(19) Евразийское патентное ведомство

(21) 201991970 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2021.03.31

(22) Дата подачи заявки
2019.09.19

(51) Int. Cl. ***G06F 21/55*** (2013.01)
G08B 31/00 (2006.01)

(54) СПОСОБ И СИСТЕМА СОНИФИКАЦИИ СОБЫТИЙ КИБЕРБЕЗОПАСНОСТИ

(31) **2019127936**
(32) **2019.09.05**
(33) **RU**

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

(72) Изобретатель:
Кузьмин Александр Михайлович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Настоящее изобретение относится к области компьютерной техники, в частности к способу и системе сонификации событий кибербезопасности. Техническим результатом является повышение эффективности реагирования на возникающие события кибербезопасности в сетевых зонах за счет применения схемы сонификации событий, формируемой средствами сетевой защиты на основании статистических характеристик соединений между узлами корпоративной сети в заданном временном интервале. Заявленный результат достигается за счет компьютерно-реализуемого способа сонификации событий кибербезопасности, генерируемых средствами сетевой защиты, выполняемый с помощью процессора, в котором осуществляют сбор данных событий кибербезопасности, которые включают в себя IP-адреса узлов сетевого обмена, сетевые порты, время выполнения соединений между узлами и реакцию средств сетевой защиты на упомянутые соединения; агрегируют полученные события кибербезопасности по различным признакам в соответствии с выбранной моделью сонификации и вычисляют статистические характеристики агрегированных событий в заданном временном интервале; генерируют схему сонификации событий на основании упомянутых статистических характеристик соединений между узлами сети, причем упомянутая схема формируется в соответствии с одной из предлагаемых моделей сонификации: источник звука - зона сети, количество соединений в зоне сети - громкость источника звука, отклонение от среднего значения во временном интервале - частота повторения звука упомянутого источника во временном интервале, соотношение заблокированных и разрешенных соединений для каждой зоны - тембр/высота тона звучания источника; а затем формируют звуковые оповещения на поступающие уведомления кибербезопасности в соответствии с упомянутой схемой сонификации.

201991970 A1

201991970 A1

201991970 A1

201991970 A1

МПК: G06F 17/00; G06F 21/00; G08B 31/00

СПОСОБ И СИСТЕМА СОНИФИКАЦИИ СОБЫТИЙ КИБЕРБЕЗОПАСНОСТИ

ОБЛАСТЬ ТЕХНИКИ

[0001] Настоящее техническое решение, в общем, относится к области компьютерной техники, а в частности к способу и системе сонификации событий кибербезопасности.

УРОВЕНЬ ТЕХНИКИ

[0002] С течением развития технического уровня в области обработки данных, требующих оперативного реагирования на скоротечное изменение их состояний, сформировался новый метод, позволяющий анализировать различные процессы на основе использования аудиального отображения информации, при котором данные, получаемые в ходе измерений или контроля различных процессов, могут быть преобразованы в звуковые колебания, что дает возможность регистрировать их посредством звуковых каналов восприятия.

[0003] Такой подход называется сонификацией (англ. «sonification») и на данный момент применяется во многих научных областях в качестве альтернативы визуальному представлению данных, позволяя формировать звуковые оповещения, связанные с изменением состояния контролируемых процессов. При этом в качестве основных преимуществ является возможность обработки и реагирования на большое количество параллельных информационных потоков в реальном времени, а также оперативное обнаружение изменения критических параметров, что является особенно критичным в обработки процессов событий кибербезопасности.

[0004] Наиболее важным критерием для сонификации является построение звуковой схемы для конкретной задачи идентификации и уведомления заданных типов событий. Как правило, звуковая схема опирается на ряд параметров для формирования сонификации событий, например, параметры звуков, количество данных, их связность и т.п.

[0005] Информация имеет свойство расти. Каждая новая виртуальная сущность индивида инициализирует новые связи с другими сущностями, получает и отправляет данные, инициализирует различные процессы, то есть осуществляет информационную активность, ведущую к нарастанию данных. Увеличение объемов хранилищ данных и уменьшение стоимости их хранения ведет к тому, что общая тенденция взаимодействия с

информационными системами может быть выражена как «сохранить все» вместо «сохранить этот фрагмент». Неоспоримым является тезис об информационной сатурации (насыщении) визуального канала восприятия. Будь то покупатель в супермаркете или оператор ситуационного центра – человек вынужден обращать свое внимание на все большее и большее количество попадающих в поле зрения данных, отображаемых визуально, и/или разделять их представление во времени, увеличивая тем самым время обработки этих данных. Это ведет к целому ряду общеизвестных проблем – от повышенной утомляемости и снижения эффективности труда до возникновения критических ошибок в процессе принятия решений. На этом фоне усиливаются проблемы, связанные с совмещением различных данных.

[0006] В настоящее время методы сонификации находят широкое применение в различных областях, среди которых можно отметить медицину, авиацию и управление сложными системами, медиаискусство, бизнес-аналитику, сейсмографию, ассистивные технологии для инвалидов по зрению, астрономию. [1]

[0007] Из существующего уровня техники известны различные подходы по сонификации наблюдаемых данных. Например, анализ сетевой активности с помощью ПО SonSTAR позволяет формировать звуковые оповещения на основании анализа потоков сетевой активности с помощью фильтрации данных передаваемых пакетов. [2]

[0008] Из патента US 7511213 B2 (Soft Sound Holdings LLC, 31.03.2009) известен принцип сонификации данных изменений рынка ценных бумаг с помощью построения схемы мэппинга звуков для формирования оповещений на основании параметров динамического изменения рынка, например, скачков курсов валют, стоимости акций и т.п.

[0009] Существующие подходы не подходят для анализа событий кибербезопасности в части выявления сетевых аномалий и формирования звукового окружения на основании статистических данных соединений между узлами, агрегированными по определенным признакам.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

[0010] Настоящее изобретение направлено на решение технической проблемы, заключающейся в создании нового принципа сонификации событий кибербезопасности, позволяющего более эффективно и своевременно идентифицировать сетевые аномалии в корпоративной сети.

