(19) Евразийское патентное ведомство

(21) 202392417 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.10.31

(22) Дата подачи заявки
2023.09.25

(51) Int. Cl. ***G06F 21/00*** (2013.01)
G06F 21/50 (2013.01)
G06F 21/60 (2013.01)

(54) СПОСОБ И СИСТЕМА ОПРЕДЕЛЕНИЯ АКТИВНОСТИ УЧЕТНЫХ ЗАПИСЕЙ В ВЫЧИСЛИТЕЛЬНОЙ СРЕДЕ

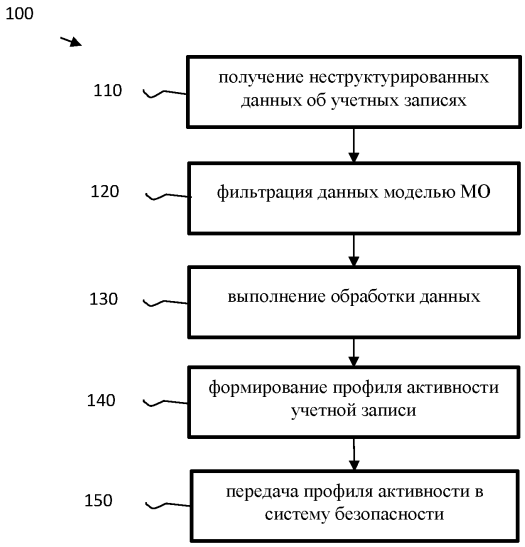
(31) **2023108563**
(32) **2023.04.05**
(33) **RU**

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

(72) Изобретатель:
Усков Святослав Александрович, Кравченко Андрей Алексеевич, Драчуков Андрей Александрович, Жиров Дмитрий Викторович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Заявленное изобретение в общем относится к области информационной безопасности, а в частности - к способу и системе определения активности учетных записей в вычислительной среде. Техническим результатом от реализации заявленного способа является сокращение времени, требуемого на формирование профиля активности учетной записи в вычислительной среде. Указанный технический результат достигается благодаря осуществлению способа определения активности учетных записей в вычислительной среде, содержащего этапы, на которых получают неструктурированные данные об учетных записях в вычислительной среде, причем указанные данные содержат, по меньшей мере, следующие технические данные: данные об идентификаторах учетных записей, данные о действиях учетных записей, время совершения действия учетными записями; осуществляют фильтрацию данных с помощью модели машинного обучения на базе нейронной сети, обученной на основе данных о событиях учётной записи, подлежащих фильтрации из общего объёма данных, в ходе которой извлекают данные о целевом событии, совершенном учетной записью, причем данные о целевом событии содержат по меньшей мере данные об описании указанного события; осуществляют обработку данных, в результате которой структурируют и нормализуют данные об описании события, причем структуризация осуществляется на основе выделения, по меньшей мере, идентификаторов учетной записи и выделении характерных для данного типа события параметров из события, полученного в результате фильтрации; формируют профиль активности по меньшей мере одной учетной записи, выполняют передачу сформированного профиля активности в систему безопасности вычислительной среды для выявления учетных записей с аномальным поведением.



202392417 A1

202392417 A1

МПК: G06F 21/00

СПОСОБ И СИСТЕМА ОПРЕДЕЛЕНИЯ АКТИВНОСТИ УЧЕТНЫХ ЗАПИСЕЙ В ВЫЧИСЛИТЕЛЬНОЙ СРЕДЕ

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное техническое решение в общем относится к области информационной безопасности, а в частности к способу и системе определения активности учетных записей в вычислительной среде.

УРОВЕНЬ ТЕХНИКИ

[0002] В настоящее время крупные предприятия используют системы сетевых взаимодействий для обмена конфиденциальной информацией между сотрудниками и клиентами. Как правило, доступ к такого рода информации предоставляется определенным сотрудникам и внутренним подсистемам посредством разрешения на подключение их учетных записей к защищенным хранилищам, где расположена конфиденциальная информация. Современные сети, используемые на крупных предприятиях, могут включать десятки или даже сотни тысяч учетных записей, каждая из которых имеет доступ к большому количеству серверов и других хранилищ данных, а, следовательно, имеет доступ к конфиденциальной информации, несанкционированное получение которой может привести к нарушению безопасности в структуре предприятия и утечки критически важных данных.

[0003] Для защиты информации от несанкционированного получения третьими лицами на предприятиях принимаются строгие меры безопасности, устанавливаются строгие стандарты доступа и используются системы противодействия атакам из вне, однако, такие меры оказываются крайне неэффективными при защите данных от кражи сотрудниками, у которых есть правомерный доступ к таким данным. Одним из методов, позволяющим выявить инциденты утечки конфиденциальной информации через внутренние каналы предприятия являются способы отслеживания активности сотрудников в вычислительной среде для обеспечения возможности мониторинга событий информационной безопасности.

[0004] Так, из уровня техники известны подходы к выявлению скомпрометированных учетных записей на основе сопоставления активности учетных записей с моделями активности для данного класса учетных записей. Такие подходы сопоставляют активность учетной записи с фиксированными правилами и статистикой, например, идентификация количества неудачных попыток входа в систему, обнаружение подозрительного поведения,

основанного на отклонении действий от стандартной частоты действий учетной записи и т.д.

[0005] Недостатками таких подходов является низкая точность и длительное время, необходимое для формирования активности учетных записей, и, как следствие низкая эффективность выявления событий информационной безопасности, например, аномального поведения из-за использования шаблонных моделей определения поведения и отсутствия эффективного и быстрого способа получения данных (профиля активности), на основе которого происходит определение поведения. Кроме того, такие системы не предназначены и не предполагают возможность работы в среде больших данных (Big Data) из-за невозможности своевременной обработки большого потока данных в приемлемое время для получения актуальных сведений об активности учетных записей.

[0006] Из уровня техники также известно решение, раскрытое в заявке на патент США № US2011/0296003 A1 (MCCANN ROBERT L et al.), опубл. 01.12.2011. Указанное решение раскрывает способ формирования модели, описывающей активность, демонстрируемую посредством взаимодействия через учетную запись пользователя и поставщика услуг. В ответ на определение того, что последующее взаимодействие, выполняемое через учетную запись пользователя, отклоняется от сгенерированной модели, учетная запись пользователя помечается как потенциально скомпрометированная злоумышленником.

[0007] Недостатком указанного решения является невозможность корректной работы способа в средах с большим потоком данных ввиду отсутствия средств, позволяющих осуществлять сбор, обработку и агрегацию данных фактической активности пользователей в такой среде (Big Data). Кроме того, данный способ не предназначен для обеспечения своевременной возможности выявления учетных записей, несоответствующих требованиям информационной безопасности корпоративной вычислительной сети при большом количестве учетных записей (сотни тысяч), из-за того, что агрегация общего объёма данных, собираемых для формирования профиля активности учетной записи и обработки указанного профиля, является чрезвычайно ресурсоёмкой задачей.

