(19) Евразийское патентное ведомство

(21) 201992874 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2020.05.08

(22) Дата подачи заявки
2018.04.12

(51) Int. Cl. ***G06F 21/60*** (2013.01)
G06F 21/71 (2013.01)

(54) СИСТЕМЫ И СПОСОБЫ ДЛЯ УПРАВЛЕНИЯ ЭФЕМЕРНЫМ СОВМЕСТНО ИСПОЛЬЗУЕМЫМ НАБОРОМ ДАННЫХ И ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ДАННЫХ

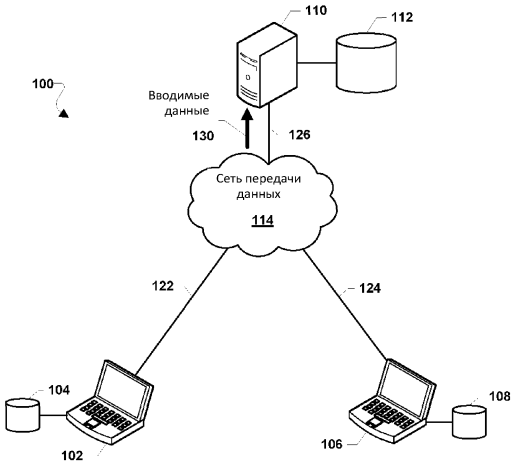
(31) **62/513,047; 15/788,981**
(32) **2017.05.31; 2017.10.20**
(33) **US**
(86) **PCT/US2018/027316**
(87) **WO 2018/222281 2018.12.06**

(71) Заявитель:
ИНФОСКИ, ЛЛК (US)

(72) Изобретатель:
Эллингсон Джон, Ричардсон Мэтью (US)

(74) Представитель:
Рыбина Н.А., Рыбин В.Н. (RU)

(57) Различные варианты воплощения изобретения предоставляют способы и вычислительные устройства, предусматривающие реализацию способов динамического изменения эфемерного совместно используемого набора данных. Различные варианты воплощения изобретения предоставляют способы и вычислительные устройства, предусматривающие реализацию способов динамического генерирования значения, которое может использоваться для защиты передаваемых данных на основе динамически измененного эфемерного совместно используемого набора данных. Различные варианты воплощения изобретения включают предположение о том, что доверенные системы в конечном счете явно небезопасны, поскольку такие системы являются проницаемыми и уязвимыми. Различные варианты воплощения изобретения предоставляют систему цифровой связи, которая не предполагает доверия между различными сетевыми элементами, по меньшей мере, по той причине, что цифровая среда по своей природе ненадежна.



201992874 A1

201992874 A1

СИСТЕМЫ И СПОСОБЫ УПРАВЛЕНИЯ ЭФЕМЕРНЫМ СОВМЕСТНО ИСПОЛЬЗУЕМЫМ НАБОРОМ ДАННЫХ И ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ДАННЫХ

Перекрестные ссылки на родственные заявки

[0001] Эта заявка испрашивает приоритет предварительной заявки США № 15/788981, озаглавленной «Systems and Methods for Ephemeral Dynamic Shared Data Set Management and Communication Protection», поданной 20 октября 2017 г., которая испрашивает приоритет предварительной заявки США № 62/513047, озаглавленной «Systems and Methods for Dynamic Shared Data Set Management and Communication Protection», поданной 31 мая 2017 года.

УРОВЕНЬ ТЕХНИКИ

[0002] Развитие цифровой среды позволяет, помимо всего прочего, значительно увеличить скорость соединений и возможности по обмену информацией. Однако парадигма безопасности из прошлого, используемая в подобной новой среде, имеет присущие ей особенности: концепцию общих секретов и сопутствующее ей доверие. Парадигма общего секрета включена в цифровую среду множеством способов, от имен пользователей и паролей до защиты передачи данных между пользователями и системами. Например, данная концепция является основополагающей для Протокола Защиты Информации (Secure Socket Layer), Центра Сертификации (Certificate Authority), инфраструктуры защиты Информации с Открытым Ключом (Public Key Information).

[0003] Однако цифровой среде присуща особенность, суть которой заключается в том, что секреты трудно хранить дольше, чем на протяжении небольшого периода времени и, после снятия грифа

секретности, подобная информация может быстро распространяться, причем она является полностью достоверной. В цифровой среде общие секреты и учетные данные являются основными целями для «взлома», в результате этого многие «секреты» (например, пароли, цифровые сертификаты, личная информация и другие типы данных аутентификации) становятся товаром, который свободно обращается на сером и черном рынках, нивелируя преимущества, связанные с применением секретов для обеспечения безопасности цифровых бирж. Основной механизм обеспечения безопасности цифровой среды по-прежнему зависит от того, является ли истинным предположение о том, что секрет все еще остается секретом.

[0004] Проверка представленной идентичности и аутентификация вычислительного устройства является критическим моментом для многочисленных электронных коммуникаций. Однако, уязвимость общих секретов, а также уязвимость сообщений в процессе их передачи резко снижают надежность и безопасность цифровых сертификатов или другой аналогичной информации, которая служит для проверки подлинности доверенных устройств.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

[0005] Различные варианты воплощения предоставляют способы и вычислительные устройства, сконфигурированные для реализации способов непрерывного обновления и изменения совместно используемого набора данных. Различные варианты воплощения предоставляют способы и вычислительные устройства, сконфигурированные с возможностью воплощения способов динамического генерирования значения, которое может использоваться для защиты передаваемых данных на основе динамически изменяемого (например, эфемерного) совместно

используемого набора данных. Различные варианты воплощения включают в себя предположение о том, что доверенные системы в конечном счете явно небезопасны, поскольку такие системы являются проницаемыми и уязвимыми. Различные варианты воплощения предоставляют систему цифровой передачи данных, которая не предполагает доверия между различными сетевыми элементами по меньшей мере по той причине, что цифровая среда по своей природе ненадежна.

[0006] Различные варианты воплощения включают в себя способы, которые могут быть реализованы на процессоре вычислительного устройства (например, на устройстве управления наборами данных). Различные варианты воплощения могут включать в себя предоставление эфемерного совместно используемого набора данных из устройства управления наборами данных первому вычислительному устройству и второму вычислительному устройству, генерирование инструкции для изменения эфемерного совместно используемого набора данных и отправку сгенерированной инструкции первому вычислительному устройству и второму вычислительному устройству для изменения эфемерного совместно используемого набора данных на первом и втором вычислительных устройствах в соответствии со сгенерированной инструкцией, так что эфемерный совместно используемый набор данных, сохраненный в первом вычислительном устройстве, совпадает с эфемерным совместно используемым набором данных, сохраненным во втором вычислительном устройстве.

[0007] В некоторых вариантах воплощения процесс генерирования инструкции для изменения совместно используемого набора данных может включать в себя определение наличия триггера обновления набора данных, и генерирование инструкции для изменения эфемерного

совместно используемого набора данных в ответ на определение наличия триггера обновления набора данных. В некоторых вариантах воплощения процесс генерирования инструкции для изменения совместно используемого набора данных может включать в себя генерирование инструкции для замены эфемерного совместно используемого набора данных заменяющим набором данных, устанавливаемым устройством управления набором данных.

[0008] В некоторых вариантах воплощения изобретения процесс генерирования инструкции для изменения эфемерного совместно используемого набора данных может включать в себя генерирование инструкции для добавления новой части в эфемерный совместно используемый набор данных на основе входных данных, принятых устройством управления набором данных. В некоторых вариантах воплощения генерирование инструкции для изменения эфемерного совместно используемого набора данных может включать в себя генерирование инструкции для вычитания части совместно используемого набора данных. В некоторых вариантах воплощения генерирование инструкции для изменения эфемерного совместно используемого набора данных может включать в себя генерирование инструкции для переупорядочения эфемерного совместно используемого набора данных. В некоторых вариантах воплощения генерирование инструкции для изменения эфемерного совместно используемого набора данных может включать в себя генерирование инструкции для преобразования эфемерного совместно используемого набора данных. В некоторых вариантах воплощения способ может дополнительно включать в себя выполнение операции синхронизации с первым вычислительным устройством и вторым вычислительным устройством, так что измененный набор данных, сохраненный в первом вычислительном устройстве,

является таким же, как измененный набор данных, сохраненный во втором вычислительном устройстве.

[0009] Различные варианты воплощения включают в себя способы, которые могут быть реализованы на процессоре вычислительного устройства для защиты передаваемых данных. Различные варианты воплощения могут включать в себя выбор элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, генерирование набора правил, указывающих на выбранные элементы, отправку сгенерированного набора правил второму вычислительному устройству, генерирование результата на основе выбранных элементов, получение зашифрованных данных, передаваемых вторым вычислительным устройством, попытку расшифровать зашифрованные данные, используя сгенерированный результат, и определение успешности попытки расшифровки.

[0010] В некоторых вариантах воплощения выбор элементов из эфемерного совместно используемого набора данных, хранящегося на вычислительном устройстве и на втором вычислительном устройстве, может включать в себя прием инструкций от устройства управления набором данных для извлечения элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и во втором вычислительном устройстве, и извлечение элементов из совместно используемого набора данных в соответствии с инструкциями. В таких вариантах воплощения выбор элементов из совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, может включать в себя выбор элементов из уже извлеченных элементов. В некоторых вариантах воплощения изобретения способ может

дополнительно включать в себя шифрование линий передачи данных с использованием первого результата в ответ на определение успешности попытки расшифровки, и отправку зашифрованных данных второму вычислительному устройству.

[0011] Дополнительные варианты воплощения изобретения могут включать в себя вычислительные устройства, имеющие схему исполняемых процессором инструкций для выполнения операций способами, которые суммируют приведенные выше. Дополнительные варианты воплощения могут включать в себя считываемые процессором носители данных, на которых хранятся исполняемые процессором инструкции, предусматривающие инициировать процессор вычислительного устройства выполнять операции способами, описанными выше. Дополнительные варианты воплощения могут включать в себя вычислительные устройства, содержащие средства, предназначенные для выполнения функций с учетом способов, описанных выше.

КРАТКОЕ ОПИСАНИЕ ГРАФИЧЕСКИХ МАТЕРИАЛОВ

[0012] Прилагаемые графические материалы, которые содержатся в данном документе и составляют часть этого описания, иллюстрируют примеры вариантов воплощения изобретения и, вместе с общим описанием, приведенным выше, и подробным описанием, приведенным ниже, служат для объяснения признаков изобретения.

[0013] На ФИГ. 1 проиллюстрирована блок-схема компонента системы передачи данных, подходящей для использования с различными вариантами воплощения изобретения.

[0014] На ФИГ. 2 проиллюстрирована блок-схема компонента устройства передачи данных, подходящая для использования с различными вариантами воплощения изобретения.

[0015] На ФИГ. 3 проиллюстрирована блок-схема процесса, иллюстрирующая способ 300 управления эфемерным совместно используемым набором данных, подходящая для использования с различными вариантами воплощения изобретения.

[0016] На ФИГ. 4 проиллюстрированы отношения между элементами частей набора данных 500, подходящие для использования с различными вариантами воплощения изобретения.

[0017] На ФИГ. 5A-5D проиллюстрированы отношения между элементами частей эфемерных совместно используемых наборов данных 500a-500d, подходящих для использования с различными вариантами воплощения изобретения.

[0018] На ФИГ. 6A-6C проиллюстрированы представления способов управления эфемерным совместно используемым набором данных, подходящие для использования с различными вариантами воплощения изобретения.

[0019] На ФИГ. 6D проиллюстрировано преобразование первого набора данных или типа данных во второй набор данных или тип данных.

[0020] На ФИГ. 7 проиллюстрирован способ управления синхронизацией 700 эфемерного совместно используемого набора данных, подходящий для использования с различными вариантами воплощения изобретения.