[0011] Техническим результатом является повышение эффективности реагирования на возникающие события кибербезопасности в сетевых зонах за счет применения схемы сонификации событий, формируемой средствами сетевой защиты на основании

статистических характеристик соединений между узлами корпоративной сети в заданном временном интервале.

[0012] Заявленный результат достигается за счет компьютерно-реализуемого способа сонификации событий кибербезопасности, генерируемых средствами сетевой защиты, выполняемый с помощью процессора и содержащий этапы, на которых:

- осуществляют сбор данных событий кибербезопасности, которые включают в себя IP-адреса узлов сетевого обмена, сетевые порты, время выполнения соединений между узлами и реакция средств сетевой защиты на упомянутые соединения;
- агрегируют полученные события кибербезопасности по различным признакам в соответствии с выбранной моделью сонификации и вычисляют статистические характеристики агрегированных событий в заданном временном интервале;
- генерируют схему сонификации событий на основании упомянутых статистических характеристик соединений между узлами сети, причем упомянутая схема формируется в соответствии с одной из предлагаемых моделей сонификации.

  источник звука – зона сети,

  количество соединений в зоне сети – громкость источника звука,

  отклонение от среднего значения во временном интервале – частота повторения звука упомянутого источника во временном интервале,

  соотношение заблокированных и разрешенных соединений для каждой зоны - тембр/высота тона звучания источника;
- формируют звуковые оповещения на поступающие уведомления кибербезопасности в соответствии с упомянутой схемой сонификации.

[0013] В одном из частных вариантов осуществления способа дополнительно осуществляется визуализация агрегированных сетевых соединений в режиме реального времени.

[0014] В другом частном варианте осуществления способа визуализация выполняется синхронно с формированием звуковых оповещений.

[0015] В другом частном варианте осуществления способа звуковое оповещение и/или визуализация зон сети передается на мобильное устройство пользователя.

[0016] В другом частном варианте осуществления способа источник выбирается из группы: музыкальный инструмент, звуки окружающей природы, звуки животных, звуки природы, синтезированные звуки или их сочетания.

[0017] Заявленный результат также достигается за счет системы сонификации событий кибербезопасности, генерируемых средствами сетевой защиты, которая содержит по меньшей мере один процессор и по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, которые при их исполнении процессором выполняют вышеописанный способ.

[0018] Иные, частные аспекты осуществления заявленного технического решения будут раскрыты далее в настоящих материалах заявки.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0019] Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей, на которых:

[0020] Фиг. 1 иллюстрирует общую схему заявленного решения.

[0021] Фиг. 2 иллюстрирует блок-схему обработки событий кибербезопасности для их сонификации.

[0022] Фиг. 3 иллюстрирует схему сонификации событий кибербезопасности при разделении на зоны сетевой активности.

[0023] Фиг. 4 иллюстрирует пример разделения звуковых источников по зонам корпоративной сети.

[0024] Фиг. 5 – Фиг. 6 иллюстрируют варианты моделей сонификации.

[0025] Фиг. 7 иллюстрирует вид вычислительной системы.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0026] Как показано на Фиг. 1 общая схема заявленного решения включает в себя сеть передачи данных (110), соединение между участками которой контролируются средством сетевой защиты (120) корпоративной инфраструктуры. Средства сетевой защиты (120) могут выбираться из различных устройств, например, межсетевой экран NGFW PaloAlto или любой другой пригодный тип устройства, обеспечивающего учет событий журнала аудита (130), связанных с инициацией соединений и сетевым взаимодействием хостов в корпоративной сети между собой и с внешними хостами.

[0027] Журнал аудита средства сетевой защиты (130) содержит события кибербезопасности, включающие данные о сетевых соединениях, в частности время события, IP-адрес отправителя, IP-адрес получателя, действие средства защиты (было ли соединение заблокировано или разрешено средством сетевой защиты). Под сетью

передачи данных может применятся информационная сеть «Интернет», образованная различными известными протоколами и принципами организации связи, например, WAN, PAN, WLAN, LAN и т.п.

[0028] Данные событий кибербезопасности из журнала аудита (130) поступают в устройство обработки (200), выполненное на базе персонального компьютера, обеспечивающее обработку данных для осуществления процесса сонификации информации.

[0029] Устройство (200) содержит модуль препроцессинга (210), выполняющий обогащение данных, получаемых от средств сетевой защиты (120), модуль сонификации (220), осуществляющий формирование звуковых оповещений согласно установленной звуковой схеме, базу данных звуков (230), содержащую источники звука для формирования звуковых оповещений, модуль визуализации (240), выполняющий визуализацию данных событий кибербезопасности.

[0030] На Фиг. 2 представлены этапы способа по сонификации событий кибербезопасности. На первом этапе (301) осуществляется сбор событий журнала аудита (130) средства сетевой защиты (120). Полученные данные с помощью модуля препроцессинга (210) агрегируются с учетом метки времени в соответствии с выбранной схемой сонификации и обогащаются дополнительной информацией, например, о принадлежности IP адреса к определенной сетевой зоне корпоративной сети, присутствия IP-адреса и/или сетевого порта в черном списке IP-адресов и/или сетевых портов. Модуль препроцессинга (210) может выполняться на языке Python и в частном варианте представлять модуль на базе алгоритмов машинного обучения, например, нейронную сеть, осуществляющую наложение схемы сонификации на сформированный набор статистических характеристик от средств сетевой безопасности (120) для генерирования звуковых оповещений по аномалиям сетевой активности.

[0031] В зависимости от полученных данных от средств сетевой защиты (120) на этапе (301) высчитываются статистические характеристики соединений (302) на основании которых потом принимается решение о применении выбранной схемы сонификации и визуализации данных на шаге (303) для последующего формирования звукового окружения в реальном масштабе времени (304).