[0008] Общими недостатками существующих решений является отсутствие эффективного способа, обеспечивающего возможность формирования активности учетной записи для мониторинга событий информационной безопасности в корпоративной вычислительной среде с высокой скоростью (пока данные актуальны), что также, как следствие, обеспечивает возможность точного и быстрого (актуального) определения аномальных событий, в том числе и в среде большого потока данных. Кроме того, такого рода решения должно обеспечивать сбор и агрегацию данных фактической активности пользователей в вычислительной среде в кратчайшие временные промежутки, за счет

возможности предварительной фильтрации ключевых событий активности из общего потока событий в среде больших данных и сокращать общий объем памяти, необходимый для хранения событий, совершенных учетными записями, связанных с мониторингом информационной безопасности в вычислительной среде.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

[0009] В заявленном техническом решении предлагается новый подход к определению активности учетных записей в вычислительной среде для мониторинга событий информационной безопасности. В данном решении используется алгоритм фильтрации событий, совершаемых учетной записью, который позволяет сократить время, требуемое на формирование профиля активности учетной записи, что обеспечивает возможность быстрого и эффективного (своевременного) получения данных об активности учетной записи для дальнейшего анализа.

[0010] Таким образом, решается техническая проблема обеспечения возможности определения активности учетных записей.

[0011] Техническим результатом, достигающимся при решении данной проблемы, является обеспечение возможности определения профиля активности учетной записи в вычислительной среде.

[0012] Дополнительным техническим результатом, проявляющимся при решении вышеуказанной проблемы, является сокращение времени определения профиля активности учетной записи в вычислительной среде.

[0013] Указанные технические результаты достигаются благодаря осуществлению способа определения активности учетных записей в вычислительной среде, выполняющегося по меньшей мере одним вычислительным устройством, и содержащего этапы, на которых:

a) получают неструктурированные данные об учетных записях в вычислительной среде, причем указанные данные содержат по меньшей мере следующие данные: данные об идентификаторах учетных записей, данные о действиях учетных записей, время совершения действия учетными записями;

b) осуществляют фильтрацию данных, полученных на этапе a), с помощью модели машинного обучения на базе нейронной сети, обученной на основе данных о событиях учётной записи, подлежащих фильтрации из общего объёма данных, в ходе которой извлекают данные о целевом событии, совершенном учетной записью, причем данные о целевом событии содержат по меньшей мере данные об описании указанного события;

c) осуществляют обработку данных, полученных на этапе b), в результате которой структурируют и нормализуют данные об описании события, причем структуризация осуществляется на основе выделения по меньшей мере идентификаторов учетной записи и выделении характерных для данного типа события параметров из события, полученного в результате фильтрации;

d) формируют профиль активности по меньшей мере одной учетной записи на основе данных, полученных на этапе c).

e) выполняют передачу сформированного профиля активности в систему безопасности вычислительной среды;

f) выявляют, на основе сформированного профиля активности по меньшей мере одной учетной записи, по меньшей мере одну учетную запись с аномальным поведением.

[0014] В одном из частных вариантов реализации неструктурированные данные об учетных записях получают по меньшей мере из журнала аудита.

[0015] В другом частном варианте реализации журнал аудита представляет собой по меньшей мере текстовый файл.

[0016] В другом частном варианте реализации идентификаторы учетных записей содержат по меньшей мере прямые и/или косвенные идентификаторы учётных записей.

[0017] В другом частном варианте реализации прямым идентификатором учетных записей является по меньшей мере одно из: логин, имя пользователя / учётной записи.

[0018] В другом частном варианте реализации косвенным идентификатором учетных записей является по меньшей мере IP адрес.

[0019] В другом частном варианте реализации выделение характерных для данного события параметров из отфильтрованного события осуществляется с помощью выделения (парсинга) целевых параметров события из события, полученного в результате фильтрации, посредством регулярных выражений.

[0020] В другом частном варианте реализации выделение характерных для данного события параметров из отфильтрованного события осуществляется с помощью выделения (парсинга) целевых параметров события из отфильтрованного события посредством нахождения именованных сущностей в указанном событии.

[0021] В другом частном варианте осуществления профиль активности содержит по меньшей мере следующие метрики:

- количество целевых событий за заданный интервал времени;
- временные метки первого и последнего целевого события;
- идентификационные данные учетной записи.

[0022] Кроме того, заявленные технические результаты достигаются за счет системы определения активности учетных записей в вычислительной среде, содержащей:

по меньшей мере один процессор;

по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивают выполнение способа определения активности учетных записей в вычислительной среде.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0023] Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей.

[0024] Фиг. 1 иллюстрирует блок-схему выполнения заявленного способа.

[0025] Фиг. 2а и Фиг. 2б иллюстрирует пример сформированного профиля активности учетной записи в вычислительной среде.

[0026] Фиг. 3 иллюстрирует пример общего вида вычислительной системы, которая обеспечивает реализацию заявленного решения.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0027] Ниже будут описаны понятия и термины, необходимые для понимания данного технического решения.

[0028] Модель в машинном обучении (МО) — совокупность методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач.

[0029] ROC-кривая – графическая характеристика качества бинарного классификатора, отражающая зависимость доли истинно-положительных классификаций от доли ложно-положительных классификаций при варьировании порога решающего правила.

[0030] Метрика AUC (Area Under Curve) - Количественная интерпретация ROC-кривой, характеризующая качество (точность) классификатора.

[0031] Неструктурированные данные - данные, которые не соответствуют заранее определённой модели данных, и, как правило, представлены в форме текста с датами, цифрами, фактами, а также большим количеством технических данных, расположенными в нём в произвольной форме. Такие данные проблематично и трудно анализировать, что не позволяет своевременно получать необходимую информацию.

[0032] Активность учетной записи - действия, совершаемые пользователем, владеющим учетной записью, в конкретной вычислительной среде с элементами указанной среды. К действиям пользователя относятся такие действия, как аутентификация,

авторизация, чтение/запись данных из различных источников хранения, расположенных в вычислительной среде, а также другие виды взаимодействий с компонентами этой среды.

[0033] Событие информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности. Так, событиями информационной безопасности могут являться такие события, как: неправомерный доступ к ресурсам, аномальное поведение учетной записи в вычислительной среде и т.д.

[0034] Заявленное техническое решение предлагает новый подход, обеспечивающий сокращение времени, затрачиваемого на формирование профиля активности учетной записи в вычислительной среде, что, как следствие, обеспечивает возможность проведения своевременного (пока данные являются актуальными) анализа указанных данных системой безопасности вычислительной среды для предотвращения и\или выявления событий информационной безопасности. Кроме того, указанное техническое решение обеспечивает возможность определения активности учетной записи в среде большого потока данных (Big Data) в приемлемое время, за счет алгоритма фильтрации большого потока данных. Также, реализация алгоритма фильтрации обеспечивает сокращения объема событий, хранящихся в памяти.

[0035] Данное техническое решение может быть реализовано на компьютере, в виде автоматизированной информационной системы (АИС) или машиночитаемого носителя, содержащего инструкции для выполнения вышеупомянутого способа.

[0036] Техническое решение может быть реализовано в виде распределенной компьютерной системы.

[0037] 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).

[0038] Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

[0039] Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройства хранения данных, например, таких устройств как оперативно запоминающие устройства (ОЗУ) и/или постоянные запоминающие устройства (ПЗУ). В качестве ПЗУ могут выступать, но, не ограничиваясь, жесткие диски

(HDD), флэш-память, твердотельные накопители (SSD), оптические носители данных (CD, DVD, BD, MD и т.п.) и др.

