которого уже имеется запись на сервере банка о регистрационных данных клиента и соответствующего статичного идентификатора мобильного устройства.

[0044] По факту совершенной транзакции, ее первичный статус неизвестен, и она, как правило, обрабатывается банком. Однако, при поступлении информации о том, что транзакция носила мошеннический характер (этап 202), то соответствующая запись делается в АСФМ, и для сформированного статичного идентификатора мобильного устройства, с которого была выполнена данная транзакция, формируется запись о внесении его в черный список (этап 203).

[0045] Такая ситуация может произойти в случае хищения данных клиента и их использования мошенником для регистрации платёжного приложения на своем мобильном устройстве.

[0046] При факте осуществления последующего совершения транзакции (этап 205) АСФМ осуществляет проверки соответствующего статичного идентификатора на предмет его наличия в черном списке.

[0047] Рассмотрим пример сравнения статичных идентификаторов.

[0048] Статичный идентификатор первого устройства получен по следующим параметрам:

BOARD : COL

BRAND : HONOR

DISPLAY : COL-L29 10.0.0.177(C10E4R1P4)

CPU_ABI : armeabi-v7a/armeabi

CPU_ABI2 : arm64-v8a

RADIO_VERSION : 21C20B369S009C000,21C20B369S009C000

HARDWARE : Hisilicon Kirin970

ID : HUAWEICOL-L29

MANUFACTURER : HUAWEI

MODEL : COL-L29

DEVICE : HWCOL

OUTPUT_SIZES : 176x144

HIGH_SPEED_SIZES : 1920x1080

MAX_FRAME_DURATION : 9000000000

CAMERA_SENSOR_SIZE : 5.16/3.87

CAMERA_0_FOCAL_LENGTH : 3.95

CAMERA_0_HORIZONTAL_ANGLE : 66.302284

CAMERA_0_VERTICAL_ANGLE : 52.19801

KERNEL_OS_NAME : Linux

KERNEL_OS_ARCH : aarch64

BOGOMIPS : 3.84

CPU_ARCHITECTURE : 8

CPU_VARIANT : 0x0

CPU_PART : 0xd09

CPU_REVISION : 2

MEMTOTAL : 3714672 kB

SWAPTOTAL : 2293756 kB

COMMITLIMIT : 4151092 kB

VMALLOCTOTAL : 263061440 kB

WIDEVINE_UUID_SYSTEM_ID : 7893

И имеет вид:

Wj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wMwAxSx0Wn:C3+zD3sl0XsjJOc:C3FzD3sl0XsjJOcWj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wlCY0Sx0Wn:C1fpwOcWj68LioBPZCiqyrGGJn1fVxv.

[0049] Статичный идентификатор второго устройства получен по следующим параметрам:

BOARD : COL

BRAND : HONOR

DISPLAY : COL-L29 10.0.0.177(C10E4R1P4)

CPU_ABI : armeabi-v7a/armeabi

CPU_ABI2 : arm64-v8a

RADIO_VERSION : 21C20B369S009C000,21C20B369S009C000

HARDWARE : Hisilicon Kirin970

ID : HUAWEICOL-L29

MANUFACTURER : HUAWEI

MODEL : COL-L29

DEVICE : HWCOL

OUTPUT_SIZES : 176x144

HIGH_SPEED_SIZES : 1920x1080

MAX_FRAME_DURATION : 9000000000

CAMERA_SENSOR_SIZE : 5.16/3.87

CAMERA_0_FOCAL_LENGTH : 3.95

CAMERA_0_HORIZONTAL_ANGLE : 66.302284

CAMERA_0_VERTICAL_ANGLE : 52.19801

KERNEL_OS_NAME : Linux

KERNEL_OS_ARCH : aarch64

BOGOMIPS : 3.84

CPU_ARCHITECTURE : 8

CPU_VARIANT : 0x0

CPU_PART : 0xd09

CPU_REVISION : 2

MEMTOTAL : 3714673 kB

SWAPTOTAL : 2293757 kB

COMMITLIMIT : 4151092 kB

VMALLOCTOTAL : 263061440 kB

WIDEVINE_UUID_SYSTEM_ID : 7893

И имеет вид:

Wj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wMwAxSx0Wn:C3+zD3sl0XsjJOc:C3FzD3sl0XsjJOcWj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wlCY0Sx0Wn:C1fpwOcWj68LioBPZCiqyrGGJn1UdAxv.

[0050] У обоих примеров устройств все параметры одинаковы, кроме MEMTOTAL и SWAPTOTAL (отличаются на 1 Кб), соответственно базовые идентификаторы у них получаются разные: 2be8b842-7c80-4480-8158-d62a3104bf53 и ee5ebc7f-5b65-41ec-87df-75b74301786f.