На Фиг. 3 представлен пример схемы заявленного решения, в которой информация, подлежащая сонификации, распределяется по зонам корпоративной сети (400). Как показано на Фиг. 4 для каждой сетевой зоны (4001-4004) и заданного временного интервала (которые может задаваться по необходимости - 1,3,5,10 сек и т.д.) назначается

свой уникальный источник звука (И1-И4), позволяющий идентифицировать каждую из зон (4001-4004).

В указанной схеме сонификации происходит определение статистических характеристик соединений с помощью модуля препроцессинга (210), которые представляют собой общее количество сетевых соединений в каждой из зон (4001-4004) корпоративной сети (400) в один временной интервал (в соответствии с выбранным интервалом агрегации (1,3,5,10 сек)), соотношение заблокированных и разрешенных соединений, отклонение текущего значения количества соединений от среднего показателя количества соединений по данной сетевой зоне, отношение количества соединений из данной зоны к общему количеству соединений, количество зон, с которыми устанавливаются соединения из данной зоны.

[0032] Данные статистические характеристики далее передаются в модуль сонификации (220) и модуль визуализации (240) для выполнения этапа, включающего сонификацию и визуализацию данных (303). На этапе сонификации (303) статистические характеристики, полученные на этапе (302) для каждой сетевой зоны (110), обрабатываются с помощью сформированной звуковой схемы. Звуковая схема выстраивается следующим образом: источник звука – зона сети, количество соединений в зоне сети – громкость источника звука, отклонение от среднего значения во временном интервале – частота повторения звука упомянутого источника во временном интервале, соотношение заблокированных и разрешенных соединений для каждой зоны - тембр/высота тона звучания источника.

[0033] Источник звука выбирается из различного вида звуковых представлений, хранящихся в базе данных (230) и назначается для каждой из зон (4001-4004). Таким представлениями могут выступать, например, музыкальный инструмент, звуки окружающей природы, звуки животных, звуки природы, синтезированные звуки или их сочетания. Перечень звуковых представлений не ограничивается приведенными примерами и может быть расширен.

[0034] Источник звука накладывается на сформированную схему сонификации для формирования звуковых оповещений (304) по зафиксированным аномалиям в сети передачи данных (110). Под аномалиями понимаются резкие изменения наблюдаемых статистических характеристик (резкое изменение количества соединений в определенной зоне, изменение соотношения заблокированных и допущенных соединений, сильное отклонение от среднего значения количества соединений по данной зоне), которые могут сигнализировать об инциденте безопасности или функционирования IT-систем. Сонификация аномалий позволяет более явно и/или на более раннем этапе оповестить о

возникновении такого рода событий и повысить эффективность и скорость реагирования операторов, осуществляющих мониторинг сетевой активности.

[0035] Например, определенные изменения сетевой активности в сети передачи данных (110) могут сигнализировать о начинающейся DDoS атаке, массовом вирусном заражении, неправильном функционировании средств защиты и прочем. С учетом того, что в крупной сетевой инфраструктуре даже одно средство сетевой защиты (130) может генерировать десятки тысяч событий в секунду, то с применением сонификации оператор получает возможность оперативного выявления из них аномального одного подмножества, которое требует более детального изучения на предмет угроз.

[0036] Модуль визуализации (240) позволяет дополнительно формировать изображения по возникающим аномалиям сетевых соединений сети передачи данных (110). Модуль (240) может быть реализован, например, на движке Unity, обеспечивающем различные типы генерации визуально воспринимаемой информации по возникающим событиям кибербезопасности. Визуализация статистических характеристик соединений сети передачи данных (110) могут формироваться одновременно со звуковыми оповещениями.

[0037] Звуковые оповещения, сформированные с помощью схемы сонификации на этапе (304), выводятся с помощью стандартных средств рабочей станции оператора, например, с помощью наушников. Звуковые оповещения также могут передаваться операторам на личные мобильные устройства или иной тип носимых устройств, например, смарт-часы. Устройство (200), обеспечивающее сонификацию данных, может выполняться в виде сервера и содержать информацию с назначением наблюдаемых аномалий профилям операторов, что позволяет формировать звуковые оповещения требуемым сотрудникам. Передача такой информации осуществляется посредством средств беспроводной связи, например, таких как Bluetooth, Wi-Fi и т.п.

[0038] В другом частном варианте схема сонификации событий кибербезопасности может формироваться на основании статистических характеристик, определяемых на основании анализа данных транспортного протокола сетевых соединений. На Фиг. 5 представлена блок-схема выполнения процесса сонификации событий кибербезопасности при использовании модели сонификации на основании анализа сетевого протокола (500). На первом этапе (501) выполняется предобработка данных, при которой осуществляется агрегация событий по задействованному транспортному протоколу (TCP/UDP/ICMP), а также выполняется проверка наличия IP-адресов и сетевых портов из событий безопасности в черных списках IP-адресов и портов. Черные списки содержат вредоносные и опасные IP-адреса (как правило хосты в сети интернет, вовлеченный в

вредоносную активность, такую как фишинг, спам, распространение ВПО и пр.) и порты, использование которых может свидетельствовать о заражении хоста корпоративной сети ВПО.

[0039] На этапе (502) для каждого транспортного протокола вычисляются статистические характеристики:

- количество соединений в единицу времени;
- отклонение от среднего значения количества соединений для конкретного транспортного протокола.

[0040] Для IP-адресов и портов из черных списков вычисляется наличие IP-адресов и портов из черных списков в каждом временном интервале.

[0041] Генерация звукового окружения с помощью схемы сонификации на этапе (503), при этом если осуществляется определение того, что в данных, полученных от средства защиты (120) присутствует IP-адреса и/или порты сетевых соединений из черного списка, то для таких IP-адресов или портов назначается отдельный источник звука для их идентификации в общем потоке данных (504).