[0040] Программа — последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

[0041] Термин «инструкции», используемый в этой заявке, может относиться, в общем, к программным инструкциям или программным командам, которые написаны на заданном языке программирования для осуществления конкретной функции, такой как, например, получение артефактов программно-аппаратного решения, формирование цифрового стандарта программно-аппаратного решения, формирование результатов проверки программно-аппаратного решения, анализ данных и т. п. Инструкции могут быть осуществлены множеством способов, включающих в себя, например, объектно-ориентированные методы. Например, инструкции могут быть реализованы, посредством языка программирования C++, Java, Python, различных библиотек (например, MFC; Microsoft Foundation Classes) и т. д. Инструкции, осуществляющие процессы, описанные в этом решении, могут передаваться как по проводным, так и по беспроводным каналам передачи данных, например Wi-Fi, Bluetooth, USB, WLAN, LAN и т. п.

[0042] Обучение модели МО производилось на записях из журнала аудита корпоративной вычислительной среды. Для формирования обучающей выборки были предварительно отобраны примеры событий учётной записи, которые требуется отфильтровать из общего объёма неструктурированных данных. Также в обучающую выборку были добавлены прочие события учётной записи, не относящиеся к целевому событию, которое требовалось отфильтровать. Соотношение событий в общем объеме выборки составляло около 1/3 для целевого события и 2/3 для прочих событий.

[0043] На момент создания модели был использован датасет (набор данных обучающей выборки) из 1 млн. размеченных записей, из них 400 тыс., которые соответствуют заданному целевому событию. Указанные события размечались меткой целевого класса. Остальные записи размечались меткой класса "OTHER". Результатом работы модели машинного обучения являлось решение задачи классификации, а именно задачи бинарной классификации элементов заданного множества в две группы. Указанный процесс обучения повторялся для каждого целевого события с соблюдением указанного выше соотношения. Таким образом, результатом обучения модели МО являлась по меньшей мере одна, обученная на распознавание всех целевых событий, МО на базе нейронной сети.

[0044] Метрика качества AUC составляет 0.98 на выборке в 1 миллион записей из журнала аудита за 1 час. При этом в среднем отбирается 300-350 тыс. записей целевого класса.

[0045] Применение данного подхода позволяет исключить необходимость использования системы правил фильтрации на последующих этапах обработки событий, что значительно сокращает время извлечения необходимых событий и увеличивает скорость формирования профиля активности учетных записей за счет возможности эффективной обработки отфильтрованных событий. Также, данное решение не использует системы предварительного извлечения именованных сущностей при выявлении целевых событий, что также сокращает время и требуемые вычислительные ресурсы. Таким образом, при использовании заявленного технического решения, обеспечивается возможность быстрого и актуального поиска, за счет профиля активности учетных записей, учетных записей с аномальным поведением. Такой подход позволяет предотвратить и/или сократить время реагирования на угрозу информационной безопасности вычислительной среды.

[0046] На **Фиг. 1** представлена блок схема способа **100** определения активности учетных записей в вычислительной среде, который раскрыт поэтапно более подробно ниже. Указанный способ **100** заключается в выполнении этапов, направленных на обработку различных цифровых данных. Обработка, как правило, выполняется с помощью системы, например, системы **300**, которая может представлять, например, сервер, компьютер, мобильное устройство, вычислительное устройство и т. д. Более подробно элементы системы **300** раскрыты на **Фиг. 3**.

[0047] На этапе **110** получают неструктурированные данные об учетных записях.

[0048] На указанном этапе **110** система **300** получает неструктурированные данные об учетных записях в вычислительной среде, причем указанные данные содержат по меньшей мере такие данные, как данные об идентификаторах учетных записей, данные о действиях учетных записей, время совершения действия учетными записями. Указанные данные содержаться в технических данных, что существенно усложняет процесс их поиска и извлечения. Стоит отметить, что под термином технические данные в данном решении следует понимать такие данные, которые изложены в неструктурированном виде. Т.е. извлечение конкретного типа (требуемых данных) из всего потока технических данных является нетривиальной задачей и требует использование дополнительных средств. Как упоминалось выше, неструктурированные данные содержат огромное количество различных данных, которые не имеют конкретной модели хранения данных. Так, в день, корпоративная вычислительная среда предприятия, работающего в среде больших данных

(Big Data) может генерировать до 8-10 млрд. различных записей в журналах аудита (технических данных). Очевидно, что задача обработки такого объема данных для возможности формирования профиля активности конкретной учетной записи является сложной и нетривиальной задачей. При этом, скорость обработки данных напрямую коррелирует со скоростью определения инцидентов информационной безопасности в вычислительной среде, например, определение учетных записей с аномальным поведением. Именно на решение указанной задачи направлено заявленное техническое решение. Таким образом, определение профиль активности учетной записи также обеспечивает возможность выявления и\или предотвращения событий информационной безопасности, посредством анализа указанного профиля.

[0049] Данные об учетных записях могут представлять собой, например, данные логов из источника хранения журналов аудита. Так, указанные неструктурированные данные содержат прямые и/или косвенные идентификаторы учётной записи. К таким идентификаторам могут относиться логин, имя пользователя / учётной записи, и/или другой идентификатор учётной записи, IP адрес. Также, среди неструктурированных данных содержится описание совершаемого действия и его результат, и/или тип, категория совершаемого действия. К таким действиям могут быть отнесены данные об аутентификации и авторизации, чтения/записи файлов, установления сессий с базой данных / хранилищем данных, выполнения запросов к данным и т.д. Кроме того, в таких данных также содержится информация о моменте времени, когда действие учётной записи было совершено и зафиксировано в вычислительной среде. Стоит отметить, что действием учетной записи в вычислительной среде может являться любое совершаемое действие пользователя, например, вход в приложение, перемещение по веб-страницы и т.д., не ограничиваясь.

[0050] Вычислительная среда может представлять, например, локальную вычислительную сеть предприятия, корпоративную сеть предприятия и т.д. Под предприятием может пониматься, любая организация, компания, фирма и т.д., обладающая структурной сетью связи. Источником хранения неструктурированных данных могут являться журналы аудита, например, хранилище Elasticsearch. Журнал аудита - это записи обо всех событиях в системе, включая доступ к ней и выполненные операций. Логи - это файлы, содержащие системную информацию о работе сервера или любой другой программы, в которые вносятся определённые действия пользователя или программы. Сбор логов может осуществляться инструментами Elasticsearch. Также, сбор логов может осуществляться сторонними приложениями, например, API приложениями, такими как Logstash, Fluentd и т.д. Указанные инструменты предназначены для ведения журнала

аудита. Журнал аудита содержит в себе набор неструктурированной информации об учетных записях, например, в виде текстового файла. Так, журнал аудита может содержать большое количество логов различных событий, что существенно затрудняет возможности его обработки, а в условиях большого потока данных, делает получение необходимых данных в приемлемое время (пока данные актуальны) сложной и нетривиальной задачей. Как упоминалось выше, в журналы аудита ежедневно могут попадать миллиарды записей, из которых требуется получить данные по всем пользователям вычислительной среды предприятия и выделить ключевые события активности из общего потока событий, для формирования профиля активности учетной записи, чтобы, как следствие, обеспечить возможность дальнейшего определения и предотвращения инцидентов информационной безопасности.