При сравнении статичных идентификаторов с помощью алгоритма ssdeep становится ясно, что с вероятностью 99% это идентификатор одного и того же устройства.

При этом, если фиксируется появление нового идентификатора у одного и того же пользователя, но при этом статичный идентификатор говорит о том, что новый идентификатор очень похож на предыдущий, то это позволяет дополнительно учитывать такие изменения в системе фрод-мониторинга и более быстро реагировать на возможные попытки мошеннической активности.

[0051] На этапе (206) по факту выполненной проверки АСФМ принимается решение о блокировке или одобрению транзакции. В случае ее блокировки и расценивании действий как мошеннических на сервере банка выполняется определение также транзакционных реквизитов мошенников, на основании информации о совершенной транзакции, что позволяет как эффективно блокировать последующие установки платежных приложений (при сравнении статичного идентификатора с ранее внесенным в черный список), так и мошеннических реквизитов для предотвращения поступления на них средств.

[0052] На Фиг. 3 представлен общий вид вычислительной системы, реализованной на базе вычислительного устройства (300). 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).

[0053] 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.

[0054] 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.).

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0060] 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.

Источники информации:

[1] Kornblum, J "Identifying almost identical files using context trigger piecewise hashing," Digital Investigation, vol. 3(S1), pp. 91–97, 2006

[2] C. Sadowsky and G. Levin, "Simhash: Hash-based similarity detection," Tech. Rep., 2007. [Online]. Available: http://simhash. googlecode.com/svn/trunk/paper/SimHashWithBib.pdf

[3] H. Baier and F. Breitinger, "Security aspects of piecewise hashing in computer forensics," in Sixth International Conference on IT Security Incident Management and IT Forensics (IMF 2001), 2011, pp. 21–36.

ФОРМУЛА

1. Способ формирования статичного идентификатора мобильных устройств под управлением ОС Android, содержащий этапы, на которых с помощью процессора мобильного устройства:

устанавливают платежное приложение в ОС мобильного устройства;

осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства;

осуществляют хэширование полученного набора параметров с помощью алгоритма кусочного хэширования, инициированного контекстом, и алгоритма блочного восстановления, при это хэширование параметров каждым из алгоритмов выполняется параллельно;

формируют статичный идентификатор мобильного устройства на основании выполненного хэширования;

связывают полученный идентификатор с платежным приложением конкретного пользователя;

передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

2. Способ по п.1, характеризующийся тем, что параметры процессора включают по меньшей мере одно из: количество ядер процессора, частота процессора, модель процессора, название ядра, архитектура ядра, поддерживаемая архитектура.

3. Способ по п.1, характеризующийся тем, что параметры модуля камеры включают по меньшей мере одно из: размер сенсора камеры, фокальное расстояние камеры, горизонтальный угол отстройки камеры, вертикальный угол отстройки камеры, максимальная продолжительность кадра.

4. Способ по п.1, характеризующийся тем, что параметры модуля памяти включают по меньшей мере одно из: общий объем физической оперативной памяти, общий объем доступного свопа, общий объем памяти от общего выделенного виртуального адресного пространства.

5. Способ по п.1, характеризующийся тем, что параметры радиомодуля включают по меньшей мере одно из: идентификатор DRM-схемы, версия прошивки радиомодуля, данные базовой платы.

6. Способ по п.1, характеризующийся тем, что параметры дополнительно включают по меньшей мере одно из: параметр проверки диапазона процессора, номер списка изменений, данные производителя, название мобильного устройства, название промышленного образца, разрешение экрана, строка идентификатора сборки.

7. Способ выявления мошеннических транзакций, осуществляемых с помощью мобильных устройств, при этом способ содержит этапы, на которых:

с помощью АСФМ:

фиксируют регистрацию платежного приложения на мобильном устройстве;

формируют статичный идентификатор мобильного устройства по любому из пп. 1-6;

связывают полученный идентификатор с регистрационными данными пользователя платежного приложения;

фиксируют выполнение транзакции посредством платежного приложения;

получают данные о совершении мошеннической транзакции посредством упомянутого платежного приложения;

вносят в черный список по меньшей мере полученный статичный идентификатор мобильного устройства;