[0042] Модель сонификации на этапе (503) выполняется следующим образом.

Для транспортных протоколов:

- Транспортный протокол - отдельный инструмент/источник звука;
- Относительное количество соединений с использованием конкретного транспортного протокола - громкость источника звука;
- Отклонение от среднего значения количества соединений для конкретного транспортного протокола - тембр/высота тона источника звука.

Для IP-адресов и сетевых портов из черных списков:

- Наличие IP-адреса/сетевого порта в черном списке - инструмент /источник звука (отдельный инструмент для IP-адресов и для сетевых портов);
- Количество IP-адресов/портов из черного списка в одном временном интервале - уровни громкости инструмента/источника звука (где нулевая громкость означает отсутствие вхождений в черный список в данном временном интервале).

[0043] Ниже представлен пример формирования звукового окружения с помощью вышеуказанной модели сонификации (500):

- протокол TCP - шелест листьев деревья от ветра (лево);
- протокол UDP - шум волн (право);
- протокол ICMP - свист ветра (лево);

- IP-адрес из черного списка - переливы\перезвоны в стиле ловца ветра (лево);
- сетевой порт из черного списка - гудок корабля (право).

[0044] Также, другим примером модели сонификации, как представлено на Фиг. 6, может выступать анализ агрегацией по действию средства защиты (600). На этапе предобработки (601) выполняется агрегация событий по типу действий средства сетевой защиты (allow/deny/alert/drop/reset), а также выполняется проверка наличия IP-адресов и сетевых портов из событий безопасности в черных списках IP-адресов и портов. Черные списки содержат вредоносные и опасные IP-адреса (как правило хосты в сети интернет, вовлеченный в вредоносную активность, такую как фишинг, спам, распространение ВПО и пр.) и порты, использование которых может говорить о заражении хоста корпоративной сети ВПО.

[0045] Для каждого транспортного протокола вычисляются статистические характеристики (602):

- количество попыток соединений с данным действием средства защиты в единицу времени;
- отклонение от среднего значения количества соединений для конкретного действия средства защиты.

  Для IP-адресов и портов из черных списков вычисляется наличие IP-адресов и портов из черных списков в каждом заданном временном интервале.

[0046] Генерация звукового окружения с помощью схемы сонификации на этапе (603), при этом если осуществляется определение того, что в данных, полученных от средства защиты (120) присутствует IP-адреса и/или порты сетевых соединений из черного списка, то для таких IP-адресов или портов назначается отдельный источник звука для их идентификации в общем потоке данных (604).

[0047] Модель сонификации на этапе (603) выполняется следующим образом:

- Тип действия средства сетевой - отдельный инструмент/источник звука;
- Относительное количество попыток соединения с данным действием средства сетевой защиты - громкость источника звука;
- Отклонение от среднего значения количества соединений для конкретного действия средства защиты - тембр/высота тона источника звука.

Для IP-адресов и сетевых портов из черных списков:

- Наличие IP-адреса/сетевого порта в черном списке - инструмент /источник звука (отдельный инструмент для IP-адресов и для сетевых портов);

– Количество IP-адресов/портов из черного списка в одном временном интервале - уровни громкости инструмента/источника звука (где нулевая громкость означает отсутствие вхождений в черный список в данном временном интервале).

[0048] Ниже представлен пример формирования звукового окружения с помощью вышеуказанной модели сонификации (600):

– действие allow (разрешить) - шелест листьев деревья от ветра (право);
– действие deny (отклонить) - звук горящего фейерверка (лево);
– действие alert (тревога) - сверчки, редко птица (лево)
– действие drop (скидывание) - воробьи и другие птицы (право)
– действие reset (сброс) - филин (право)
– действие не определено - (лево) свист ветра;
– ip-адрес из черного списка - переливы, ловец ветра (центр);
– сетевой порт из черного списка - колокола (центр).

[0049] Представленные схемы и примеры распределения источников звука представлены только в целях отображения одного из примеров формирования звукового окружения.

[0050] На Фиг. 7 представлен пример общего вида вычислительной системы (700) на базе вычислительного устройства, которое обеспечивает реализацию заявленного способа. Вычислительное устройство может представлять собой компьютерное устройство, пригодное для исполнения функционала по сонификации и обработки данных, например, персональной компьютер, ноутбук, смартфон, планшет, сервер и т.п. Устройство (200) может представлять собой частный вариант исполнения вычислительной системы (700).

[0051] В общем случае, система (700) содержит объединенные общей шиной (710) информационного обмена один или несколько процессоров (701), средства памяти, такие как ОЗУ (702) и ПЗУ (703), интерфейсы ввода/вывода (704), устройства ввода/вывода (705), и устройство для сетевого взаимодействия (706).

[0052] Процессор (701) (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 обработки и сонификации данных. При этом, средством памяти может выступать доступный объем памяти графической карты или графического процессора.

[0053] ОЗУ (702) представляет собой оперативную память и предназначено для хранения исполняемых процессором (701) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (702), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

[0054] ПЗУ (703) 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.

[0055] Для организации работы компонентов вычислительной системы (700) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (704). 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.

[0056] Для обеспечения взаимодействия пользователя с вычислительной системой (300) применяются различные средства (705) 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.

[0057] Средство сетевого взаимодействия (706) обеспечивает передачу данных системой (300) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (706) 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.

[0058] Дополнительно могут применяться также средства спутниковой навигации в составе системы (400), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0059] Модификации и улучшения вышеописанных вариантов осуществления настоящего технического решения будут ясны специалистам в данной области техники. Предшествующее описание представлено только в качестве примера и не несет никаких

ограничений. Таким образом, объем настоящего технического решения ограничен только объемом прилагаемой формулы изобретения.