[0051] Для решения указанной проблемы, в настоящем техническом решении осуществляется обработка неструктурированных данных, полученных на этапе **110,** для обеспечения возможности своевременного получения ключевых событий активности учетных записей и эффективного выявления параметров из указанных ключевых событий на основе которых обеспечивается возможность быстрого и эффективного определения аномального поведения учетных записей (этап **120**).

[0052] Так, для возможности определения активности учетной записи требуется получить данные, касающиеся того, какой пользователь, когда и к каким данным (например, к репликам и таблицам) обращался. Указанные данные собираются в журнале аудита, например, в предпочтительном варианте реализации настоящего технического решения, в виде логов протокола аутентификации (логи HDFS (Hadoop Distributed File System)), однако, как упоминалось выше, ввиду огромного количества логов других протоколов, содержащихся в указанном журнале и неструктурированном виде, в котором получаемые логи хранятся, выделение требуемых логов является сложной и нетривиальной задачей.

[0053] Так, на этапе **120** выполняется обработка данных, полученных на этапе **110**, с помощью фильтрации указанных данных с применением модели машинного обучения на базе нейронной сети, описанной выше. Данные об используемой модели машинного обучения были приведены выше.

[0054] На указанном этапе **120**, из записей журнала аудита выделяются все целевые события, необходимые для формирования профиля активности учетной записи. Целевые события содержатся в действиях пользователя. Сложность выделения событий заключается в том, что одно действие пользователя может содержать несколько событий, которые требуется выделить из массива неструктурированных данных. Так, например, запрос

пользователя на изменение данных в хранилище вычислительной среды содержит два события, где первое событие — это обращение к хранилищу, а второе событие — это внесение изменений в данные в указанном хранилище. Событие в неструктурированном наборе данных представлено в виде текстового лога, например, лога обращения к хранилищу и т.д.

[0055] Так, например, из неструктурированных данных выделяются события, относящиеся к логам протокола аутентификации. Стоит отметить, что в одном частном варианте осуществления, профиль активности может содержать наборы метрик, связанных с разными целевыми событиями.

[0056] Так, протокол аутентификации содержит следующие целевые параметры, которые необходимо извлечь: учетную запись, запрашивающую аутентификацию, тип учетной записи (например, технологическая или пользовательская), домен учетной записи, IP адрес учетной записи, область ресурса, откуда пришла учетная запись, критичность, имя хоста, время и дата.

[0057] С помощью указанных параметров, в дальнейшем, определяется какой пользователь (пользовательская учетная запись\ технологическая учетная запись, ПУЗ/ТУЗ), где (ip, host, domain) и когда (в рабочее/не рабочее время) произвел аутентификацию, также определяется частота аутентификации в разрезах временных интервалов, сетевых диапазонов и контекста приложений; отклонение от среднего количества аутентификаций одним пользователем и т.д.

[0058] Для выполнения указанных действий, данные об учетной записи, полученные на этапе **110** токенизируются и векторизуются. Поток логов, представленный в журнале аудита разбивается на равные отрезки и токенизируется. Под токеном в данном решении следует понимать последовательность символов в документе, которая имеет значение для анализа. Так, токенами могут являться, например, отдельные слова, выражения, написанные на языке программирования и т.д. После токенизации данных выполняется векторизация каждого токена, например, с помощью прямого кодирования (one shot encoding). Так, например, при токенизации на основе алгоритма BPE, каждый токен, полученный в ходе указанного процесса токенизации, представлен в словаре своим индексом, отображающий позицию в указанном словаре. Таким образом, каждый токен представляет бинарный вектор (значения 0 или 1), а единица ставится тому элементу, который соответствует номеру токена в словаре, что позволяет представить каждый токен в виде вектора фиксированной длины, соответствующей размерности словаря. Далее, выполняют преобразование вектора каждого токена, полученного в ходе векторизации, в вектор вероятностей принадлежности соответствующего токена заданному классу. Так,

вектор каждого токена подается в классификатор. В качестве классификатора может быть использован, например, бинарный классификатор. Результатом применения этого классификатора к вектору является вектор вероятностей принадлежности соответствующего токена заданному классу. Так, например, в качестве целевого класса может быть задан лог аутентификации, например, Kerberos log/hadoop-hdfs/hdfs-audit.log. Указанный лог содержит информацию об аутентификации учетной записи в вычислительной среде.

[0059] Пример типового лога аудита протокола аутентификации:

{'_index': 'logs-megapack-ipa-2023.01.24.00', '_type': '_doc', '_id': 'xo-H4IUB4pCq1PMe7RnW', '_score': 0.0, '_source': {'type_id': 'Audit', 'krb5kdc_hostname': 'pvli-um0023.df.sbrf.ru', 'krb5kdc_client': '16989043_omega-sbrf-ru', 'log': {'file': {'path': '/var/log/krb5kdc.log'}, 'offset': 536416945}, 'message': 'Jan 24 00:28:00 pvli-um0023.df.sbrf.ru krb5kdc[4267](info): TGS_REQ (4 etypes {18 17 16 23}) 10.114.16.60: ISSUE: authtime 1674509279, etypes {rep=18 tkt=18 ses=18}, 16989043_omega-sbrf-ru@DF.SBRF.RU for hdfs/pklis-mvp002747.labiac.df.sbrf.ru@DF.SBRF.RU', 'krb5kdc_level': 'info', 'krb5kdc_etypes_count': '4', '@version': '1', 'krb5kdc_etype_rep': '18', 'ls_processed_idxstamp': '2023.01.24.00', 'krb5kdc_req_status': 'ISSUE', 'input': {'type': 'filestream'}, 'time_lag2': 2, 'krb5kdc_authtime': '1674509279', 'krb5kdc_client_realm': 'DF.SBRF.RU', 'agent': {'id': 'a7fe3265-887a-4215-a0fa-e093d6b89947', 'hostname': 'pvli-um0023.df.sbrf.ru', 'name': 'pvli-um0023.df.sbrf.ru', 'version': '7.16.3', 'ephemeral_id': '040723c7-fad7-4a71-8742-3e7f90648197', 'type': 'filebeat'}, 'ecs': {'version': '1.12.0'}, 'ls_processed_timestamp': '2023-01-23T21:28:02.487Z', 'krb5kdc_client_etypes': '18 17 16 23', 'krb5kdc_service': 'krb5kdc', 'krb5kdc_server': 'hdfs/pklis-mvp002747.labiac.df.sbrf.ru', 'syslog_timestamp': 'Jan 24 00:28:00', 'krb5kdc_server_realm': 'DF.SBRF.RU', 'krb5kdc_etype_ses': '18', 'tags': ['file', 'prod', 'ipa', 'krb5kdc', 'kerberos', 'heavy', 'calculated_diff', 'host_hash', 'params_unknown', 'parsed_kerberos'], 'krb5kdc_reqtype': 'TGS_REQ', 'krb5kdc_pid': '4267', 'environment': 'prod', 'ls_hostname': 'pvlas-log000226.log.df.sbrf.ru', 'krb5kdc_etype_tkt': '18', '@timestamp': '2023-01-23T21:28:00.688Z', 'app_id': 'kerberos', 'host_h': {'name': 'pvli-um0023.df.sbrf.ru'}, 'krb5kdc_clientip': '10.114.16.60', 'cluster_name': 'ipa'}}

[0060] События, которые выделяем – факты аутентификации с деталями и контекстом:

client	Учетная запись (login)
client_type	Тип Учетной Записи (пользовательская или технологическая)
domain	Домен (суффикс Учетной Записи)
client_ip	ip, с которого была аутентификация

action	в контексте какого приложения (директории) была аутентификация: 'http', host', 'hdfs', 'yarn', 'hive', 'kafka', 'hbase','zookeeper'
level	Критичность лога (info, warn и т.п.)
host_name	имя хоста, с которого была аутентификация
timestamp	дата и время

[0061] Таким образом, из всех логов, связанных с целевыми событиями, осуществляется извлечение целевых событий.