[0021] На ФИГ. 8A проиллюстрирован способ 800A для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0022] На ФИГ. 8B проиллюстрирован способ 800B для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0023] На ФИГ. 9A проиллюстрирован способ 900A для защиты передаваемых данных, подходящий для использования с различными

вариантами воплощения изобретения.

[0024] На ФИГ. 9B проиллюстрирован способ 900B для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0025] На ФИГ. 10A проиллюстрирован способ 1000A для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0026] На ФИГ. 10B проиллюстрирован способ 1000B для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0027] На ФИГ. 11A проиллюстрирован способ 1100A для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0028] На ФИГ. 11B проиллюстрирован способ 1100B для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0029] На ФИГ. 12A проиллюстрирован способ 1200A для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0030] На ФИГ. 12B проиллюстрирован способ 1200B для защиты передаваемых данных, подходящий для использования с различными вариантами воплощения изобретения.

[0031] На ФИГ. 13 проиллюстрирована блок-схема компонента мобильного беспроводного вычислительного устройства, которая подходит для реализации различных вариантов воплощения изобретения.

[0032] На ФИГ. 14 проиллюстрирована блок-схема компонента портативного устройства беспроводной передачи данных, которая подходит для реализации различных вариантов воплощения изобретения.

[0033] На ФИГ. 15 проиллюстрирована блок-схема компонента серверного устройства, которая подходит для реализации различных вариантов воплощения изобретения.

ПОДРОБНОЕ ОПИСАНИЕ

[0034] Различные варианты воплощения изобретения будут подробно описаны со ссылкой на прилагаемые фигуры. Везде, где возможно, одни и те же ссылочные позиции будут использоваться на всех фигурах для обозначения одинаковых или похожих элементов. Ссылки на конкретные примеры и реализации приведены для иллюстративных целей и не предназначены для ограничения объема изобретения или формулы изобретения.

[0035] Различные варианты воплощения изобретения предоставляют способы и вычислительные устройства (или другие цифровые или программируемые устройства), предусматривающие реализацию способов, которые позволяют управлять совместно используемым набором данных. В различных вариантах воплощения изобретения совместно используемый набор данных может храниться на двух или более вычислительных устройствах. В некоторых вариантах воплощения изобретения совместно используемый набор данных может быть динамическим и может время от времени изменяться. В различных вариантах воплощения изобретения совместно используемый набор данных может быть эфемерным и может изменяться через относительно короткий период времени. В некоторых вариантах воплощения изобретения динамически измененный совместно используемый набор данных может предоставлять огромное количество сложных случайных данных с использованием относительно небольшого набора начальных данных. В различных вариантах воплощения изобретения эфемерный

совместно используемый набор данных может применяться двумя или более вычислительными устройствами для генерирования динамического значения. В некоторых вариантах воплощения изобретения динамически генерируемое значение может использоваться для защиты линии передачи данных между двумя или более вычислительными устройствами.

[0036] В различных вариантах воплощения изобретения система передачи данных может использовать динамически изменяющиеся совместно используемые данные и динамически генерируемое значение для защиты передачи данных таким образом, чтобы не полагаться на парадигму общих секретов и статической информации.

[0037] Поскольку эфемерный совместно используемый набор данных может время от времени динамически изменяться (например, при возникновении события запуска, периодически, апериодически и т. д.) и динамически генерируемое значение может основываться на динамически изменяющемся эфемерном совместно используемом наборе данных, различные варианты воплощения изобретения улучшают функцию безопасности любой сети передачи данных или любой системы электронной передачи данных, усиливая безопасность линии передачи данных. Различные варианты воплощения также совершенствуют функцию безопасности любой сети или системы передачи данных, используя эфемерный (динамически изменяющийся) совместно используемый набор данных и динамически генерируемое значение, не полагаясь на легко компрометирующую себя статическую идентификационную информацию, такую как общий секрет (например, общий сертификат для общего ключа, например, который может использоваться в инфраструктуре открытого ключа (PKI)), которая может быть уязвимой для атаки путем доступа и/или копирования. Различные варианты воплощения изобретения также совершенствуют функцию

безопасности любой сети или системы передачи данных, поскольку динамический, совместно используемый набор данных не передается от одного вычислительного устройства к другому. Различные варианты воплощения изобретения также повышают степень безопасности функций любой сети или системы обмена данными, поскольку динамически генерируемое значение не передается между вычислительными устройствами.

[0038] Термин «вычислительное устройство» относится к любому программируемому компьютеру или процессору, который иметь схему программируемых инструкций для выполнения различных способов воплощения. Вычислительное устройство может содержать одно или все из персональных компьютеров, ноутбуков, планшетных компьютеров, сотовых телефонов, смартфонов, сотовых телефонов с поддержкой Интернета, электронных устройств с поддержкой Wi-Fi, карманных компьютеров, переносных вычислительных устройств (включая смарт-часы, ожерелья, медальоны и любое вычислительное устройство, выполненное с возможностью ношения, прикрепления к носимому предмету или встроенное в носимый предмет), беспроводных вспомогательных устройств, карт памяти, ключей, беспроводных периферийных устройств, устройств Интернета вещей (IoT), автономных транспортных средств, полуавтономных транспортных средств и транспортных средств с дистанционным управлением, интеллектуальных огнестрельных оружий, сетевых элементов, таких как серверы, маршрутизаторы, шлюзы и тому подобное (включая так называемые «облачные» вычислительные устройства), и аналогичных электронных устройств, оснащенных радиосвязью ближнего действия (например, радио Bluetooth, Peanut, ZigBee и/или Wi-Fi и т. д.) и/или подключенных к глобальной сети (например, с использованием одной или более

технологий сотового радиодоступа для передачи данных с использованием беспроводного трансивера глобальной сети или проводного соединения с сетью передачи данных).

[0039] Термины «компонент», «система» и тому подобное обозначают связанные с компьютером сущности, такие как, но не ограничиваясь ими, оборудование, прошивку, комбинации аппаратных и программных средств, программы или исполняемые программы, которое настроены для выполнения определенных операций или функций. Например, компонент может быть, но не ограничивается этим, процессом, выполняющимся на процессоре, объектом, исполняемым файлом, потоком выполнения, программой и/или компьютером. В качестве иллюстрации, и приложение, работающее на беспроводном устройстве, и само беспроводное устройство могут называться компонентом. Один или более компонентов могут находиться в процессе и/или потоке выполнения, и компонент может быть локализован на одном процессоре или ядре и/или распределен между двумя или более процессорами или ядрами. Кроме того, эти компоненты могут выполняться с различных постоянных машиночитаемых носителей, на которых хранятся различные инструкции и/или структуры данных. Компоненты могут связываться посредством локальных и/или удаленных процессов, функций или вызовов процедур, электронных сигналов, пакетов данных, посредством чтения/записи в память и другими известными методологиями передачи данных, связанными с компьютером, процессором и/или процессом.

[0040] Помимо прочего, цифровая среда обеспечивает быстрые коммуникации и информационные транзакции в глобальном масштабе. Однако текущая цифровая среда опирается на шаткую основу безопасности: старую парадигму статического распространения секретов. Существуют многочисленные фундаментальные различия между чисто

человеческой средой, в которой мы работали на протяжении тысячелетий до конца 20-го века, и цифровой средой, в которой мы работаем сегодня.

[0041] Кроме того, цифровая среда является такой средой, в которой трудно сохранить секреты в течение какого-то времени. Если секретность утеряна, ранее секретная информация может быстро распространяться с полной точностью и использоваться злоумышленниками. Сбои в защите цифровых систем, приводящие к массовым утечкам данных, стали почти обычным явлением, и частота сбоев растет.

[0042] На самом деле быстрое развитие индустрии кибербезопасности, стоимость которой уже достигла нескольких миллиардов долларов, свидетельствует об общем кризисе системы безопасности в цифровой среде. В качестве одного из примеров можно отметить, что киберпреступления, такие как мошенничество с использованием личных данных, находятся в числе наиболее быстро растущих преступлений, а угрозы и возможности их реализации продолжают возрастать. Широкое распространение устройств, подключенных к сети, в том числе смартфонов, переносных компьютеров, игровых систем, устройств Интернета вещей и т. п. усугубляет масштабы и степень угроз цифровой безопасности. Например, многие из этих устройств либо сами не заслуживают доверия, либо взаимодействуют с ненадежными мобильными сетями, и лишь немногие подобные устройства обладают вычислительной мощностью, которая была бы достаточной для реализации традиционных функций безопасности привычных настольных компьютеров и ноутбуков.

[0043] В большинстве случаев реализации взлома, его причиной является нарушение доверия или неправильное использование общего секрета (например, учетных данных). В то время как в определенных случаях конкретный сбой безопасности может быть связан с недостатком технологий, используемых для обеспечения доверия и безопасности, в

целом сбои безопасности в цифровой среде происходят в широком спектре отраслей, использующих различные современные технологии. Сбои в системе безопасности происходят по всем направлениям и связаны не только с какой-либо конкретной технологией, но также с практикой и процедурами, присущими применению и использованию технологии. Таким образом, сбои безопасности в цифровой среде имеют в основе нечто более фундаментальное и эндемичное, что находится в корневой стратегии парадигмы доверия общего секрета, которая терпит неудачу.

[0044] Современная устаревшая парадигма цифровой безопасности терпит неудачу по меньшей мере по трем фундаментальным причинам: (1) данная парадигма основана на доверии, а доверие часто нарушается или бывает безосновательно; (2) данная парадигма основана на поддержании стабильных или статических общих секретов, но секреты не остаются таковыми и так же используются злоумышленником, как и авторизованным пользователем; и (3) наличие огромного числа информационных транзакций между анонимами (незнакомцами). Таким образом, «системы доверия» в конечном итоге не работают должным образом, поскольку они проницаемы и уязвимы. Более того, современные «системы доверия» уязвимы для проникновения и эксплуатации в значительной степени вследствие использования статической или постоянной информации, которая не изменяется во времени (или продолжительности); и, конечно же, имеют место «уязвимые места» в политике и роли человеческих факторов (например, социальная инженерия, халатность и т. д.). Уязвимость распространяемых секретов резко подрывает надежность цифровых сертификатов или другой подобной информации, которая должна служить для защиты передаваемых данных.

[0045] Различные варианты воплощения изобретения, раскрытые в этой заявке, относятся к вопросам уязвимости безопасности цифровых систем и

улучшают электронную безопасность при поддержке обмена данными между устройствами. Различные варианты воплощения изобретения предоставляют реализованные на компьютере способы для обеспечения постоянного обновления и изменения эфемерного совместно используемого набора данных. Различные варианты воплощения предоставляют реализованные на компьютере способы обеспечения динамического генерирования значений, которое может использоваться для защиты передачи данных на основе динамически измененного эфемерного совместно используемого набора данных. Различные варианты воплощения изобретения включают в себя предположение о том, что доверенные системы, в конечном счете, явно небезопасны, поскольку такие системы являются проницаемыми и уязвимыми. Различные варианты воплощения изобретения обеспечивают цифровые системы передачи данных, которые не предполагают наличия доверия между различными элементами сети по меньшей мере по той причине, что цифровая среда по своей сути ненадежна.

[0046] Различные варианты воплощения изобретения позволяют генерировать огромное количество случайных данных из относительно небольшого начального набора информации. Различные варианты воплощения изобретения обеспечивают динамическое изменение набора данных таким образом, что набор данных изменяется непредсказуемо. В некоторых вариантах воплощения изобретения динамически измененный набор данных или его подмножество может предоставляться или приниматься двумя или более вычислительными устройствами, так что каждое из двух или более вычислительных устройств сохраняет эфемерный совместно используемый набор данных. В некоторых вариантах воплощения изобретения эфемерный совместно используемый набор данных двух или более вычислительных устройств может

динамически изменяться. В некоторых вариантах воплощения изобретения изменения эфемерных совместно используемых наборов данных могут быть синхронизированы таким образом, чтобы измененный набор данных оставался общим для двух или большего числа вычислительных устройств.