Источники информации:

1. Рогозинский Г.Г. Модели и методы сонификации киберфизических систем / Диссертация, Санкт-Петербург, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019 г.
2. Debashi M, Vickers P (2018) Sonification of network traffic flow for monitoring and situational awareness. PLoS ONE 13(4): e0195948. https://doi.org/10.1371/journal.pone.0195948

ФОРМУЛА

1. Компьютерно-реализуемый способ сонификации событий кибербезопасности, генерируемых средствами сетевой защиты, выполняемый с помощью процессора и содержащий этапы, на которых:

- осуществляют сбор данных событий кибербезопасности, которые включают в себя IP-адреса узлов сетевого обмена, время выполнения соединений между узлами и реакция средств сетевой защиты на упомянутые соединения;
- агрегируют полученные IP-адреса по принадлежности к зонам сети передачи данных и вычисляют статистические характеристики соединений между узлами каждой агрегированной зоны сети в заданном временном интервале;
- генерируют схему сонификации событий на основании упомянутых статистических характеристик соединений между узлами сети, причем упомянутая схема формируется, как:

  источник звука – зона сети,

  количество соединений в зоне сети – громкость источника звука,

  отклонение от среднего значения во временном интервале – частота повторения звука упомянутого источника во временном интервале,

  соотношение заблокированных и разрешенных соединений для каждой зоны - тембр/высота тона звучания источника;
- формируют звуковые оповещения на поступающие уведомления кибербезопасности в соответствии с упомянутой схемой сонификации.

2. Способ по п.1, характеризующийся тем, что дополнительно осуществляется визуализация зон сети и соединений между ними в режиме реального времени.

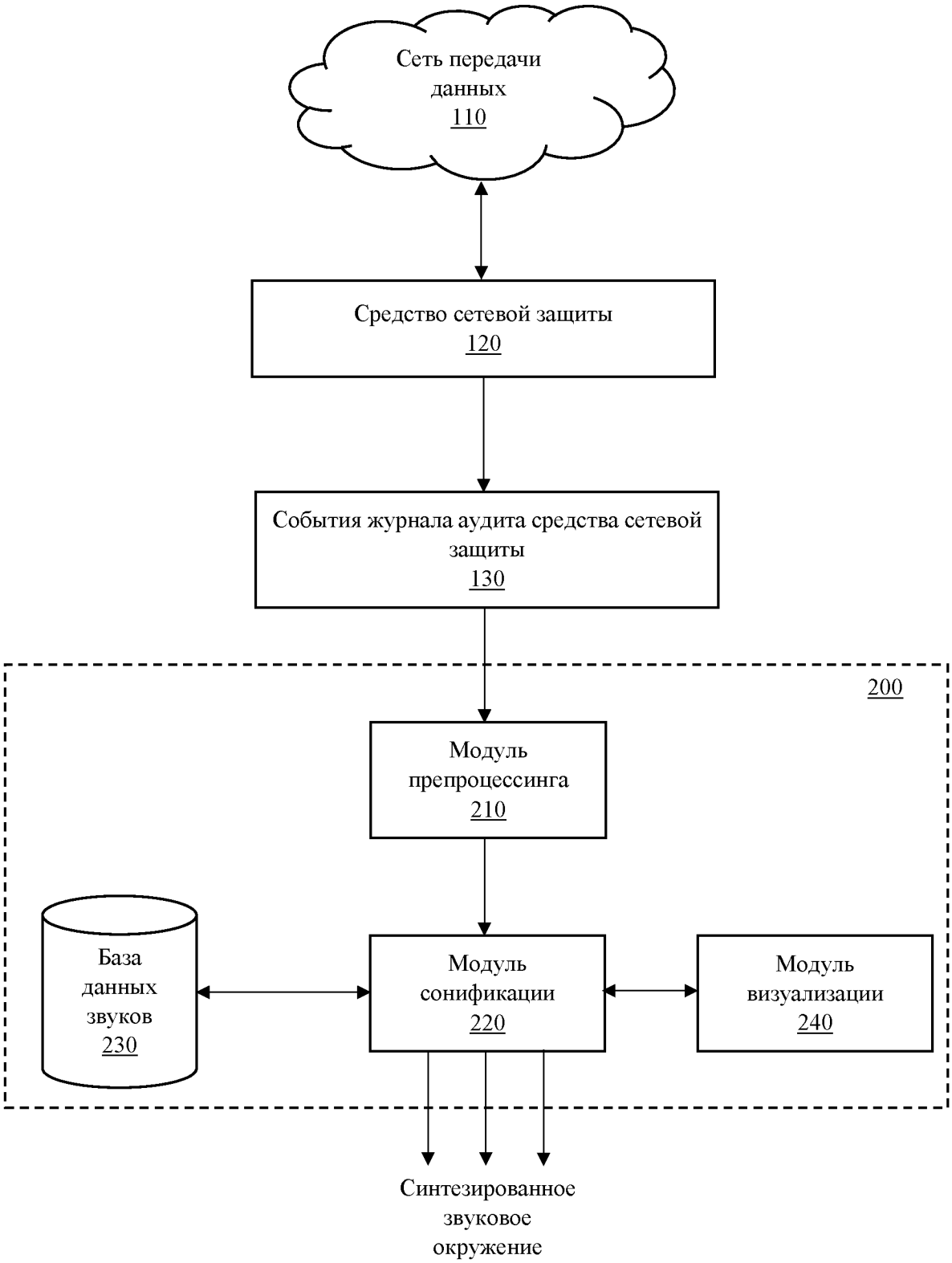
3. Способ по п.2, характеризующийся тем, что визуализация выполняется синхронно с формированием звуковых оповещений.

4. Способ по любому из пп. 1 - 3, характеризующийся тем, что звуковое оповещение и/или визуализация зон сети передается на мобильное устройство пользователя.