[0062] В качестве нейронной сети может быть использована, например, нейронная сеть сверточная нейронная сеть и т.д., не ограничиваясь. В одном частном варианте осуществления модель МО может представлять собой модель классификации на базе Catboost. Данные, относящиеся к заданному классу сохраняются в памяти для последующей обработки, например, в памяти системы **300.**

[0063] В соответствии с вышеописанным принципом фильтрации, из неструктурированного набора данных выделяются все целевые события и идентификаторы учетных записей. Стоит отметить, что в одном частном варианте осуществления вычислительное устройство может содержать несколько моделей МО, обученных на разные типы целевых событий.

[0064] Таким образом, на указанном этапе **120** выделяются требуемые записи (данные) об учетных записях из всего набора неструктурированных данных. Указанный этап позволяет сократить количество обрабатываемых далее данных в десятки раз. Так, в результате эксплуатации заявленного решения на предприятии, количество записей в журнале аудита для последующей обработки сократилось с 8 млрд до 400-450 тыс. Также, указанный этап позволяет исключить системы предварительного извлечения именованных сущностей при выявлении целевых событий, используемые в уровне техники, что сокращает время и требуемые вычислительные ресурсы. Кроме того, исключение системы предварительного извлечения именованных сущностей также позволяет исключить этап фильтрации контента с помощью правил.

[0065] Далее, на этапе **130** осуществляется дальнейшая обработка данных, полученных на этапе **120** с помощью выделения конкретных параметров**.**

[0066] На этапе **130** осуществляют обработку данных, полученных на этапе **120**, в результате которой структурируют и нормализуют данные об описании события, причем структуризация осуществляется на основе выделения по меньшей мере идентификаторов учетной записи и выделении характерных для данного типа события параметров из события, полученного в результате фильтрации.

[0067] На указанном этапе **130** из целевых отфильтрованных событий выделяются параметры указанных событий, характерные для данного типа события. Отфильтрованное

событие содержит в себе описание указанного события, а также сопутствующую техническую информацию. С учетом объема данных, полученных в результате фильтрации, наличие технических данных не позволяет беспрепятственно определить параметры события, которые можно было бы интерпретировать в человеко-читаемую форму (профиль активности учетной записи).

[0068] Так, на этапе **130**, полученные на этапе **120** данные нормализуют, например, очищая от заголовков, повторяющихся данных и т.д. Так, нормализация данных также может включать по меньшей мере устранение из полученного массива данных нецелевых записей. Указанный этап **130** может выполняться, например, при помощи выделения требуемых данных посредством цикла поиска по словарю. Указанный поиск по словарю широко известен из уровня техники, см. например, https://ru.wikijournal.org/wiki/Циклы_со_словарями_в_Python, найдено в Интернет, 25.02.2022. После этого происходит структуризация указанных данных. Для этого из неструктурированного текста описания события выделяют прямые и/или косвенные идентификаторы учётной записи (логин, имя пользователя / учётной записи, и/или другой идентификатор учётной записи, ip адрес), временную метку события, название события, идентификаторы и названия объектов события – таких, как базы/хранилища данных, таблицы, файлы и т.п.

[0069] Структуризация осуществляется на основе сопоставления параметров из отфильтрованного события с известными, для такого типа события, параметрами. Указанное выделение параметров события может выполняться, например, процедурой парсинга данных параметров в указанном событии, например, посредством регулярных выражений, выделения подстроки по позиции, и/или моделью выделения именованных сущностей.

[0070] Так, например, для события протокола аутентификации, из указанного события (текстового файла из журнала аудита) выделяются параметры за определенный (заданный) временной период: параметры идентифицируемые учетную запись (логин, имя пользователя), статус прохождения аутентификации (успешная/неуспешная), количество попыток прохождения аутентификации за выбранный временной период, элемент вычислительной среды, к которому осуществлялась попытка аутентификации и т.д. Указанные параметры также могут быть сохранены в хранилище вычислительной среды, например, в виде текстового файла.

[0071] Возвращаясь к примеру лога аутентификации, описанному в абзаце [0059], описанием целевых событий будет являться непосредственно информация, содержащаяся в заголовке события. Так, например, из целевого параметра client (учетная запись), будет

выделено следующее название учетной записи - 16989043, client_type – user (пользовательская учетная запись), домен - omega-sbrf-ru (внутренний домен предприятия), client_ip - 10.114.16.60, action – hdfs, level – info, host_name - 'pvli-um0023.df.sbrf.ru, timestamp - 2023-01-23T21:28:00, количество попыток аутентификации – количество обращений пользователя к серверу (в настоящем примере = 1) и т.д. При этом, как указывалось выше, вся нецелевая и\или повторяющаяся информация будет также отфильтрована.

[0072] Таким образом на этапе **130** выделяются параметры целевого события, связанные с действием, совершенным учетной записью. Указанный этап также позволяет сократить количество хранящихся записей в вычислительной среде в 3-5 раз.

[0073] На этапе **140** осуществляют формирование профиля активности учетной записи

[0074] Указанный процесс может быть реализован, например, в графическом интерфейсе системы **300.** В еще одном частном варианте осуществления, профиль пользователя может представлять собой текстовый файл с упорядоченной структурой данных, указанный файл также может быть сохранен в системе **300.**

[0075] Формирование профиля активности учетной записи осуществляется с помощью агрегации параметров целевых событий и кластеризации указанных параметров в соответствии с типами совершаемых действий учетной записи. Примеры сформированного профиля активности показаны на **фиг. 2а** и **фиг. 2б**.

[0076] Так, в одном частном варианте осуществления (фиг. 2а), профиль активности учетной записи будет содержать такие параметры, как: Автоматизированные системы (АС) к которым осуществлялся доступ (блок Источники в верхнем левом углу), число сессий с использованием ПУЗ/ТУЗ, число подключений к АС из офиса, число подключений без формализованного оформления заявок. Так, количество подключений к АС формируется на основе успешных попыток аутентификации пользователя и т.д.

[0077] На фиг. 2б показано продолжение параметров, содержащихся в профиле активности, например, IP и время подключения, заявка на обслуживание, в рамках которой предоставлялся доступ и т.д.

[0078] Таким образом, на основе агрегаций всех параметров, характерных для данного типа события, полученного в результате фильтрации, формируется профиль активности учетной записи по меньшей мере одного пользователя.

[0079] Таким образом, на указанном этапе **140** выполняется формирование профиля активности для всех исследуемых учетных записей.