[0047] Различные варианты воплощения изобретения позволяют генерировать динамическое значение двумя или более вычислительными устройствами. В некоторых вариантах воплощения изобретения динамическое значение генерируется на основе эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения динамическое значение может использоваться для шифрования процесса обмена данными между двумя или большим количеством вычислительных устройств.

[0048] Различные варианты воплощения изобретения также улучшают функцию безопасности любой сети или системы передачи данных, поскольку динамический совместно используемый набор данных не передается от одного вычислительного устройства к другому устройству. Различные варианты воплощения изобретения также улучшают функцию безопасности любой сети или системы передачи данных, поскольку динамически сгенерированное значение не передается от одного вычислительного устройства к другому устройству.

[0049] Поскольку общим вектором угрозы обычно является кража учетных данных, таких как сертификаты и информация о ключах, а не использование вычислительной мощности для дешифрования кодированной аутентифицирующей информации, различные варианты воплощения изобретения повышают безопасность данных, передаваемых по линиям передачи данных. В некоторых вариантах воплощения изобретения динамический совместно используемый набор данных может

существовать в одном состоянии в течение относительно короткого периода времени, который может составлять минуты или даже секунды. В некоторых вариантах воплощения изобретения динамическое значение может использоваться для шифрования и дешифрования только одного сообщения. Это отличается от действительной продолжительности сертификатов от обычного сертифицирующего органа (ЦС), которая в некоторых случаях может иметь продолжительность до десятилетий. Относительно короткая полезная продолжительность и характерная сложность эфемерного совместно используемого набора данных, а также динамическое значение уменьшают на порядки вероятность того, что такая информация будет угадана, доступна или «взломана», и затем применена как средство атаки системы.

[0050] Дополнительные подробности, относящиеся к различным вариантам воплощения изобретения, раскрыты в предварительной заявке США № 62/423 593, озаглавленной «Systems and Methods for Multipath Authentication», поданной 17 ноября 2016 г., в заявке на патент США № 15/395336, озаглавленной «Systems and Methods for Multipath Authentication», поданной 30 декабря 2016 г. и патентной заявке США № 15/493572, озаглавленной «Systems and Methods for Device Verification and Authentication», поданной 21 апреля 2017 г., и все они включены в настоящий документ в качестве ссылки в полном объеме.

[0051] Различные варианты воплощения изобретения включают в себя системы и способы для управления эфемерным совместно используемым набором данных, который сохраняется двумя или более вычислительными устройствами. В различных вариантах воплощения два или более вычислительных устройства могут содержать любые два конечных устройства в вычислительной сети, такие как пользовательское устройство, сетевой сервер, сервер аутентификации или другое

вычислительное устройство. Эфемерный совместно используемый набор данных может быть скомпилирован с течением времени и может изменяться вычислительным устройством случайным образом, периодически и/или при возникновении события-триггера. Процесс внесения изменений или изменение эфемерного совместно используемого набора данных может включать в себя переупорядочение одной или более частей набора данных, добавление информации в набор данных, вычитание информации из набора данных и/или преобразование одной или более частей эфемерного совместно используемого набора данных. Эфемерный совместно используемый набор данных может содержать две или более частей. Каждая часть набора данных может содержать два или более элементов. В некоторых вариантах воплощения изобретения вычислительное устройство может определять взаимосвязь между двумя или более элементами эфемерного совместно используемого набора данных. Соотношение между двумя или более элементами может включать в себя сравнительную разницу между двумя или более элементами, такую как разница во времени, разница в местоположении, разница в положении, разница в цвете, разница в высоте тона, разница в частоте или другая разница. Соотношение между двумя или более элементами также может включать в себя сравнительную разницу между каждым из двух или более элементов и третьим элементом, таким как относительное время, местоположение, положение, цвет, высота, частота или другое различие.

[0052] В некоторых вариантах воплощения изобретения множество файлов может содержать множество файлов изображений. В различных вариантах воплощения изобретения вычислительные устройства могут использовать согласованный способ изменения эфемерного совместно используемого набора данных, который позволяет обоим вычислительным

устройствам изменять эфемерный совместно используемый набор данных при сохранении идентичного эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкции, предназначенные для изменения эфемерного совместно используемого набора данных, могут быть предоставлены вычислительным устройствам сетевым элементом, таким как диспетчер наборов данных (например, устройство управления набором данных). В некоторых вариантах воплощения изобретения изменения эфемерного совместно используемого набора данных могут динамически устанавливаться администратором набора данных и/или вычислительными устройствами (например, «на лету»).

[0053] В некоторых вариантах воплощения изобретения диспетчер наборов данных может динамически генерировать одну или более инструкций для изменения эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкции могут включать инструкцию для замены эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкция может включать инструкцию для добавления новой части набора данных. В некоторых вариантах воплощения изобретения инструкция может включать инструкцию для вычитания части эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкция может включать инструкцию для переупорядочения эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкция может включать инструкцию для преобразования эфемерного совместно используемого набора данных.

[0054] В различных вариантах воплощения изобретения выполнение одного или более преобразований для эфемерного совместно

используемого набора данных позволяет генерировать очень большое количество непредсказуемых значений элементов и взаимосвязей между элементами данных из относительно небольшого количества частей. В различных вариантах воплощения изобретения простые вычисления или вычисления, которые не используют интенсивно процессор, могут создавать сложнейшие выражения из относительно небольшого и/или простого начального набора данных. В отличие от обычной секретной информации (такой как сертификат PKI, который представляет одномерные линейные вычисления), динамический набор данных может быть многомерным (n-мерным) и может предоставлять значительно большую сложность, превышая сложность обычной секретной информации на несколько порядков. Кроме того, различные варианты воплощения изобретения могут определять отношения между и среди элементов эфемерного совместно используемого набора данных. Выполнение преобразования набора данных может изменять различные отношения между и среди элементов данных. В качестве только одного примера, файл изображения может содержать множество пикселей, и каждый пиксель может быть связан с рядом различных значений, таких как информация о местоположении в файле изображения, цвет, оттенок, насыщенность, значение черно-белого изображения и другая подобная пиксельная информация. Даже без преобразования файл изображения может содержать уникальный набор информации. Затем процессор может выполнить преобразование для одного или более файлов изображений, тем самым изменяя не только значения различных пикселей в файлах преобразованного изображения, но также многочисленные взаимопередачи данных между элементами данных файлов из преобразованного изображения и другими частями набора данных.

[0055] В некоторых вариантах воплощения изобретения одно из

вычислительных устройств (первое вычислительное устройство) может отправлять указание менеджеру набора данных о том, что вычислительное устройство использует линию передачи данных для отправки данных второму вычислительному устройству. В ответ на указание от первого вычислительного устройства диспетчер наборов данных может генерировать инструкции для извлечения одного или более элементов из эфемерного совместно используемого набора данных и может отправлять инструкции извлечения первому и второму вычислительному устройству. Согласно инструкциям, первое и второе вычислительные устройства могут извлекать элементы из эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкции извлечения могут включать в себя указание элемента (ов), которые должны быть извлечены. В некоторых вариантах воплощения инструкции извлечения могут включать в себя набор правил, который позволяет каждому из первого и второго вычислительных устройств идентифицировать элемент(ы) эфемерного совместно используемого набора данных, подлежащих выборке. В некоторых вариантах воплощения изобретения инструкции извлечения могут включать инструкцию, применяемую для выполнения операции преобразования на одном или более из выбранных элементов. В различных вариантах воплощения изобретения инструкции извлечения могут давать возможность первому вычислительному устройству и второму вычислительному устройству динамически генерировать уникальный набор элементов, которые совместно используются первым вычислительным устройством и вторым вычислительным устройством (то есть извлеченные элементы хранятся в каждом, как в первом вычислительном устройстве, так и во втором вычислительном устройстве) на основе элементов в эфемерном совместно используемом наборе данных.

.**[0056]** В некоторых вариантах воплощения изобретения первое вычислительное устройство может выбирать элементы из числа извлеченных элементов. В некоторых вариантах воплощения изобретения первое вычислительное устройство может генерировать набор правил, указывающий выбранные элементы. Набор правил может идентифицировать выбранные элементы из числа извлеченных элементов данных из эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения вычислительное устройство может генерировать набор правил на основе одного или более отношений как между, так и среди выбранных элементов данных. В некоторых вариантах воплощения изобретения набор правил может идентифицировать первый элемент и одно или более отношений между первым элементом и другими элементами данных, которые позволяют вычислительному устройству выбирать элементы из извлеченных элементов на основе идентичности первого элемента и одного или большего числа связей с другими элементами данных. Первое вычислительное устройство может отправлять сгенерированный набор правил второму вычислительному устройству.

[0057] В качестве одного примера, эфемерный совместно используемый набор данных может включать в себя два или более файлов изображений, и каждый файл изображения может содержать множество пикселей (элементов изображения). Каждый файл изображения может быть связан с дополнительными данными, такими как метка времени или другая информация о времени, информация о местоположении и/или информация о геолокации, где получено изображение, информация о погоде и тому подобное. Каждый пиксель может быть связан с большим количеством информационных элементов, таких как местоположение координат в изображении, цвет, интенсивность, яркость и тому подобное.

Каждый пиксель также может быть связан с информацией соответствующего ему файла изображения. Таким образом, каждый пиксель может быть связан с большим количеством информационных элементов, которые могут рассматриваться как переменные. В некоторых вариантах воплощения изобретения набор правил может включать информацию, идентифицирующую один или более пикселей эфемерного совместно используемого набора данных. В некоторых вариантах воплощения набор правил может включать информацию, идентифицирующую один пиксель эфемерного совместно используемого набора данных, и информацию о взаимопередаче данных, которая позволяет идентифицировать один или более других пикселей с использованием идентифицированного первого пикселя и информации о взаимопередаче данных.

[0058] Эфемерный совместно используемый набор данных не ограничен файлами изображений, причем совместно используемый набор данных может быть сгенерирован или скомпилирован с использованием данных, которые могут содержать идентифицируемые элементы данных, и/или в которых могут быть определены отношения между двумя или более элементами данных. Примерами таких данных являются видеофайлы, аудиофайлы, биометрические образцы, данные местоположения (например, данные спутниковой системы глобального позиционирования) и тому подобное. Кроме того, набор правил может включать информацию, идентифицирующую один или более элементов данных компонента эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения набор правил может включать информацию, идентифицирующую один элемент данных, и информацию о взаимопередаче данных, которая позволяет идентифицировать один или более других элементов данных в наборе данных (например, элементы,

выбранные из извлеченных элементов данных).

[0059] В некоторых вариантах воплощения изобретения первое вычислительное устройство может генерировать первый результат на основе выбранных элементов. В некоторых вариантах воплощения изобретения сгенерированный результат может включать в себя строку данных. В некоторых вариантах воплощения изобретения сгенерированный результат может включать в себя значение, основанное на информации об элементах, выбранных из извлеченных элементов эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения первое вычислительное устройство может выполнять преобразование информации выбранных элементов, такое как генерирование хеша значений информации. В некоторых вариантах воплощения изобретения первое вычислительное устройство может генерировать строку данных на основе информации о выбранных элементах и может выполнять преобразование (например, генерировать хеш) на основе информации о выбранных элементах для генерирования первого результата.