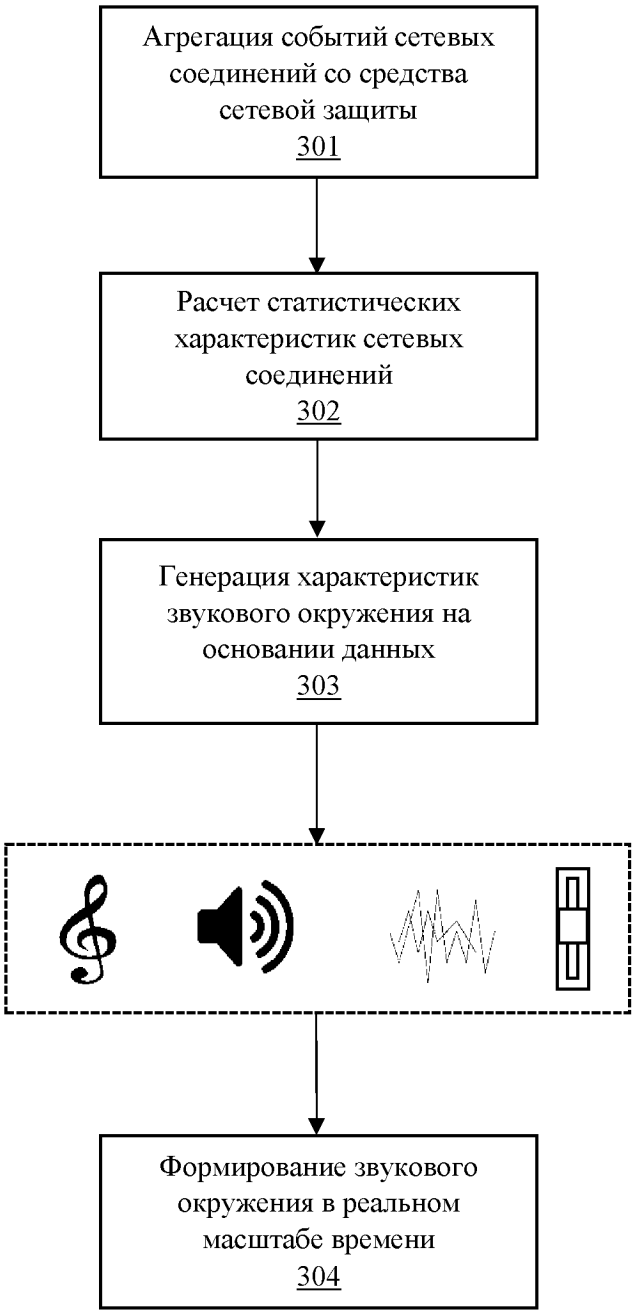
5. Способ по п.1, характеризующийся тем, что источник выбирается из группы: музыкальный инструмент, звуки окружающей природы, звуки животных, звуки природы, синтезированные звуки или их сочетания.

6. Система сонификации событий кибербезопасности, генерируемых средствами сетевой защиты, содержащая по меньшей мере один процессор и по меньшей мере одно

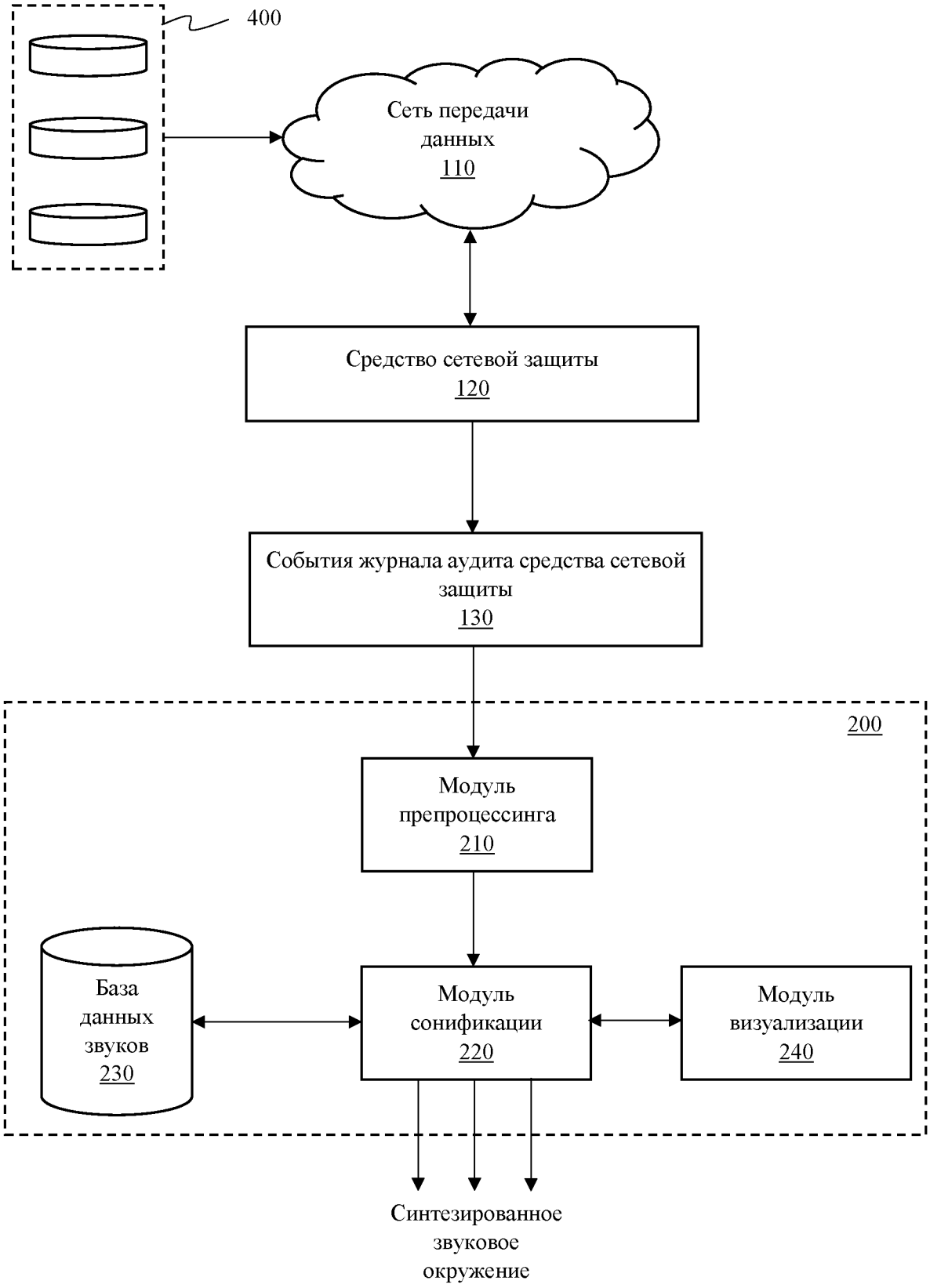
средство хранения данных, содержащее машиночитаемые инструкции, которые при их исполнении процессором выполняют способ по любому из пп. 1-5.