[0080] Далее, на этапе **150** указанный профиль активности передается в систему безопасности вычислительной среды.

[0081] Так, указанная система информационной безопасности на основе сформированного профиля активности учетных записей выполнена с возможностью определения аномального поведения по меньшей мере одной учетной записи.

[0082] В одном частном варианте осуществления аномальное поведение учетных записей может быть определено посредством определения отклонения действий учетной записи от исторического профиля, характеризующего обычное поведение указанной учетной записи. Указанное действие может быть реализовано с помощью вычислительных средств системы **300,** например, сервером, содержащим модуль определения аномального поведения учетных записей. Указанный модуль может представлять собой как программное, так и программно-аппаратное средство, например, процессор. Так, указанный модуль выполнен с возможностью осуществлять сбор событий учетных записей за первый выбранный период. Заданный первый временной период может представлять, например, 7 суток, 14 суток и т.д. В другом частном варианте осуществления события учетных записей могут поступать из хранилища журналов аудита за соответствующий период и подаваться в модуль определения аномального поведения для обработки. Стоит отметить, что настоящие варианты осуществления подразумевают как возможность анализа какого-то определенного кластера сотрудников, например, отдела, направления и т.д., так и других различных групп, выбранных администратором системы информационной безопасности (например, территориального расположения и/или принадлежности). По каждой требуемой учетной записи далее может быть сформирован исторический профиль, содержащий по меньшей мере среднее время, проведенное учетной записью в каждой БД предприятия, количество БД предприятия, посещаемое пользователем, временная активность пользователя, количество успешных\неуспешных попыток входа и т.д.

[0083] Для идентификации отклонений в поведении учетной записи, система также выполнена с возможностью сбора данных за второй временной период. Вторым временным периодом может являться непосредственно период получения данных об учетных записях, близкий к реальному времени. Как описывалось выше, за счет выполнения этапов **120-140** обеспечивается возможность своевременного получения требуемых данных для обеспечения более эффективного и быстрого процесса выявления учетных записей с аномальным поведением. На основе данных, собранных за второй временной период, также формируется текущий профиль пользователя. После формирования текущего профиля, указанный профиль сравнивается с историческим профилем. Для измерения величины отклонения между профилями, указанные профили сравниваются, например, при помощи функции расстояния, такой как среднеквадратическая ошибка, расхождение

Кульбака-Либлера или средней абсолютной ошибки. При отклонении между профилями более чем на пороговое значение, поведение учетной записи определяется как аномальное поведение. После этого к такой учетной записи могут быть применены меры безопасности, например, автоматическая временная блокировка указанной записи, уведомление о необходимости связаться со службой безопасности предприятия, блокировка доступа к критическим системам предприятия, комбинация вышеуказанных мер и т.д.

[0084] Кроме того, в некоторых частных вариантах осуществления на основе данных, полученных на этапе **140** также могут осуществляться и другие действия, направленные на сохранность информационной безопасности предприятия. Так, может быть осуществлен мониторинг по выявлению пользовательских учетных записей, генерирующих подозрительную активность. В результате такого мониторинга выявляются сотрудники предприятия, которые генерировали чрезмерную нагрузку под своей персональной учетной записью, хотя подобные активности разрешены только для технологических учетных записей. Кроме того, в еще одном частном варианте осуществления может быть осуществлен мониторинг обращения пользователей к репликам, к которым у указанного пользователя отсутствуют права обращаться. Например, посредством определения выхода пользователя в другие БД, которые по роду деятельности не должны использоваться указанным пользователем. Подобный мониторинг может быть осуществлен через BI-системы типа Qlik Sense, Apache SuperSet и т.п. посредством отрисовки и подсвечивания целевых событий в Гистограммах и Метриках, с дополнительной возможностью автоматической рассылки информационных писем ответственным офицерам кибербезопасности.,

[0085] Кроме того, в еще одном частном варианте осуществления, профиль пользователя может быть дополнен данными из смежных систем, например, данными от СКУД, HR, статистических характеристик использования устройств ввода, слепков используемых устройств пользователя и т.д. В указанном варианте осуществления, система безопасности вычислительной среды, на основании экстрагированной информации о профиле активности учетной записи может отслеживать отклонение профиля от допустимых границ. Например, при наличии слепка устройства (авторизация устройства по MAC адресу в системе безопасности) и средней частоты аутентификации в АС предприятия, отклонением будет являться выход хотя бы одного параметра за пределы нормы (например, вход с другого устройства). При этом, при определении такого отклонения система безопасности может временно заблокировать учетную запись и\или запросить дополнительную аутентификацию, например, посредством известного устройства.

[0086] Таким образом, в представленных материалах заявки раскрыт способ определения активности учетной записи в вычислительной среде, который обеспечивает быструю и эффективную возможность получения данных об активности учетных записей даже в среде большого потока данных (Big Data).

[0087] На **Фиг. 3** представлен пример общего вида вычислительной системы (300), которая обеспечивает реализацию заявленного способа или является частью компьютерной системы, например, сервером, персональным компьютером, частью вычислительного кластера, обрабатывающим необходимые данные для осуществления заявленного технического решения.

[0088] В общем случае система (300) содержит такие компоненты, как: один или более процессоров (301), по меньшей мере одну память (302), средство хранения данных (303), интерфейсы ввода/вывода (304), средство В/В (305), средство сетевого взаимодействия (306), которые объединяются посредством универсальной шины.

[0089] Процессор (301) выполняет основные вычислительные операции, необходимые для обработки данных при выполнении способа (100). Процессор (301) исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти (302).

[0090] Память (302), как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

[0091] Средство хранения данных (303) может выполняться в виде HDD, SSD дисков, рейд массива, флэш-памяти, оптических накопителей информации (CD, DVD, MD, Blue-Ray дисков) и т. п. Средства (303) позволяют выполнять долгосрочное хранение различного вида информации, например истории обработки транзакционных запросов (логов), идентификаторов пользователей и т. п.

[0092] Для организации работы компонентов системы (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.

[0093] Выбор интерфейсов (304) зависит от конкретного исполнения системы (300), которая может быть реализована на базе широко класса устройств, например, персональный компьютер, мейнфрейм, ноутбук, серверный кластер, тонкий клиент, смартфон, сервер и т. п.

[0094] В качестве средств В/В данных (305) может использоваться: клавиатура, джойстик, дисплей (сенсорный дисплей), монитор, сенсорный дисплей, тачпад,

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.

[0095] Средства сетевого взаимодействия (306) выбираются из устройств, обеспечивающий сетевой прием и передачу данных, например, Ethernet карту, WLAN/Wi-Fi модуль, Bluetooth модуль, BLE модуль, NFC модуль, IrDa, RFID модуль, GSM модем и т. п. С помощью средств (305) обеспечивается организация обмена данными между, например, системой (300), представленной в виде сервера и вычислительным устройством пользователя, на котором могут отображаться полученные данные (результаты выявленных аномальных учетных записей и т.д.) по проводному или беспроводному каналу передачи данных, например, WAN, PAN, ЛВС (LAN), Интранет, Интернет, WLAN, WMAN или GSM.

[0096] Конкретный выбор элементов устройства (300) для реализации различных программно-аппаратных архитектурных решений может варьироваться с сохранением обеспечиваемого требуемого функционала.