[0060] В различных вариантах воплощения изобретения второе вычислительное устройство, содержащее элементы, которые извлечены из эфемерного совместно используемого набора данных, может принимать набор правил от первого вычислительного устройства и может использовать набор правил и извлеченные элементы эфемерного совместно используемого набора данных для выбора элементов из извлеченных элементов. Например, второе вычислительное устройство может применять набор правил к своим сохраненным извлеченным элементам данных для идентификации, например, пикселей и их связанного местоположения, порядка в наборе данных, числовых значений для цвета, плотности и т.д. В некоторых вариантах воплощения

изобретения второе вычислительное устройство может создавать строку данных на основе приложенного набора правил.

[0061] В некоторых вариантах воплощения изобретения второе вычислительное устройство может генерировать второй результат на основе выбранных элементов. В некоторых вариантах воплощения изобретения сгенерированный результат может включать строку данных. В некоторых вариантах воплощения изобретения сгенерированный результат может включать значение, основанное на информации о выбранных элементах эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения второе вычислительное устройство может выполнять преобразование информации выбранных элементов, такое как генерация хеша значений информации. В некоторых вариантах воплощения изобретения второе вычислительное устройство может генерировать строку данных на основе информации или внутри выбранных элементов и может выполнять преобразование (например, генерировать хеш) строки данных для генерирования второго результата.

[0062] В некоторых вариантах воплощения изобретения второе вычислительное устройство может шифровать сообщение с использованием второго результата, и второе вычислительное устройство может направлять зашифрованное сообщение первому вычислительному устройству. В некоторых вариантах воплощения изобретения сообщение может содержать очень маленький объем данных. В некоторых вариантах воплощения изобретения зашифрованное сообщение может функционировать как тестовое сообщение для отправки первому устройству передачи данных, что дает возможность первому устройству передачи данных определять, соответствует ли второй результат, сгенерированный вторым устройством передачи данных, первому

результату, сгенерированному первым устройством передачи данных.

[0063] В некоторых вариантах воплощения изобретения первое устройство передачи данных может принимать зашифрованное сообщение от второго устройства и может предпринимать попытки расшифровать сообщение, используя первый результат. Например, первое устройство передачи данных может инициировать процесс дешифровки сообщения. Первое устройство передачи данных может определять, была ли успешной его расшифровка. В некоторых вариантах воплощения изобретения в ответ на указание того, что дешифровка неуспешна, первое устройство передачи данных может определить, что второе вычислительное устройство не аутентифицировано. В некоторых вариантах воплощения изобретения в ответ на определение того, что дешифровка неуспешна, первое устройство передачи данных может отправить запрос о синхронизации диспетчеру наборов данных. В некоторых вариантах воплощения изобретения в ответ на запрос о синхронизации диспетчер наборов данных может затем сгенерировать новые инструкции извлечения и отправить эти новые инструкции извлечения первому и второму устройствам передачи данных. В некоторых вариантах воплощения в ответ на запрос о синхронизации диспетчер наборов данных, а также первое и второе устройства передачи данных могут выполнять операции синхронизации для синхронизации эфемерного совместно используемого набора данных.

[0064] В различных вариантах воплощения изобретения каждое из первого вычислительного устройства и второго вычислительного устройства может выбирать элементы из числа извлеченных элементов, и каждое из первого вычислительного устройства и второго вычислительного устройства может генерировать набор правил. В некоторых вариантах воплощения изобретения элементы, выбранные первым вычислительным устройством,

могут отличаться от элементов, выбранных вторым вычислительным устройством. Например, в некоторых вариантах воплощения изобретения первое вычислительное устройство может генерировать первый набор правил, указывающий элементы, выбранные первым вычислительным устройством. В некоторых вариантах воплощения изобретения второе вычислительное устройство может генерировать второй набор правил, указывающий элементы, выбранные вторым вычислительным устройством. В некоторых вариантах воплощения изобретения первое вычислительное устройство может отправлять первый набор правил второму вычислительному устройству, а второе вычислительное устройство может отправлять второй набор правил первому вычислительному устройству.

[0065] В некоторых вариантах воплощения изобретения первый и/или второй наборы правил могут включать в себя инструкции/правила для объединения выбранных элементов (т.е. элементов, выбранных каждым устройством, и элементов, выбранных с использованием набора правил из другого вычислительного устройства), что позволит сформировать объединенный набор выбранных элементов.

[0066] В некоторых вариантах воплощения изобретения первое вычислительное устройство может генерировать первый результат на основе элементов, выбранных первым вычислительным устройством. В некоторых вариантах воплощения изобретения первое вычислительное устройство может выбирать элементы из числа извлеченных элементов, используя второй набор правил (из второго вычислительного устройства). Первое вычислительное устройство может генерировать второй результат из элементов, выбранных с использованием второго набора правил. В некоторых вариантах воплощения изобретения первое вычислительное устройство может объединять первый результат и второй результат, чтобы

формировать объединенный результат.

[0067] В некоторых вариантах воплощения изобретения второе вычислительное устройство может генерировать третий результат на основе элементов, выбранных вторым вычислительным устройством. В некоторых вариантах воплощения изобретения первое вычислительное устройство может выбирать элементы из числа извлеченных элементов, используя первый набор правил (из первого вычислительного устройства). Второе вычислительное устройство может генерировать четвертый результат из элементов, выбранных с использованием первого набора правил. В некоторых вариантах воплощения изобретения второе вычислительное устройство может объединять третий результат и четвертый результат для формирования объединенного результата. В различных вариантах воплощения изобретения объединенные результаты, генерируемые как первым вычислительным устройством, так и вторым вычислительным устройством, являются одинаковыми.

[0068] В некоторых вариантах воплощения изобретения первый и/или второй наборы правил могут включать инструкции/правила для объединения первого и второго наборов правил в целях генерирования объединенного набора правил. Каждое вычислительное устройство может затем использовать объединенный набор правил для выбора элементов среди извлеченных элементов и может применять выбранные элементы для генерирования объединенного результата.

[0069] В некоторых вариантах воплощения изобретения второе вычислительное устройство может шифровать сообщение, используя объединенный результат, сгенерированный вторым вычислительным устройством, и второе вычислительное устройство может отправлять зашифрованное сообщение первому вычислительному устройству. В некоторых вариантах воплощения изобретения первое устройство

передачи данных может принимать зашифрованное сообщение от второго устройства и может пытаться расшифровывать сообщение, используя объединенный результат, сгенерированный первым вычислительным устройством. В ответ на определение успешности дешифрования первое вычислительное устройство может зашифровать передаваемые данные, используя объединенный результат, и может отправить зашифрованные данные второму вычислительному устройству. Второе вычислительное устройство может расшифровать данные, используя объединенный результат.

[0070] Различные варианты воплощения изобретения могут быть реализованы в различных системах передачи данных 100, пример которой проиллюстрирован на ФИГ. 1. Система передачи данных 100 может содержать вычислительные устройства 102 и 106 и сетевой элемент 110. В некоторых вариантах воплощения изобретения вычислительные устройства 102 и 106 могут содержать вычислительное устройство, используемое непосредственно пользователем, такое как смартфон, ноутбук, настольный компьютер и т.п. В некоторых вариантах воплощения изобретения вычислительные устройства 102 и 106 могут включать в себя сетевое устройство, такое как маршрутизатор, интеллектуальный коммутатор, маршрутизатор или концентратор IoT, или другое подобное устройство. Вычислительное устройство 102 может содержать или предусматривать возможность передачи данных с хранилищем данных 104, а вычислительное устройство 106 может содержать или предусматривать возможность передачи данных с хранилищем данных 108. Понятно, что пользователь может управлять более, чем одним таким вычислительным устройством, аналогично вычислительным устройствам 102 и 106. В некоторых вариантах воплощения изобретения вычислительные устройства 102 и 106 могут содержать одно или более

устройств IoT. Неограничивающие примеры устройств IoT содержат персональные или мобильные мультимедийные проигрыватели, игровые системы и контроллеры, интеллектуальные телевизоры, телевизионные приставки, интеллектуальные кухонные приборы, интеллектуальные системы подсветки и освещения, интеллектуальные счетчики электроэнергии, интеллектуальные системы отопления, вентиляции и кондиционирования воздуха (ОВКВ), интеллектуальные термостаты, системы обеспечения безопасности зданий, включая дверные и оконные замки, автомобильные развлекательные системы, системы диагностики и мониторинга транспортных средств, межмашинные устройства и аналогичные устройства, которые содержат программируемый процессор, память и схемы для установления беспроводной передачи данных пути и передача/прием данных по каналам беспроводной передачи данных. Вычислительные устройства 102 и 106 могут также включать дистанционно управляемое, автономное, полуавтономное или роботизированное транспортное средство, способное перемещаться по суше, морю, воздуху или в космосе. Вычислительные устройства 102 и 106 могут дополнительно содержать интеллектуальное огнестрельное оружие или другое оружие или систему оружия, оснащенные процессором.

[0071] В некоторых вариантах воплощения изобретения сетевой элемент 110 может содержать внутреннее вычислительное устройство, такое как сервер. Сетевой элемент 110 может содержать или предусматривать возможность передачи данных с хранилищем данных 112.

[0072] Каждое из вычислительных устройств 102 и 106 и сетевой элемент 110 могут связываться с сетью передачи данных 114 по соответствующей линии передачи данных 122, 124 и 126. В некоторых вариантах воплощения сеть передачи данных 112 может содержать две или более сетей передачи данных. Линии передачи данных 122, 124 и 126 могут

содержать проводные или беспроводные линии передачи данных и могут дополнительно содержать дополнительные устройства для облегчения передачи данных между вычислительными устройствами 102 и 106, сетевой элемент 110 и сеть передачи данных 114. Примеры таких дополнительных устройств могут включать точки доступа, базовые станции, маршрутизаторы, шлюзы, устройства проводной и/или беспроводной передачи данных, а также транзитные линии передачи данных, которые могут включать в себя оптоволоконные линии передачи данных, микроволновые линии передачи данных и другие подходящие каналы передачи данных.

[0073] В некоторых вариантах воплощения изобретения сетевой элемент 110 может быть выполнен с возможностью управления набором данных, который может храниться в хранилище данных 112. В некоторых вариантах воплощения изобретения сетевой элемент 110 может быть выполнен с возможностью управления эфемерным совместно используемым набором данных, который может храниться в хранилище данных 104 вычислительного устройства 102 и в хранилище данных 108 вычислительного устройства 106, как дополнительно описано ниже.

[0074] В различных вариантах воплощения изобретения сетевой элемент 110 может принимать входные данные 130 с течением времени. Входные данные 130 могут включать в себя информацию о том, что вычислительное устройство 130 может использоваться для генерирования, изменения и/или управления набором данных, который может использоваться совместно с другим вычислительным устройством (например, вычислительными устройствами 102 и 106). Вводимые данные 130 могут содержать, например, изображения, фотографии, видео, звукозаписи (например, музыку, записи окружающего звука или другую такую запись), вводимую биометрическую информацию (например,

результаты сканирования в процессе распознавания лица, результаты сканирования радужной оболочки, информацию об образцах ДНК, записи голосовых отпечатков, отпечатки пальцев и т. п.) или любые другие подобные вводимые данные.