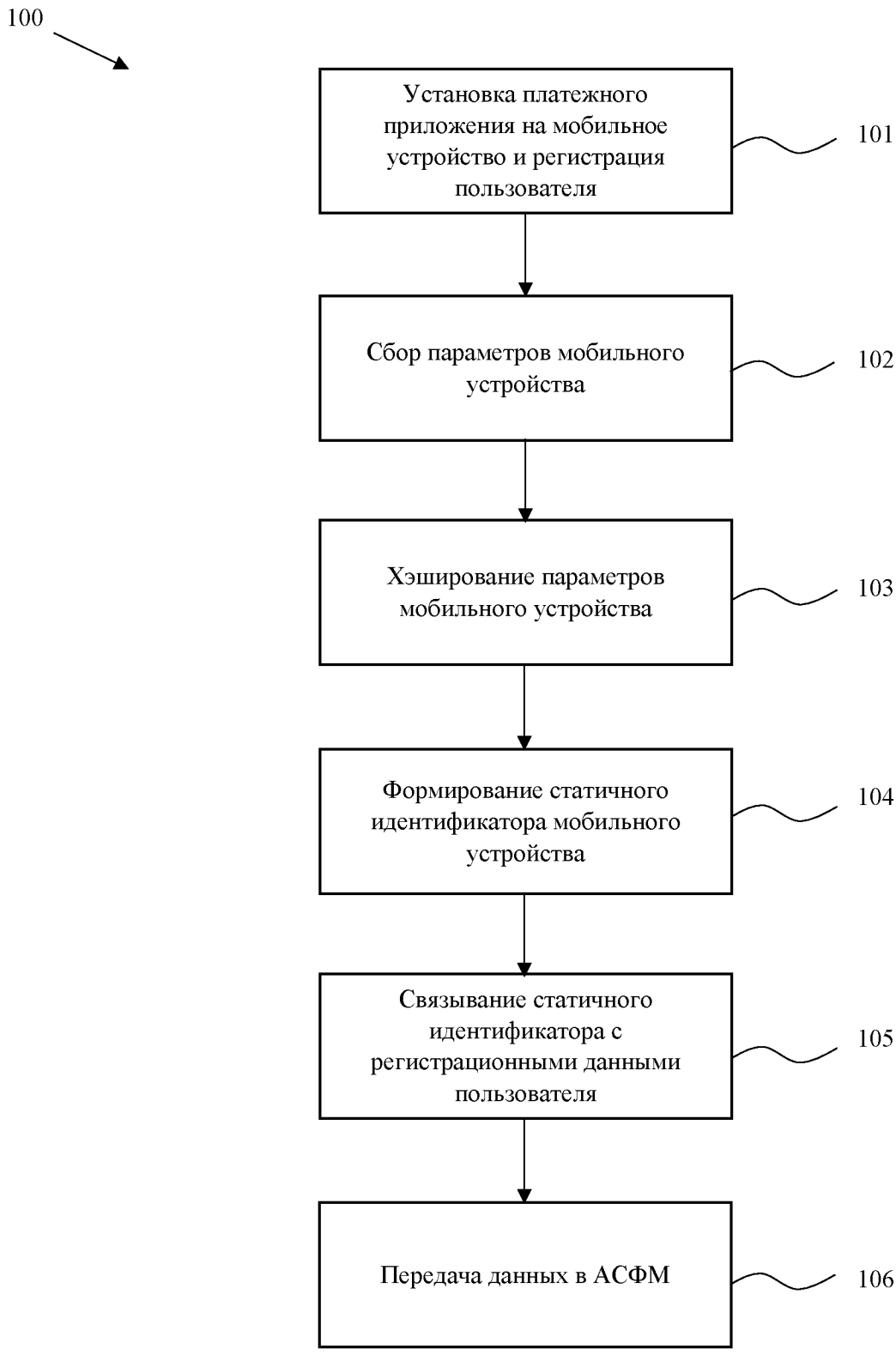
блокируют работу платежного приложения на мобильном устройстве, содержащем идентификатор, внесенный в черный список.

8. Способ по п. 7, характеризующийся тем, что фиксируют реквизиты счетов, на которые была осуществлена мошенническая транзакция.