[0097] 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. Таким образом, объем настоящего технического решения ограничен только объемом прилагаемой формулы.

ФОРМУЛА

1. Способ определения активности учетных записей в вычислительной среде, выполняющийся по меньшей мере одним вычислительным устройством, и содержащий этапы, на которых:
    a) получают неструктурированные данные об учетных записях в вычислительной среде, причем указанные данные содержат по меньшей мере следующие данные: данные об идентификаторах учетных записей, данные о действиях учетных записей, время совершения действия учетными записями;
    b) осуществляют фильтрацию данных, полученных на этапе a), с помощью модели машинного обучения на базе нейронной сети, обученной на основе данных о событиях учётной записи, подлежащих фильтрации из общего объёма данных, в ходе которой извлекают данные о целевом событии, совершенном учетной записью, причем данные о целевом событии содержат по меньшей мере данные об описании указанного события;
    c) осуществляют обработку данных, полученных на этапе b), в результате которой структурируют и нормализуют данные об описании события, причем структуризация осуществляется на основе выделения по меньшей мере идентификаторов учетной записи и выделении характерных для данного типа события параметров из события, полученного в результате фильтрации;
    d) формируют профиль активности по меньшей мере одной учетной записи на основе данных, полученных на этапе c).
    e) выполняют передачу сформированного профиля активности по меньшей мере одной учетной записи в систему безопасности вычислительной среды;
    f) выявляют, на основе сформированного профиля активности по меньшей мере одной учетной записи, по меньшей мере одну учетную запись с аномальным поведением.
2. Способ по п. 1, характеризующийся тем, что неструктурированные данные об учетных записях получают по меньшей мере из журнала аудита.
3. Способ по п. 2, характеризующийся тем, что журнал аудита представляет собой по меньшей мере текстовый файл.
4. Способ по п. 1 характеризующийся тем, что идентификаторы учетных записей содержат по меньшей мере прямые и/или косвенные идентификаторы учётных записей.
5. Способ по п. 4, характеризующийся тем, что прямым идентификатором учетных записей является по меньшей мере одно из: логин, имя пользователя / учётной записи.

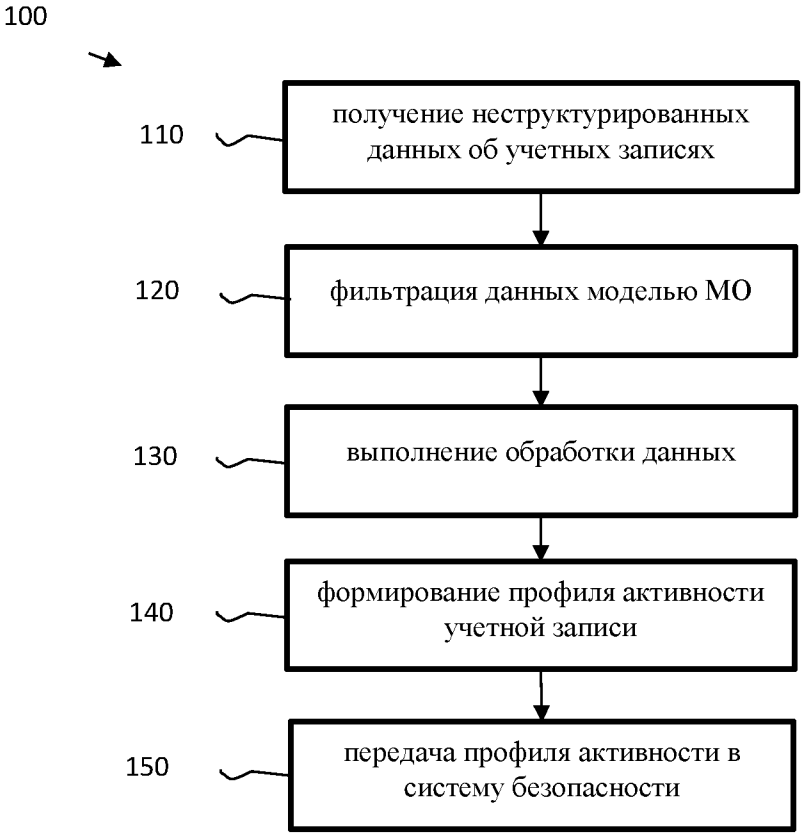
6. Способ по п. 4, характеризующийся тем, что косвенным идентификатором учетных записей является по меньшей мере IP адрес.
7. Способ по п. 1, характеризующийся тем, что выделение характерных для данного события параметров из отфильтрованного события осуществляется с помощью парсинга целевых параметров события из отфильтрованного события посредством регулярных выражений.
8. Способ по п. 1, характеризующийся тем, что выделение характерных для данного события параметров из отфильтрованного события осуществляется с помощью парсинга целевых параметров события из отфильтрованного события посредством нахождения именованных сущностей в указанном событии.
9. Способ по п. 1, характеризующийся тем, что профиль активности содержит по меньшей мере следующие метрики:
    - количество целевых событий за заданный интервал времени;
    - временные метки первого и последнего целевого события;
    - идентификационные данные учетной записи.
10. Система определения активности учетных записей в вычислительной среде, содержащая:

    по меньшей мере один процессор;

    по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивают выполнение способа по любому из п.п. 1-9.

    .