.**[0075]** Сеть 112 передачи данных может содержать множество сетей передачи данных, в том числе сети передачи данных внутри объекта или предприятия, а также сети внешней передачи данных, общедоступные сети передачи данных и комбинации сетей, а также межсетевые сети, включая Интернет. Сеть передачи данных 112 может поддерживать связь с использованием одного или более протоколов проводной и беспроводной передачи данных. Каждая из линий передачи данных 120, 122, 124 и 126 может являться двусторонней проводной или беспроводной линией передачи данных. Протоколы беспроводной передачи данных могут включать в себя одну или более технологий радиодоступа (Radio Access Technologies, RAT). Примеры беспроводных сетей RAT включают сети LTE (3GPP Long Term Evolution, «долгосрочное развитие), WiMAX (Worldwide Interoperability for Microwave Access, технология широкополосного доступа в микроволновом диапазоне), CDMA (Code Division Multiple Access, множественный доступ с кодовым разделением), TDMA (Time Division Multiple Access, множественный доступ с временным разделением), широкополосный CDMA (WCDMA), GSM (Global System for Mobility, глобальная система мобильности) и другие беспроводные сети. Примеры сетей RAT также могут включать в себя Wi-Fi, Bluetooth, Zigbee, LTE в нелицензированном спектре (LTE-U), лицензионный доступ (LAA) и MuLTEfire (система, которая использует LTE в нелицензированной несущей полосе). Протоколы проводной передачи данных могут использовать различные проводные сети (например, Ethernet, телевизионный кабель, телефонию, оптоволокно и другие виды

физических сетевых подключений), которые могут использовать один или более протоколов проводной передачи данных, таких как Ethernet, протокол «точка-точка» (Point-To-Point), высокоуровневое управление каналом передачи данных (HDLC, High-Level Data Link Control), расширенный протокол управления передачей данных (ADCCP, Advanced Data Communication Control Protocol) и протокол управления передачей/Интернет-протокол (TCP/IP, Transmission Control Protocol/Internet Protocol).

[0076] В некоторых вариантах воплощения вычислительные устройства 102 и 106 и сетевой элемент 110 могут быть частью защищенной сети, такой как внутренняя сеть предприятия, защищенная сеть правительственного учреждения, виртуальная частная сеть (VPN, virtual private network) или другая аналогичная сетевая среда. В такой защищенной сети линии передачи данных 122, 124 и 126 могут обеспечивать дополнительную безопасность, такую как шифрование на одном или более уровнях, то есть уровнях взаимодействия открытых систем (OSI, Open Systems Interconnection layers) и другие реализации для защиты передачи данных по линиям передачи данных 122, 124 и 126.

[0077] Хотя линии передачи данных 122, 124 и 126 проиллюстрированы как одиночные линии, каждая из линий передачи данных может содержать множество проводных или беспроводных линий, таких как множество частот или полос частот, каждая из которых может содержать множество логических каналов. Кроме того, каждый из различных каналов передачи данных 122, 124 и 126 может использовать более одного протокола передачи данных.

[0078] На ФИГ. 2 проиллюстрирована блок-схема компонента вычислительного устройства 200, подходящая для использования с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1 и

2, в различных вариантах воплощения изобретения вычислительное устройство 200 может быть аналогичным вычислительным устройствам 102,106 и 110.

[0079] Вычислительное устройство 200 может содержать процессор 202. Процессор 202 может иметь схему исполняемых процессором инструкций для выполнения операций различных вариантов воплощения изобретения, специализированный процессор, такой как модемный процессор, имеющий схему исполняемых процессором инструкций для выполнения операций различных вариантов воплощения изобретения в дополнение к основной функции, выделенная аппаратная схема (то есть, «прошивка»), предусматривающая выполнение операций различных вариантов воплощения изобретения, или комбинация выделенного оборудования/прошивки ПО и программируемого процессора.

[0080] Процессор 202 может быть связан с памятью 204, которая может быть постоянным машиночитаемым носителем данных, сохраняющим исполняемые процессором инструкции. Память 204 может хранить операционную систему, а также пользовательское прикладное программное обеспечение и исполняемые инструкции. Память 204 также может хранить данные приложения, такие как структура данных массива. Память 204 может содержать один или более кэшей, постоянное запоминающее устройство (ПЗУ), оперативное запоминающее устройство (ОЗУ), электрически стираемое программируемое ПЗУ (ЭСППЗУ), статическое ОЗУ (SRAM), динамическое ОЗУ (DRAM) или другие типы памяти. Процессор 202 может считывать и записывать информацию в память и из памяти 204. Память 204 также может хранить инструкции, связанные с одним или более стеков протокола. Стек протокола обычно содержит исполняемые компьютером инструкции для обеспечения передачи данных с использованием протокола радиодоступа или

протокола передачи данных.

[0081] Процессор 202 может также обмениваться данными с множеством модулей для блоков, предусматривающих возможность выполнения множества операций, как дополнительно описано ниже. Например, процессор 202 может обмениваться данными с интерфейсом передачи данных 206, модулем совместно используемого набора данных 208 и модулем извлечения/выбора элементов 210, модулем набора правил 212 и модулем преобразования данных 214. Модули/блоки 206-214 могут быть реализованы на вычислительном устройстве 200, в программном обеспечении, в оборудовании или в комбинации оборудования и программного обеспечения, включая микропрограммное обеспечение, однокристальную систему (SOC, system-on-a-chip), выделенную аппаратную (т.е. микропрограммную) схему, предусматривающую выполнение операций различных вариантов воплощения изобретения, или комбинацию выделенного аппаратного обеспечения/встроенного программного обеспечения и программируемого процессора. Процессор 202, память 204 и различные модули/блоки 206-214 могут обмениваться данными по шине передачи данных или любой другой схеме передачи данных или через интерфейс.

[0082] Интерфейс передачи данных 206 может содержать сетевой интерфейс, который может поддерживать связь с сетью передачи данных (например, сетью передачи данных 114). Интерфейс передачи данных 206 может содержать один или более портов ввода/вывода (I/O), через которые осуществляется подключение, такое как подключение Ethernet, оптоволоконное подключение, подключение с помощью широкополосного кабеля, подключение с помощью телефонной линии или могут быть предоставлены другие типы проводной передачи данных. Интерфейс передачи данных 206 также может содержать радиоблок, который может

обеспечивать радиочастотную связь.

[0083] Модуль совместно используемого набора данных 208 может принимать от интерфейса передачи данных 206 информацию для использования в качестве совместно используемого набора данных (например, от сетевого элемента 110). Модуль совместно используемого набора данных 208 может предусматривать возможностью изменения совместно используемого набора данных в соответствии с инструкциями процессора 202.

[0084] Модуль извлечения/выбора элементов 210 может быть выполнен с возможностью извлечения и/или выбора одного или более элементов данных из совместно используемого набора данных.

[0085] Модуль набора правил 212 может быть выполнен с возможностью генерирования набора правил, идентифицирующего один или более элементов данных. Модуль набора правил 212 также может быть выполнен с возможностью синтаксического разбора или анализа набора правил, принятого от другого вычислительного устройства, так что модуль извлечения/извлечения элементов может использовать полученный набор правил для извлечения и/или выбора одного или более элементов данных из совместно используемого набора данных.

[0086] Модуль преобразования данных 214 может быть выполнен с возможностью выполнять одно или более преобразований данных для одного или более элементов совместно используемого набора данных, одного или более извлеченных элементов и/или одного или более выбранных элементов. Модуль преобразования данных 214 также может быть выполнен с возможностью выполнения операций по изменению совместно используемого набора данных.

[0087] На ФИГ. 3 проиллюстрирован способ управления эфемерным совместно используемым набором данных 300 в соответствии с

различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-3, способ 300 может быть реализован процессором (например, процессором 202 и/или подобным) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110).

[0088] В блоке 302 процессор может установить набор данных. Например, процессор может принимать входные данные (например, входные данные 130) и может устанавливать набор данных на основе одного или более входных данных. Входные данные и набор данных дополнительно описаны ниже.

[0089] После установления набора данных, процессор может выполнить одну или более операций для изменения набора данных.

[0090] В блоке 304 процессор может добавить новую часть набора данных и/или новый элемент данных на основе полученных входных данных.

[0091] Дополнительно или альтернативно, процессор может вычитать одну или более частей и/или один или более элементов набора данных в блоке 306.

[0092] Дополнительно или альтернативно, процессор может переупорядочивать одну или более частей и/или один или более элементов набора данных в блоке 308.

[0093] Дополнительно или альтернативно, процессор может выполнять преобразование одной или более частей и/или одного или более элементов набора данных в блоке 310.

[0094] Преобразование элемента и/или части может включать в себя выполнение одной или более операций по изменению одного или более значений элемента и/или части. Например, преобразование элемента и/или части изображения или видеофайла может включать в себя вращение, отражение, инвертирование, смещение позиции, смещение

цвета, применение фильтра или предустановленное преобразование (например, которое может быть доступно на фотографии или с помощью программы для редактирования видео), или другую аналогичную операцию. В качестве другого примера, преобразование элемента и/или части музыкального или аудиофайла может включать в себя повышение или понижение высоты тона, реверсирование содержимого файла, инвертирование содержимого аудиофайла (то есть преобразование содержимого вдоль выбранной оси), добавление звукового эффекта, такого как реверберация, искажение, окаймление и т.п. или другую подобную операцию. В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора данных может включать в себя элементы данных перекодирования (например, преобразование аудиоданных в визуальные данные или текст). В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора данных может включать в себя выполнение одной или более математических функций для преобразования элемента и/или части.

[0095] На ФИГ. 4 проиллюстрирован один пример набора данных 400 в соответствии с некоторыми вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-4, в некоторых вариантах воплощения изобретения набор данных может содержать две или более частей. Каждая часть набора данных может содержать один или более элементов. В некоторых вариантах воплощения изобретения части набора данных могут содержать дискретную составляющую, такую как изображение, фотография, видео, звукозапись, биометрический вход или другую подобную дискретную составляющую. В различных вариантах воплощения изобретения набор данных или одна или более частей и/или элементов набора данных могут использоваться для генерирования эфемерного совместно используемого

набора данных, который может храниться в двух или более вычислительных устройствах (например, в вычислительных устройствах 102 и 106).

[0096] Набор данных 400 может содержать одну или более частей, таких как части 402, 404 и 406. Каждая из частей 402, 404 и 406 может содержать один или более элементов. Например, часть 402 может содержать элементы 420 и 422, часть 404 может содержать элемент 424, а часть 406 может содержать элементы 426 и 428. В некоторых вариантах воплощения изобретения части 402, 404 и 406 могут содержать отдельные составляющие, такие как фотографии, звукозаписи, отпечатки пальцев, биометрические данные или другие дискретные части.

[0097] В некоторых вариантах воплощения изобретения набор данных 400 может формироваться со временем. Например, вычислительное устройство (например, сетевой элемент 110) может принимать входные данные (например, входные данные 130) и может со временем формировать набор данных 400 с использованием принятых входных данных. В некоторых вариантах воплощения изобретения процессор может предоставлять некоторые или все наборы данных 400 двум или более вычислительным устройствам для использования в качестве эфемерного совместно используемого набора данных.

[0098] В различных вариантах воплощения изобретения элементы 420-428 могут содержать информацию, которая позволяет идентифицировать или индексировать каждый элемент части. Например, элемент может содержать информацию, идентифицирующую местоположение, положение и/или время элемента в его части, или любую другую информацию, которая позволяет индексировать или идентифицировать каждый выбранный элемент.

[0099] В различных вариантах воплощения изобретения части 402-406

и/или элементы 420-428 могут содержать данные, на основе которых может быть определена одна или более взаимосвязей с по меньшей мере одним другим элементом данных. Например, элементы 402-406 и/или элементы 420-428 могут быть связаны с отметкой времени. В качестве другого примера, части и/или элементы могут быть связаны с различными данными, такими как местоположение, позиция, цвет, высота тона, частота, биометрический аспект или другой аспект части и/или элемента. Соотношение между двумя или более элементами может включать в себя сравнительную разницу между двумя или более элементами, такую как разница во времени, разница в местоположении, разница в положении, разница в цвете, разница в высоте тона, разница в частоте, биометрическая разница, или другие виды различий.