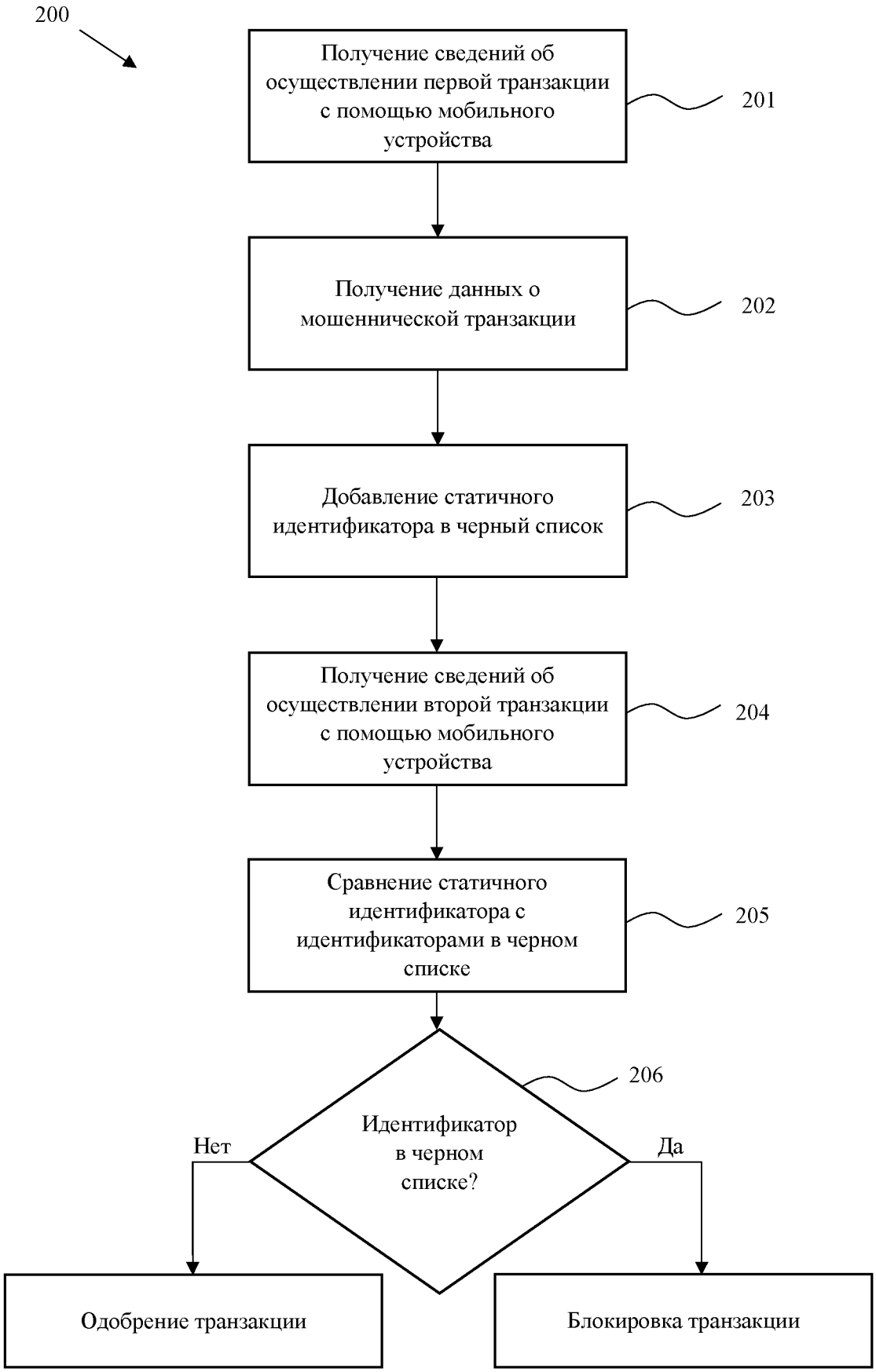
9. Способ по п. 8, характеризующийся тем, что выполняется внесение реквизитов счетов в черный список для последующих блокировок транзакций.

10. Устройство формирования статичного идентификатора мобильных устройств под управлением ОС Android, содержащее по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют способ по любому из пп. 1-6.