Сеть передачи данных
110
Средство сетевой защиты
120
События журнала аудита средства сетевой защиты
130
200
Модуль препроцессинга
210
База данных звуков
230
Модуль сонификации
220
Модуль визуализации
240
Синтезированное звуковое окружение

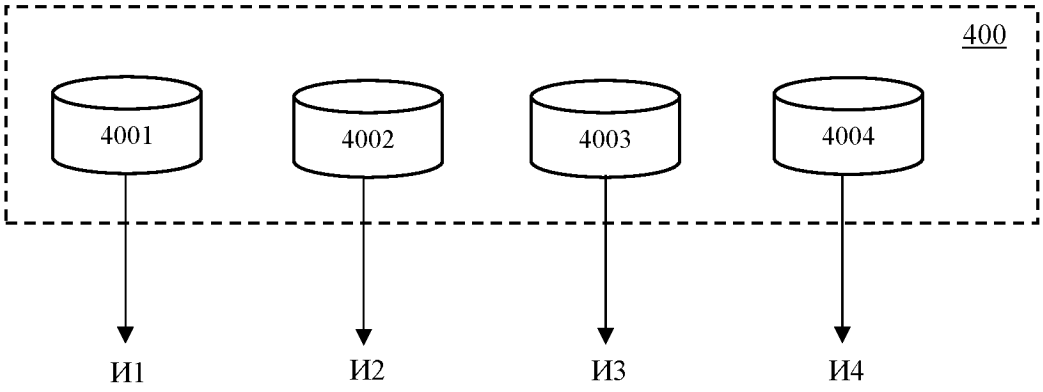
Фиг. 1


Агрегация событий сетевых соединений со средства сетевой защиты
301
Расчет статистических характеристик сетевых соединений
302
Генерация характеристик звукового окружения на основании данных
303
Формирование звукового окружения в реальном масштабе времени
304

Фиг. 2


400
Сеть передачи данных
110
Средство сетевой защиты
120
События журнала аудита средства сетевой защиты
130
200
Модуль препроцессинга
210
База данных звуков
230
Модуль сонификации
220
Модуль визуализации
240
Синтезированное звуковое окружение