[0100] В качестве другого примера, элементы 420-428 могут иметь разные положения или местоположения внутри части или между разными частями. Элементы 420-428 также могут быть связаны с другими отметками времени, а также с различными положениями или местоположениями относительно двух или более иных элементов. В некоторых вариантах воплощения изобретения три или более элементов могут определять отношение одного элемента к двум или более иным элементам. Например, различия в положении/местоположении среди элементов 420, 422 и 424 могут определять три угла, угол A, угол B и угол D. Аналогично, относительные различия положения/местоположения и/или отметки времени между элементами 420, 422, 424 , 426 и 428 могут определять дополнительные углы, углы C, E, F, G, H, I и J. В различных вариантах воплощения изобретения взаимосвязь может представлять собой относительную разницу во времени, пространстве, расстоянии или другую информационную разницу в пределах части, между или среди частей, и/или в наборе данных 400.

[0101] Набор данных, такой как набор данных 400, может состоять из большого количества частей и/или элементов. На ФИГ. 5A-5D проиллюстрированы примеры наборов данных 500a, 500b, 500c и 500д. Набор данных может содержать один или более из множества типов данных, и примеры, проиллюстрированные на ФИГ. 5 и 5A-5D предназначены для иллюстрации разнообразных типов данных, но не их ограничений.

[0102] Например, набор данных 500a может содержать отпечатки пальцев 502a, 504a и 505a. Отпечатки пальцев 502a-505a могут быть восприняты, например, биометрическим сканирующим устройством, таким как сканер отпечатков пальцев. Отпечатки пальцев 502a-506a могут учитывать течение времени, так что отпечатки 502a-506a каждый составляют часть набора данных 500a. Процессор вычислительного устройства (например, вычислительные устройства 102-108) может выбирать элементы из частей (например, отпечатков 502a-506a) из набора данных 500a, например, элементы 520a-538a. В некоторых вариантах воплощения изобретения элементы 520a-538a могут содержать мелкие детали отпечатков пальцев. Элементы 520a-538a могут содержать информацию, которая позволяет процессору вычислительного устройства идентифицировать или индексировать каждый элемент в части (например, в пределах одного из отпечатков пальцев 502a-506a), такую как информация, идентифицирующая местоположение или положение элемента в пределах его части. Кроме того, каждая часть может быть связана с отметкой времени или другим элементом времени.

[0103] Элементы (например, отпечатки пальцев 502a-506a) могут включать данные, из которых может быть определена одна или более взаимосвязей с по меньшей мере одним другим элементом данных, таким как информация о позиции, местоположении и/или информация

о времени. В некоторых вариантах воплощения изобретения, части и/или элементы могут включать данные, из которых может быть определена одна или более взаимосвязей среди элементов. В некоторых вариантах воплощения изобретения, взаимосвязи могут основываться на одном или более сравнительном различии между элементами или среди них.

[0104] В качестве другого примера, набор данных 500b может содержать звукозаписи 502b, 504b и 506b. Звукозаписи могут быть восприняты, например, микрофоном или подобным устройством, или звукозаписи могут быть получены электронным способом с помощью устройства обработки данных (например, вычислительных устройств 102-108) от подобного устройства. Звукозаписи 502b-506b могут отражать изменения во времени и могут содержать или ассоциироваться с информацией о времени. Каждая из звукозаписей 502b-506b может составлять часть набора данных 500b. Дополнительно или в качестве альтернативы, одна запись (например, одна из записей 502b, 504b или 506b) может разделяться на части, например, части определенной длительности, части, разделенные на частотный диапазон, части, разделенные на амплитудные диапазоны, и другие виды разделений.

[0105] Процессор вычислительного устройства может выбирать элементы из частей звукозаписей 502b-506b, такие как элементы 520b-530b. Элементы 520b-530b могут содержать информацию, которая позволяет идентифицировать или индексировать каждый элемент в звукозаписи, такую как информация, идентифицирующая местоположение или положение элемента в его части. Каждый элемент 520b-530b может быть связан с временной меткой или другим временным элементом и/или другой информацией, такой как частота, шаг и амплитуда, скорость атаки, скорость затухания,

длительность сустейна.

[0106] Части (например, одна или более звукозаписей 502b) и/или элементы 520b-530b могут содержать данные, из которых может быть определена одна или более взаимосвязей с по меньшей мере одним другим элементом данных, таким как информация о позиции, местоположении и/или информация о времени. В некоторых вариантах воплощения части и/или элементы могут содержать данные, среди которых процессор вычислительного устройства может определять одну или более взаимосвязей между элементами. В некоторых вариантах воплощения изобретения взаимосвязи могут быть основаны на одном или более сравнительном различии между элементами или среди них.

[0107] В качестве другого примера, набор данных 500c может содержать изображения 502c, 504c и 506c. Изображения 502c-506c могут иметь, например, вид, проиллюстрированный на ФИГ. 5C, но в различных вариантах воплощения изображения 502a-506c могут быть любыми изображениями. Изображения 502a-506c могут быть сняты, например, камерой или другим устройством восприятия изображения. Изображения 502a-506c могут быть восприняты с изменением во времени, так что каждое из изображений 502a-506c составляет часть набора данных 500a. Процессор вычислительного устройства (например, вычислительные устройства 102-108) может выбирать элементы из частей (например, изображений 502a-506c) набора 500c данных, таких как элементы 520c-536c. Например, процессор вычислительного устройства может выбирать элементы 520c-536c с использованием системы распознавания лиц или другой аналогичной системы распознавания. Элементы 520c-536c могут содержать информацию, которая позволяет процессору вычислительного устройства идентифицировать или индексировать каждый элемент в пределах части (например, в одном из изображений 502a-506c), такую как

информация, идентифицирующая местоположение или положение элемента в пределах его части. Кроме того, каждая часть может быть связана с отметкой времени или другим элементом времени.

[0108] Части (например, изображения 502a-506c) и/или элементы 520c-536c могут содержать данные, на основе которых может быть определена одна или более взаимосвязей с по меньшей мере одним другим элементом данных, таким как информация о позиции, местоположении и/или времени. В некоторых вариантах воплощения изобретения элементы 520c-536c могут быть связаны с информацией изображения, такой как цвет, оттенок, оттенок, оттенки серого, информация RGB, номер цвета Pantone, цифровой цветовой код (например, цветовой код языка разметки гипертекста), насыщенность, яркость, контраст или другая информация об изображении. В некоторых вариантах воплощения изобретения части и/или элементы могут содержать данные, на основе которых может быть установлена одна или более взаимосвязей между элементами. В некоторых вариантах воплощения изобретения отношения могут быть основаны на одном или большем числе сравнительных различий между элементами или среди них. В некоторых вариантах воплощения изобретения сравнительные различия могут включать различия в информации об изображении, включая относительные, линейные и/или численные различия в информации, указывающей цвет, оттенок, оттенок и т.п.

[0109] В качестве другого примера, набор данных 500d может содержать один или более блоков биометрических данных или составляющих, таких как образцы ДНК 502d, 504d и 506d. Биометрические данные могут быть восприняты соответствующим сканером или устройством захвата и приняты процессором вычислительного устройства (например, вычислительными устройствами 102-108). Биометрические данные могут

быть получены с течением времени и могут содержать или быть связанными с информацией о времени. Набор данных 500d может содержать две или более составляющих или единиц биометрических данных, каждая из которых может составлять часть набора данных (например, две или более дискретных биометрических выборок). Дополнительно или альтернативно, биометрический образец может быть разделен на части, причем подобные разделения могут быть определены на основе информации, доступной в биометрическом образце. Например, образцы ДНК 502d, 504d и 506d можно разделить на части определенной длины или по числу пар оснований, по определенной длине основной цепи ДНК, по типу нуклеотида (например, аденин, гуанин, цитозин или тиамин), по типу пары оснований (например, аденин-тиамин, цитозин-гуанин) или воспользоваться другими видами разделений.

[0110] Процессор вычислительного устройства может выбирать элементы из частей блока биометрических данных 500d, такие как элементы 520d-530d. Элементы 520d-530d могут содержать информацию, которая позволяет идентифицировать или индексировать каждый элемент в биометрических данных, такую как информация, идентифицирующая местоположение или положение элемента в его части, например положение вдоль цепи ДНК 502d. Каждый элемент 520d-530d может быть связан с меткой времени или другим элементом времени.

[0111] Части (например, один или более блоков биометрических данных 502d и/или элементы 520d-530d могут содержать данные, на основе которых может быть определена одна или более взаимосвязей с по меньшей мере одним другим элементом данных, таким как информация о позиции, местоположении и/или информация о времени. В некоторых вариантах воплощения изобретения части и/или элементы могут содержать данные, на основе которых процессор вычислительного

устройства может определять одну или более взаимосвязей между элементами. В некоторых вариантах воплощения изобретения взаимосвязи могут быть основаны на одном или более сравнительном различии между элементами или среди них.

[0112] На ФИГ. 6A-6C проиллюстрированы представления способов управления набором данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-6C, набор данных 600 может содержать две или более частей 602, 604, 606 и 608. Части 602-608 могут содержать элементы данных (например, элементы 420-428, 520a-538a, 520b-530b, 520c -536c и 520d-530d). Кроме того, части 602, 604, 606 и 608 могут быть связаны с разными промежутками времени (например, получены в разное время или связаны с другой информацией об отметке времени).

[0113] Процессор (например, процессор 202 и/или тому подобный) вычислительного устройства (например, вычислительные устройства 102 и 106 и сетевой элемент 110) может выполнить преобразование в наборе данных 600, чтобы изменить одно или более значений элементов данных в наборе данных. В качестве одного примера, части 602, 604, 606 и 608 могут быть файлами изображений. Процессор может вращать набор данных 600 или любую из частей 602-608 вдоль одной или более осей 620, 624 и 626. Процессор также может вращать набор данных 600 вдоль края 628. Процессор также может вращать набор данных 600 вдоль оси 630 с наклоном, от «угла» набора данных до «центра» набора данных. Любое из вращений может изменять одно или более значений элементов частей 602-608. Вращение (я) также могут изменять одно или более соотношений между значениями элементов частей 602-608. Выполняя преобразование в наборе данных 600, процессор может генерировать большое количество изменений значений элементов данных каждой из

частей 602-608. Измененные значения могут обеспечить большое количество крайне непредсказуемых значений даже из относительно небольшого набора данных.

[0114] В некоторых вариантах воплощения изобретения процессор может добавить новую часть или изменить часть, присутствующую в наборе данных 600. В некоторых вариантах воплощения изобретения процессор может добавить или изменить часть таким образом, что отношения между элементами добавленной/модифицированной части и другие части набора данных остались нерегулярными и, следовательно, их трудно предсказать. Например, в некоторых вариантах воплощения изобретения процессор может добавлять или изменять часть таким образом, что добавленная/измененная часть имеет другую относительную ориентацию или другую связь с другими частями набора данных. Например, процессор может добавить часть 610 к набору данных 600 в ориентации, которая, например, перпендикулярна частям 602-608. В качестве другого примера процессор может добавить часть 612 к набору данных 600 с ориентацией, которая находится под острым углом к частям 602-608. Нерегулярные, непредсказуемые отношения между элементами данных частей 602-612 могут обеспечить большое количество крайне непредсказуемых значений даже на основе относительно небольшого набора данных.