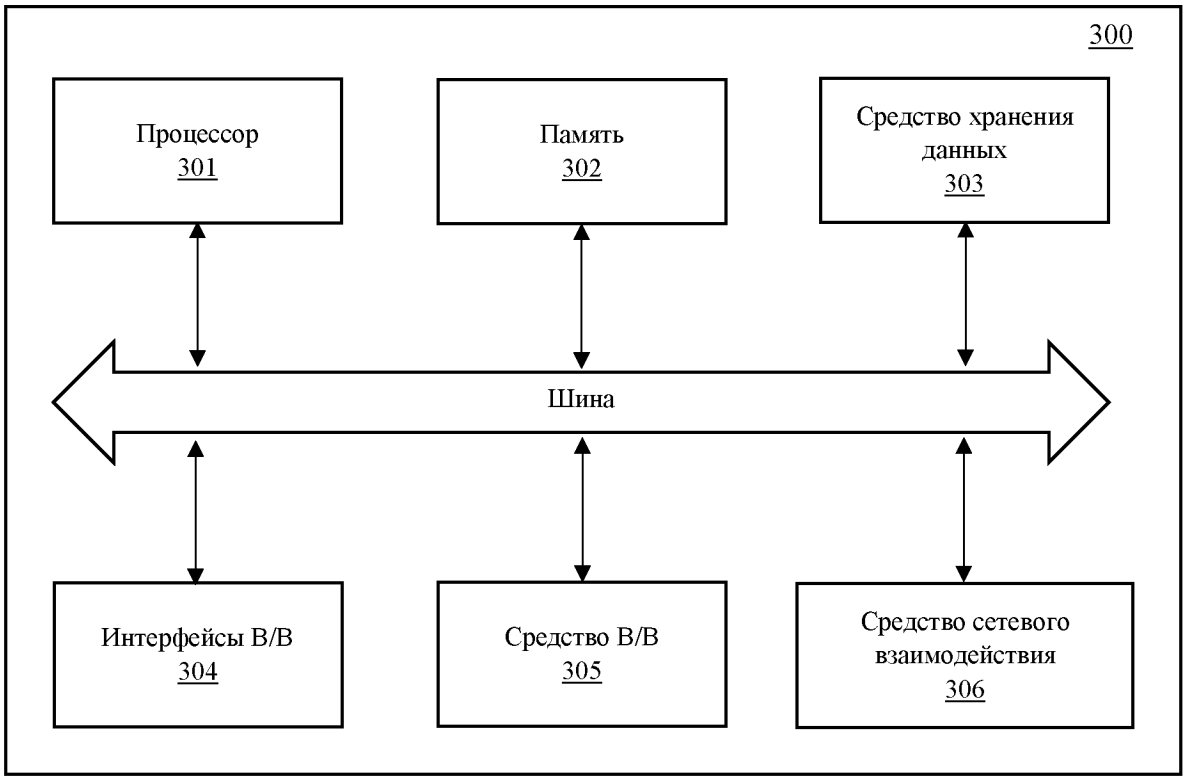
11. Система выявления мошеннических транзакций, содержащая по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют способ по любому из пп. 7-9.


100
Установка платежного приложения на мобильное устройство и регистрация пользователя
101
Сбор параметров мобильного устройства
102
Хэширование параметров мобильного устройства
103
Формирование статичного идентификатора мобильного устройства
104
Связывание статичного идентификатора с регистрационными данными пользователя
105
Передача данных в АСФМ
106

Фиг. 1


200
Получение сведений об осуществлении первой транзакции с помощью мобильного устройства
201
Получение данных о мошеннической транзакции
202
Добавление статичного идентификатора в черный список
203
Получение сведений об осуществлении второй транзакции с помощью мобильного устройства
204
Сравнение статичного идентификатора с идентификаторами в черном списке
205
206
Идентификатор в черном списке?
Нет
Да
Одобрение транзакции
Блокировка транзакции

Фиг. 2


300
Процессор
301
Память
302
Средство хранения данных
303
Шина
Интерфейсы В/В
304
Средство В/В
305
Средство сетевого взаимодействия
306

Фиг. 3

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202293481

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

G06F 21/30 (2013.01)
G06F 21/73 (2013.01)
G06Q 20/08 (2012.01)

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G06F 21/00-21/30, 21/73, G06Q 20/00-20/08

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, используемые поисковые термины)
Espacanet, ЕАПАТИС, EPOQUE Net, Reaxys, Google

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	US 2016/0205096 A1 (HOYOS LABS IP LTD) 14.07.2016, реферат, параграфы [0013], [0073], [0222], [0234], пункты 1, 15 формулы	1-11
A	US 2020/0280550 A1 (NOK NOK LABS, INC) 03.09.2020	1-11
A	US 2020/0184085 A1 (PASIG AND HUDSON, PVT LIMITED) 11.06.2020	1-11
A	RU 2715032 C2 (ВИЗА ИНТЕРНЭШНЛ СЕРВИС АССОСИЭЙШН) 21.02.2020	1-11

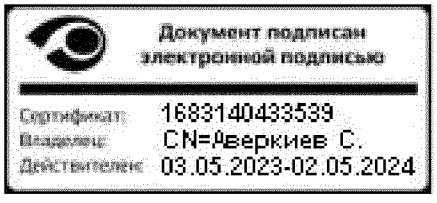
☐ последующие документы указаны в продолжении

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: 03 июля 2023 (03.07.2023)

Уполномоченное лицо:
Начальник Управления экспертизы



С.Е. Аверкиев