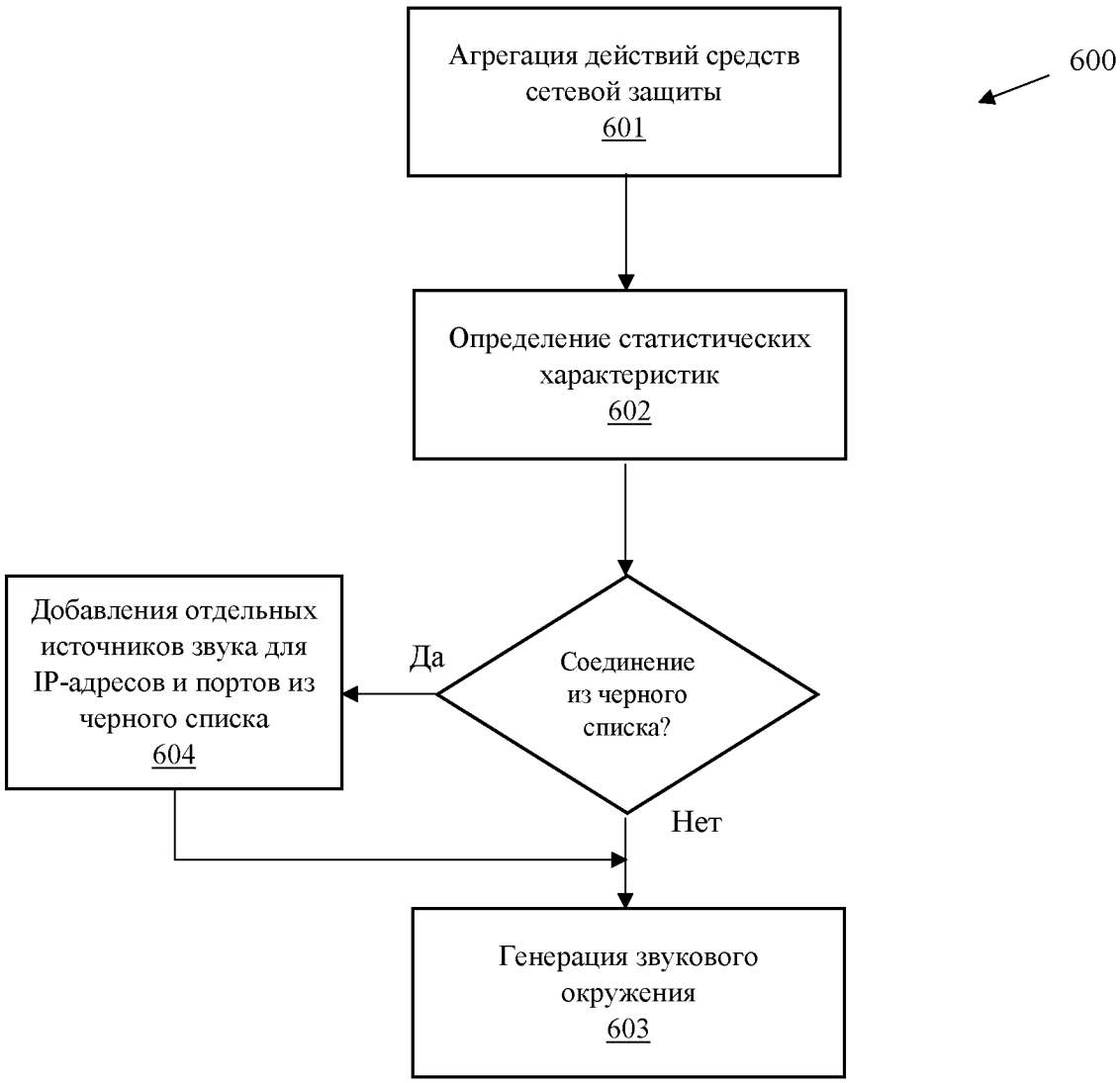
Фиг. 3


400
4001
4002
4003
4004
И1
И2
И3
И4

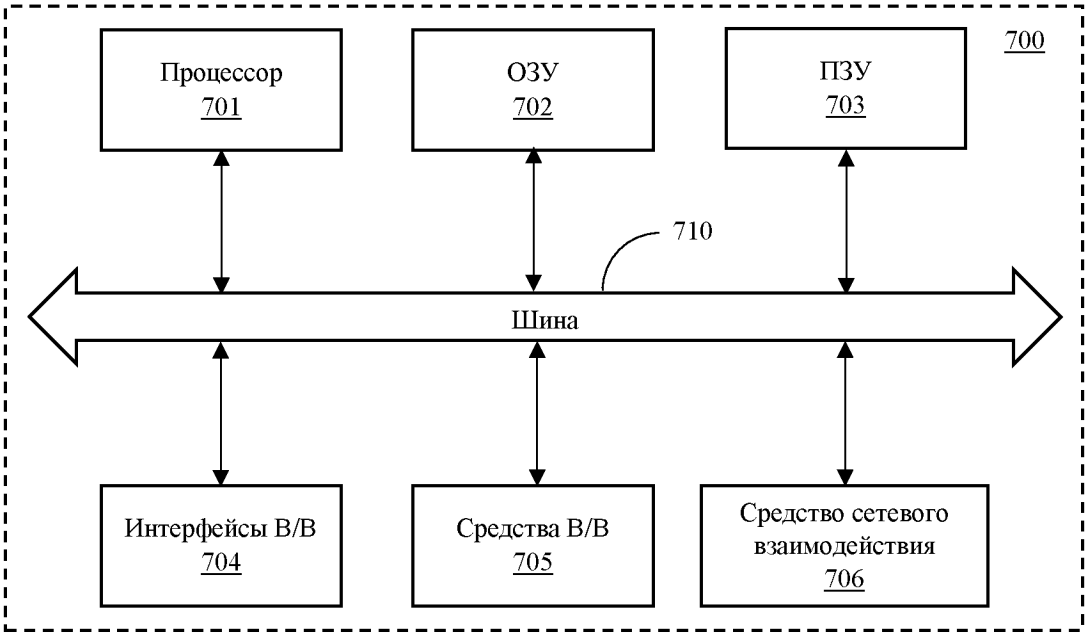
Фиг. 4


500
Агрегация событий сетевых соединений по транспортному протоколу
501
Определение статистических характеристик
502
Соединение из черного списка?
Да
Нет
Добавления отдельных источников звука для IP-адресов и портов из черного списка
504
Генерация звукового окружения
503

Фиг. 5


Агрегация действий средств сетевой защиты
601
600
Определение статистических характеристик
602
Соединение из черного списка?
Да
Нет
Добавления отдельных источников звука для IP-адресов и портов из черного списка
604
Генерация звукового окружения
603

Фиг. 6


Процессор
701
ОЗУ
702
ПЗУ
703
700
710
Шина
Интерфейсы В/В
704
Средства В/В
705
Средство сетевого
взаимодействия
706

Фиг. 7

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

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

Номер евразийской заявки:

201991970

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

G06F 21/55 *(2013.01)*
G08B 31/00 *(2006.01)*

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G06F 21/00 – 21/55, H04L 29/00 – 29/06, G10L 25/00 – 25/51, G10H 1/00, H04L 63/00 – 63/145, G06N 99/00

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
ESP@CENET, K-PION, PAJ, RUPTO, USPTO, WIPO, GOOGLE, ЕАПАТИС

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X	US2019/0253441 A1, (CISCO TECHNOLOGY, INC), 15.08.2019 реферат, абзацы [0023] - [0026], [0030], [0046], фиг. 9	1, 6
Y		2 – 5
Y	US2015/0213789 A1, (CALIFORNIA INSTITUTE OF TECHNOLOGY), 30.07.2015 реферат, абзац [0049]	2 – 5
A	COURTNEY FALK et al, «SONIFICATION WITH MUSIC FOR CYBERSECURITY SITUATIONAL AWARENESS»,The 25th International Conference on Auditory Display, Northumbria University, 23 – 27 June 2019, размещено в Интернет: https://smartech.gatech.edu/bitstream/hadle/ 1853/61496/ icad2019_014.pdf; jsesionid =88B7D39DDA44132FD6C5CFB6C9785ECE.smart1?sequence=1	1 – 6
A	RU2680756 C1, (ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ОБРАЗОВАТЕЛЬНОЙ ПОЛИТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»), 26.02.2019	1 – 6

☐ 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: **18/12/2020**

Уполномоченное лицо:
Начальник отдела механики,
физики и электротехники

Д.Ф. Крылов