[0115] Как отмечено выше, преобразование элемента и/или части может включать в себя выполнение одной или более операций для изменения одного или более значений элемента и/или части. Например, преобразование элемента и/или части изображения либо видеофайла может включать в себя поворот, переворачивание, инвертирование, смещение позиции, смещение цвета, применение фильтра или преобразование заранее выполненных настроек (например, доступных в программе

редактирования фотографий или видео) или другую подобную операцию. В качестве другого примера, преобразование элемента и/или части музыкального или аудиофайла может включать в себя повышение или понижение высоты тона, реверсирование содержимого файла, инвертирование содержимого аудиофайла (то есть преобразование содержимого вдоль выбранной оси) добавление подобного звукового эффекта в качестве реверберации, искажения, окаймления и тому подобного эффекта или при другой подобной операции. В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора данных может включать в себя элементы данных перекодирования (например, преобразование аудиоданных в визуальные данные или текст). В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора данных может включать в себя выполнение одной или более математических функций для преобразования элемента и/или части. В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора данных может включать в себя изменение размера или формы, искажение доли, выполнение перекоса, растяжения или другого изменения размеров элемента и/или части набора данных. Как отмечено выше, преобразование элемента и/или части набора данных может изменять не только значение элемента и/или части, они также могут изменять одно или более отношений преобразованного элемента и/или части на другие элементы и/или части набора данных.

[0116] В качестве другого примера преобразование элемента и/или части набора данных (например, набора данных 600) может включать в себя

выполнение одной или более операций перекодирования элементов данных из одного формата или типа данных в другой формат или тип данных. На ФИГ. 6D проиллюстрированы два представления 650 и 660 преобразования первого формата или типа данных во второй формат или тип данных. Представления 650 и 660 иллюстрируют преобразования аудиоданных в визуальные данные, в частности спектрограммы данных, представленных космическим аппаратом НАСА Кассини, когда он пересекает плоскость колец Сатурна. Спектрограммы 650 и 660 иллюстрируют преобразование аудиоданных в визуальные данные. Это всего лишь один пример, и в различных вариантах воплощения изобретения любой формат или тип данных может быть преобразован в другой формат или тип данных.

[0117] В различных вариантах воплощения изобретения выполнение одного или более преобразований для набора данных 600 позволяет процессору генерировать очень большое количество непредсказуемых значений элементов и отношений между элементами данных из относительно небольшого числа частей. Например, в случае, когда части 602-612 представляют файлы изображений, каждый файл изображения может содержать большое количество пикселей, и каждый пиксель может быть связан с рядом различных значений, таких как информация о местоположении в файле изображения, цвет, оттенок, насыщенность, черно-белое значение и другая подобная информация о пикселях. Даже без преобразования каждый файл изображения из серии файлов изображений может содержать уникальный набор информации. Например, каждое изображение в серии изображений, полученных с камеры, направленной на дорогу, будет включать в себя уникальный выбор транспортных средств, находящихся в разных местах на дороге, с различными условиями окружающей среды (например, облачные

образования, солнечный свет, темнота, солнечные блики, тени и т.д.). Затем процессор может выполнять преобразование одного или более файлов изображений, тем самым изменяя не только значения различных пикселей в файлах преобразованного изображения, но также многочисленные взаимные передачи данных между элементами данных файлов преобразованного изображения и другими частями набора данных.

[0118] На ФИГ. 7 проиллюстрирован способ 700 управления синхронизацией эфемерного совместно используемого набора данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-7, способ 700 может быть реализован процессором (например, процессором 202 и/или т.п.) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110). В различных вариантах воплощения изобретения динамический (например, эфемерный) совместно используемый набор данных может существовать в одном состоянии в течение относительно короткого периода времени, который может составлять, например, минуты или секунды. Относительно короткая продолжительность и сложность, присущая любому состоянию динамического совместно используемого набора данных, на порядок уменьшает вероятность того, что подобная информация будет угадана, к ней получен доступ, или она будет «взломана», а затем использована в качестве средства для атаки на систему.

[0119] В блоке 702 процессор первого вычислительного устройства (CD1) (например, вычислительное устройство 102, 106) может получить эфемерный совместно используемый набор данных.

[0120] В блоке 704 процессор второго вычислительного устройства (CD2) (например, вычислительное устройство 102, 106) может получить эфемерный совместно используемый набор

данных.

[0121] В блоке 706 процессор диспетчера наборов данных (например, устройство управления набором данных, например, сетевой элемент 110) может предоставить эфемерные совместно используемые данные, установленные в устройствах CD1 и CD2. В некоторых вариантах воплощения изобретения эфемерный совместно используемый набор данных может содержать некоторые или все наборы данных, находящиеся на сохранении и управляемые менеджером набора данных (например, набор данных 400, 500a, 500b, 50c, 500d и 600).

[0122] В блоке 708 процессор устройства CD1 может хранить эфемерный совместно используемый набор данных (например, в хранилище 104). В блоке 710 процессор устройства CD2 может хранить эфемерный совместно используемый набор данных (например, в хранилище 108).

[0123] В добавочном блоке 712 процессор диспетчера наборов данных может выполнять одну или более операций для синхронизации эфемерного совместно используемого набора данных. В добавочном блоке 714, процессор устройства CD1 может выполнять одну или более операций синхронизации эфемерного совместно используемого набора данных. В добавочном блоке 716 процессор устройства CD2 может выполнять одну или более операций синхронизации эфемерного совместно используемого набора данных. В различных вариантах воплощения изобретения операции синхронизации блоков 712, 714 и 716 могут быть инициированы менеджером набора данных, CD1 или CD2. Операции синхронизации блоков 712, 714 и 716 могут включать в себя передачу и/или обмен одного или более сообщений, указывающих статус и/или состояние эфемерного совместно используемого набора данных, хранящихся в каждом из менеджеров наборов данных, устройства CD1 и CD2. Операции синхронизации блоков 712, 714 и 716 могут включать в

себя выполнение процессором диспетчера наборов данных, устройства CD1 и CD2 одного или более анализов их соответствующих сохраненных эфемерных совместно используемых наборов данных, таких как определение контрольной суммы, выполнение хеширования и т.п.

[0124] В блоке определения 718 процессор диспетчера наборов данных может определить, произошел ли запуск обновления набора данных. Например, процессор может определить, истек ли период времени. В качестве другого примера процессор может определить, произошло ли событие запуска. Инициирующее событие может включать, например, использование эфемерного совместно используемого набора данных в процессе аутентификации, такого как извлечение элемента(ов) из эфемерного совместно используемого набора данных, определение значения из элемента(ов) и т. д., как дополнительно описано ниже. В некоторых вариантах воплощения изобретения событие триггера может включать в себя, например, использование эфемерного совместно используемого набора данных в процессе шифрования, как дополнительно описано ниже. Событие триггера может включать в себя, например, запрос от одного или более вычислительных устройств на обновление эфемерного совместно используемого набора данных.

[0125] В ответ на определение отсутствия запуска триггера обновления (т.е. блок определения 718 = «No» (Нет)), процессор диспетчера наборов данных может снова выполнить операции синхронизации эфемерного совместно используемого набора данных в добавочном блоке 712. Процессоры CD1 и CD2 также могут выполнять операции синхронизации эфемерного совместно используемого набора данных в добавочных блоках 714 и 716, соответственно.

[0126] В ответ на определение запуска триггеров обновления набора

данных (то есть блок определения 718 = «Yes» (Да)), процессор может выполнить одну или более операций для динамического изменения эфемерного совместно используемого набора данных.

[0127] Например, процессор диспетчера наборов данных может генерировать инструкцию для замены эфемерного совместно используемого набора данных в блоке 720. В некоторых вариантах воплощения изобретения процессор диспетчера наборов данных может определять замещающий (новый) набор данных. В некоторых вариантах воплощения изобретения набор данных для замены может содержать одну или более частей набора данных, управляемых администратором набора данных.

[0128] Дополнительно или альтернативно, процессор диспетчера наборов данных может генерировать инструкцию для добавления новой части набора данных в блоке 722. В некоторых вариантах воплощения изобретения новая часть набора данных может быть основана на принятых входных данных (например, входных данных 130). В некоторых вариантах воплощения изобретения процессор диспетчера наборов данных может генерировать новую часть набора данных, которая должна быть добавлена. В некоторых вариантах воплощения изобретения сгенерированные инструкции могут включать в себя инструкции, позволяющие генерировать новую часть набора данных (которая может быть, например, отослана устройствам CD1 и CD2, как описано ниже).

[0129] Дополнительно или в качестве альтернативы, процессор диспетчера наборов данных может генерировать инструкцию для вычитания части эфемерного совместно используемого набора данных в блоке 724.

[0130] Дополнительно или в качестве альтернативы, процессор может генерировать инструкцию для переупорядочения эфемерного совместно

используемого набора данных в блоке 726. Например, процесс переупорядочения эфемерного совместно используемого набора данных может включать в себя размещение одной или более частей эфемерного совместно используемого набора данных в другое время, позиции, положении или другом отличии относительно других частей эфемерного совместно используемого набора данных.

[0131] Дополнительно или альтернативно, процессор может генерировать инструкцию для преобразования эфемерного совместно используемого набора данных в блоке 728. Например, процессор может генерировать инструкцию для преобразования одного или более элементов и/или одной или более частей эфемерного совместно используемого набора данных. В различных вариантах воплощения изобретения преобразование части и/или элемента части эфемерного совместно используемого набора данных может включать в себя выполнение одной или более операций по изменению одного или более значений элемента и/или части. Например, преобразование элемента и/или части изображения или видеофайла может включать в себя вращение, отражение, инвертирование, смещение позиции, смещение цвета, применение фильтра или предустановленное преобразование (например, которое может быть доступно на фотографии, или программу для редактирования видео), или другую аналогичную операцию. В качестве другого примера, преобразование элемента и/или части музыкального или аудиофайла может включать в себя повышение или понижение высоты тона, реверсирование содержимого файла, инвертирование содержимого аудиофайла (то есть преобразование содержимого вдоль выбранной оси) добавление звукового эффекта, такого как реверберация, искажение, окаймление и тому подобного, или другую аналогичную операцию. В качестве другого примера, преобразование элемента и/или части эфемерного совместно используемого набора

данных может включать в себя элементы данных перекодирования (например, преобразование аудиоданных в визуальные данные или текст). В качестве другого примера, преобразование элемента и /или части эфемерного совместно используемого набора данных может включать в себя выполнение одной или более математических функций для преобразования элемента и/или части.

[0132] В блоке 730 процессор может генерировать одну или более инструкций для изменения эфемерного совместно используемого набора данных. Одна или более инструкций могут быть основаны на инструкции для замены эфемерного совместно используемого набора данных, инструкции на добавление новой части набора данных (и/или сгенерированной новой части набора данных), инструкции на вычитание части эфемерного совместно используемого набора данных, инструкции для переупорядочения эфемерного совместно используемого набора данных и/или инструкции по преобразованию эфемерного совместно используемого набора данных.

[0133] В блоке 732 процессор второго вычислительного устройства может передавать одну или более инструкций для изменения эфемерного совместно используемого набора данных, установленных на устройствах CD1 и CD2.

[0134] В блоке 734 процессор устройства CD1 может принять одну или более инструкций для изменения эфемерного совместно используемого набора данных.

[0135] В блоке 736 процессор устройства CD1 может изменить свою сохраненную копию эфемерного совместно используемого набора данных на основании принятых одной или более инструкций.

[0136] В блоке 738 процессор устройства CD2 может принять одну или более инструкций для изменения эфемерного совместно используемого

набора данных.

[0137] В блоке 740 процессор устройства CD2 может изменять свою сохраненную копию эфемерного совместно используемого набора данных на основании принятых одной или более инструкций.

[0138] Процессоры диспетчера наборов данных, устройства CD1 и CD2 могут затем выполнять операции для синхронизации эфемерного совместно используемого набора данных в добавочных блоках 712, 714 и 716, соответственно.