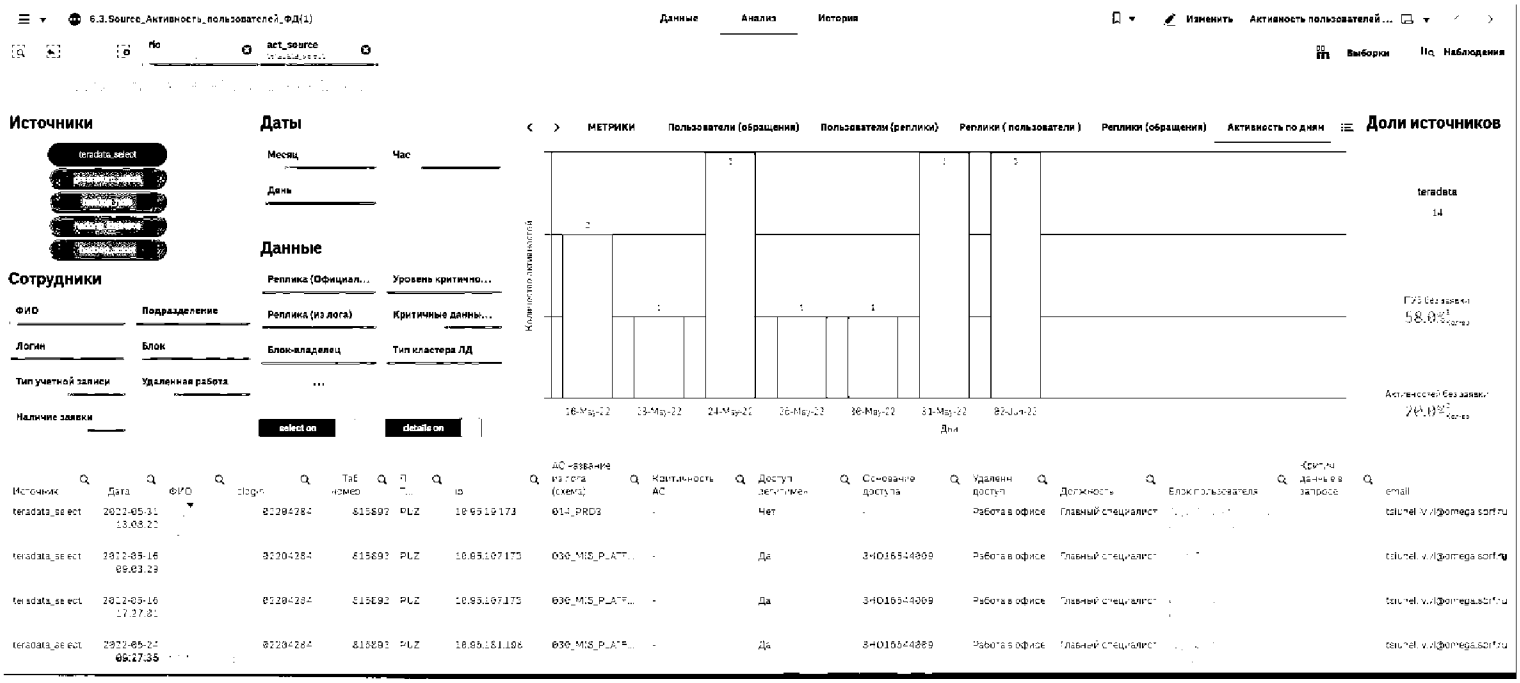
ЧЕРТЕЖИ К ОПИСАНИЮ



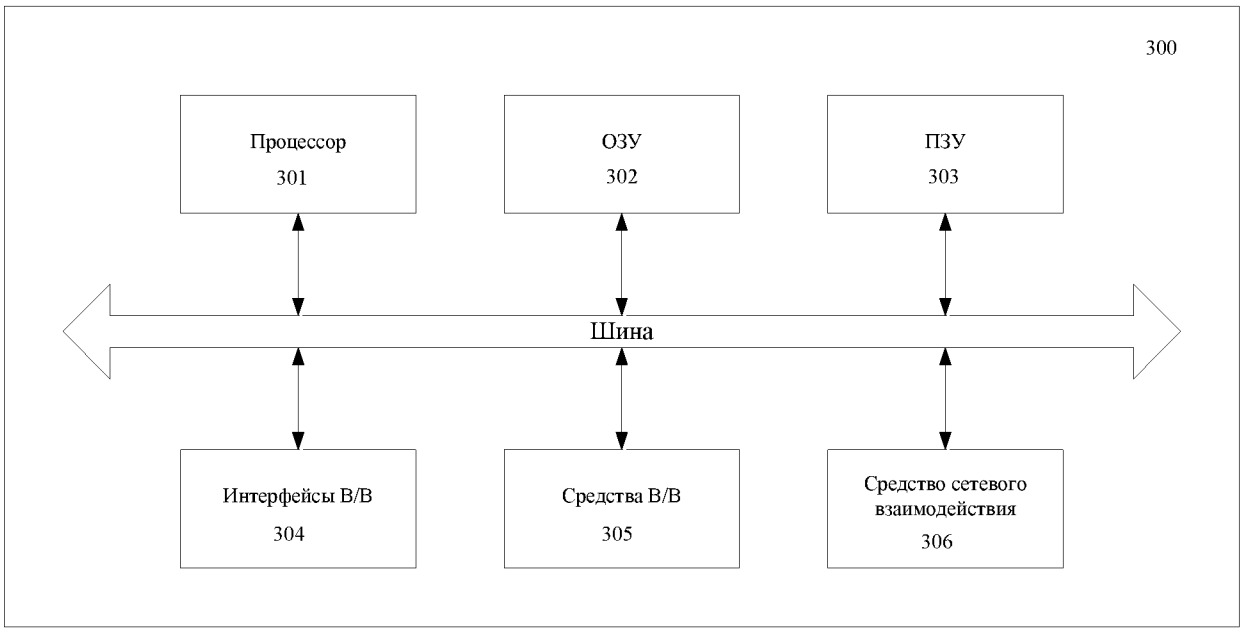
Фиг. 1


6.3.Source_Активность_пользователей_ФД(1)
Данные
Анализ
История
Изменить
Активность пользователей ...
Выборки
Наблюдения
Источники
Даты
Данные
Сотрудники
МЕТРИКИ
Пользователи (обращения)
Пользователи (реплики)
Реплики (пользователи)
Реплики (обращения)
Активность по дням
Доли источников
teradata
8
ГУЗ без заявки
58.0%
Активностей без заявки
0.0%

Фиг. 2а


6.3.Source_Активность_пользователей_ФД(1)
Данные
Анализ
История
Изменить
Активность пользователей ...
Выборки
Наблюдения
Источники
Даты
Данные
Сотрудники
МЕТРИКИ
Пользователи (обращения)
Пользователи (реплики)
Реплики (пользователи)
Реплики (обращения)
Активность по дням
Доли источников
teradata
14
ГУЗ без заявки
58.0%
Активностей без заявки
Дни

Фиг. 2б


300
Процессор
301
ОЗУ
302
ПЗУ
303
Шина
Интерфейсы В/В
304
Средства 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:

202392417

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

МПК:		СПК:
G06F 21/00	(2013.01)	**G06F 21/00**
G06F 21/50	(2013.01)	**G06F 21/50**
G06F 21/60	(2013.01)	**G06F 21/60**

Б. ОБЛАСТЬ ПОИСКА:

G06F 21/00, G06F 21/50, G06F 21/60

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, используемые поисковые термины)
EAPATIS, GOOGLE PATENTS, Espacenet, YANDEX

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	US20220207506 A1 (CAPITAL ONE SERVICES, LLC) 2022-06-30 формула изобретения п.п. 1-19; абзацы [0042]; [0045]; [0047]; [0045]; [0049]; [0052]-[0058]; [0072]-[0074]; [0080]; [0083]; [0084]; [0086]; [0088]; [0090]; [0092];[0093]; [0106]; [0111]; [0115]	1-10
A	US20220366422 A1 (Sift Science Inc) 2022-11-17 формула изобретения п.п. 1-13; абзацы [0007]; [0015]-[0021]; [0038]; [0039]; [0035]; [0036]; [0038]; [0040]; [0047]; [0057]-[006; [0063]-[0068]	1-10
A	US20200410091 A1 (PAYPAL INC.) 2020-12-31 формула изобретения п. 1; абзацы [0015]; [0031]-[0035]; [0046]-[0048]; [0059]; [0060]	1-10
A	CN 115022052 A (SHANDONG COMPUTER SCIENCE CENTER (NATIONAL SUPERCOMPUTER CENTER IN JINAN)) 2022-09-06 формула изобретения п.п. 1-6	1-10
A	US20180167402 A1 (BALABIT S. A.) 2018-06-14 формула изобретения п.п. 1, 16, 25, 26, 28, 29, 31, 32, 39, 40, 52, 53	1-10

☐ последующие документы указаны в продолжении графы

* 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: 19 июня 2024 (19.06.2024)

Уполномоченное лицо:
Начальник Управления экспертизы

Документ подписан электронной подписью
Сертификат: 1711998581100
Владелец: CN=Аверкиев С.
Действителен: 01.04.2024-01.04.2025

С.Е. Аверкиев