[0139] В некоторых вариантах воплощения изобретения вычислительное устройство (например, устройства CD1, CD2) может определять, что его эфемерный совместно используемый набор данных не синхронизирован, и вычислительное устройство может выполнять операции для синхронизации эфемерного совместно используемого набора данных, хранящегося в вычислительном устройстве. Например, вычислительное устройство может потерять сетевое соединение на некоторый период времени, может быть выключено или иным образом находиться вовне или за пределами сетевого взаимодействия. В некоторых вариантах воплощения изобретения диспетчер наборов данных может хранить одну или большее число предыдущих инструкций для изменения эфемерного совместно используемого набора данных. В некоторых вариантах воплощения изобретения операции синхронизации, выполняемые вычислительным устройством, могут включать в себя определение того, что вычислительное устройство не выполнило одну или более инструкций для изменения эфемерного совместно используемого набора данных. Например, вычислительное устройство может обмениваться одним или более сообщениями синхронизации с администратором набора данных, когда вычислительное устройство восстанавливает линию передачи данных с сетью передачи данных, и на основе информации в одном или

более из сообщений синхронизации вычислительное устройство может определить, что сохраненная им версия эфемерного совместно используемого набора данных не синхронизирована. В некоторых вариантах воплощения изобретения вычислительное устройство может запросить, чтобы администратор набора данных направил вычислительному устройству неисполненные инструкции для изменения эфемерного совместно используемого набора данных. Затем вычислительное устройство может выполнять принятые и еще не выполненные инструкции, чтобы изменить свою версию эфемерного совместно используемого набора данных, что позволит привести эфемерный совместно используемый набор данных, хранящийся в вычислительном устройстве, в состояние синхронизации.

[0140] ФИГ.8А иллюстрирует способ 800А для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-8А, способ 800А может быть осуществлен процессором (например, процессором 202 и/или ему подобным) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110).

[0141] В блоке 802 процессор первого вычислительного устройства (CD1) (например, вычислительное устройство 102) может выполнять операции по аутентификации второго вычислительного устройства (CD2) (например, вычислительного устройства 106) и диспетчера наборов данных (например, устройства управления набором данных, например, сетевой элемент 110). В блоке 804 процессор устройства CD2 может выполнять операции по аутентификации устройства CD1 и диспетчера наборов данных. В блоке 806 диспетчер наборов данных может выполнять операции по аутентификации устройств CD1 и CD2. Примеры применимых операций описаны в заявке на патент США № 15/493572, озаглавленной

«Системы и способы проверки и аутентификации устройства», поданной 21 апреля 2017 года.

[0142] В блоке 808 процессор устройства CD1 может направлять указание администратору набора данных, что устройство CD1 имеет линию передачи данных для передачи данных устройству CD2.

[0143] В блоке 810 процессор диспетчера наборов данных может принимать указание от устройства CD1.

[0144] В блоке 812 процессор диспетчера наборов данных может выбирать элементы из совместно используемого набора данных. Совместно используемый набор данных может храниться в диспетчере наборов данных и на устройствах CD1 и CD2, так что каждое из устройств CD1 и CD2 имеет копию совместно используемого набора данных. В некоторых вариантах воплощения процессор диспетчера наборов данных может выбирать два или более элементов из одной или более частей совместно используемого набора данных. Например, процессор первого вычислительного устройства может выбирать два или более элементов из совместно используемых наборов данных 400 и 500a-500d и 600 (например, элементы 420-428, 520a-538a, 520b-530b, 520c-536c и 520d-530d).

[0145] В блоке 814 процессор диспетчера наборов данных может генерировать инструкции извлечения. Инструкции извлечения могут предоставлять инструкции другому вычислительному устройству (например, CD1, CD2) для извлечения элементов данных из совместно используемого набора данных. В некоторых вариантах воплощения изобретения инструкции извлечения могут включать в себя набор правил, который позволяет процессору принимающего вычислительного устройства (например, CD1, CD2) идентифицировать элемент(ы), выбранные процессором диспетчера наборов данных, из сохраненного

совместно используемого набора данных на приемном вычислительном устройстве. В некоторых вариантах воплощения изобретения инструкции извлечения могут включать в себя инструкцию для выполнения операции преобразования над одним или более извлеченными элементами. В некоторых вариантах воплощения изобретения инструкции извлечения могут включать в себя инструкцию для выполнения операции преобразования над одной или более частей совместно используемого набора данных или всего набора общих данных до или после извлечения элемента данных из совместно используемого набора данных. В качестве одного примера, командные инструкции могут включать в себя первую инструкцию для выбора первого элемента, вторую инструкцию для выполнения указанного преобразования первого элемента, третью инструкцию для выполнения преобразования совместно используемого набора данных, четвертую инструкцию для выбора второго элемента, пятую инструкцию для выполнения преобразования второго элемента и т.д.

[0146] В некоторых вариантах воплощения изобретения инструкции извлечения могут включать в себя набор правил, который позволяет процессору принимающего вычислительного устройства (например, CD1, CD2) извлекать элементы на основе взаимосвязей между элементами. Например, процессор диспетчера наборов данных может определить одно или более отношений между выбранными двумя или более элементами. В некоторых вариантах воплощения изобретения отношения могут основываться на одном или более сравнительных или реляционных различиях между элементами или среди них, таких как те, которые описаны выше в отношении наборов данных 400 и 500a-500d.

[0147] В различных вариантах воплощения инструкции извлечения могут позволить устройствам CD1 и CD2 динамически генерировать уникальный

набор элементов (извлеченные элементы данных), которые уникальным образом совместно используются устройствами CD1 и CD2, на основе элементов в совместно используемом наборе данных.

[0148] В блоке 816 процессор диспетчера наборов данных может направлять инструкции извлечения устройствам CD1 и CD2.

[0149] В блоке 818 процессор устройства CD1 может принимать инструкции извлечения от диспетчера наборов данных. В блоке 820 процессор устройства CD2 может принимать инструкции извлечения от диспетчера наборов данных.

[0150] В блоке 822 процессор устройства CD1 может извлекать элементы из эфемерного совместно используемого набора данных, сохраненного на устройстве CD1, в соответствии с инструкциями. В блоке 824 процессор устройства CD2 может извлекать элементы из эфемерного совместно используемого набора данных, сохраненного на устройстве CD2, в соответствии с инструкциями.

[0151] В некоторых вариантах воплощения изобретения операции блоков 822 и 824 могут включать в себя выполнение преобразования извлеченных элементов. Например, процессор устройства CD1 и/или CD2 может преобразовывать элемент изображения или видеофайл (например, такие преобразования включают в себя вращение, переворачивание, инвертирование, смещение позиции, смещение цвета, применение фильтра или предварительно заданное преобразование или другие подобные операции). В качестве другого примера, процессор устройства CD1 и/или CD2 может преобразовать элемент музыкального или аудиофайла (например, повысить или понизить высоту тона, обратить содержимое файла, преобразовать содержимое вдоль выбранной оси,

добавить звуковой эффект, например, как реверберация, искажение, окаймление и тому подобное, или другая подобная операция). В качестве другого примера, процессор устройства CD1 и/или CD2 может перекодировать элементы данных из одного формата или типа данных в другой формат или тип данных. В качестве другого примера, процессор устройства CD1 и/или CD2 может выполнять одну или более математических функций для преобразования элемента.

[0152] В блоке 826 процессор устройства CD1 может выбрать один или более элементов из извлеченных элементов.

[0153] В блоке 828 процессор устройства CD1 может генерировать набор правил, указывающий выбранные элементы. Например, процессор устройства CD1 может выбирать один или более элементов из одной или более частей совместно используемого набора данных и может генерировать набор правил, идентифицирующий выбранные два или более элементов. В некоторых вариантах воплощения изобретения процессор устройства CD1 может определять одно или более отношений между выбранными двумя или более элементами и может генерировать набор правил на основе определенного одного или более отношений между выбранными двумя или более элементами. В некоторых вариантах воплощения изобретения отношения могут основываться на одном или более сравнительных или реляционных различиях между элементами или среди них, таких как те, которые описаны выше в отношении совместно используемых наборов данных 400 и 500a-500d. В некоторых вариантах воплощения изобретения набор правил может указывать систему исчисления, которая должна использоваться при идентификации и выборе элементов из совместно используемого набора данных, таких как десятичные, восьмеричные, шестнадцатеричные и т.д. В некоторых вариантах воплощения изобретения набор правил может указать протокол

шифрования, который будет использоваться устройствами CD1 и CD2. В различных вариантах воплощения изобретения набор правил может указывать два или более протоколов шифрования, которые должны использоваться, так что протокол шифрования, используемый устройствами CD1 и CD2, изменяется со временем.

[0154] В блоке 830 процессор устройства CD1 может направить набор правил устройству CD2.

[0155] В блоке 832 процессор устройства CD1 может генерировать первый результат на основе выбранных элементов.

[0156] В блоке 834 процессор устройства CD2 может принимать набор правил от устройства CD1.

[0157] В блоке 836 процессор устройства CD2 может выбирать элементы из своих извлеченных элементов, используя набор правил. Например, процессор устройства CD2 может использовать идентификаторы каждого из выбранных элементов (например, один или более элементов 420-428 или один или более элементов совместно используемых наборов данных 500a-500d) для выбора элементов среди извлеченных элементов из эфемерного совместно используемого набора данных, хранящегося на устройстве CD2. В качестве другого примера, процессор устройства CD2 может использовать один или более идентификаторов одного из элементов и одну или более взаимосвязей среди выбранных элементов для выбора элементов из извлеченных элементов.

[0158] В блоке 838 процессор устройства CD2 может генерировать второй результат на основе выбранных элементов. В некоторых вариантах воплощения изобретения второй результат может включать в себя строку данных. В некоторых вариантах воплощения изобретения второй результат может включать в себя значение, основанное на информации о

выбранных элементах совместно используемого набора данных. В некоторых вариантах процессор устройства CD2 может выполнять преобразование информации для выбранных элементов, такое как создание хеша значений в информации. В некоторых вариантах процессор устройства CD2 может генерировать строку данных на основе информации о выбранных элементах и может выполнять преобразование (например, генерировать хеш) информации о выбранных элементах для генерирования первого результата. В различных вариантах воплощения изобретения процессор устройства CD2 может использовать один и тот же способ генерирования второго результата, который устройство CD1 использует для генерирования первого результата.

[0159] В блоке 840 процессор устройства CD2 может зашифровать сообщение, используя второй результат. Например, процессор устройства CD2 может использовать метод шифрования, такой как MD5, SHA2, SHA256, BLAKE2 и тому подобное, вместе со вторым результатом для шифрования сообщения. В некоторых вариантах воплощения изобретения сообщение может служить в качестве тестового сообщения, чтобы дать возможность процессору устройства CD1 определить, соответствует ли второй результат, сгенерированный процессором устройства CD2, первому результату, сгенерированному процессором устройства CD1.

[0160] В блоке 842 процессор устройства CD2 может направлять зашифрованное сообщение устройству CD1.

[0161] В блоке 844 процессор устройства CD1 может принять зашифрованное сообщение.

[0162] В блоке 846 процессор устройства CD1 может попытаться расшифровать сообщение, используя первый результат. Например, процессор устройства CD1 может инициировать процесс дешифрования сообщения. В различных вариантах воплощения изобретения процессор

устройства CD1 может использовать формат дешифрования, такой как MD5, SHA2, SHA256, BLAKE2 и т.п. для попытки дешифрования сообщения.

[0163] В блоке 848 определения процессор устройства CD1 может определить, была ли расшифровка сообщения, направленного с устройства CD2, успешной. В некоторых вариантах воплощения изобретения успешное дешифрование зашифрованного сообщения, направленного с устройства CD2, может указывать, что первый и второй результаты совпадают.

[0164] В ответ на идентификацию сбоя дешифрования (то есть блок определения 848 = «No» (Нет)), в некоторых вариантах воплощения изобретения процессор устройства CD1 может определить, что CD2 не аутентифицирован в добавочном блоке 850.

[0165] В ответ на идентификацию сбоя дешифрования (то есть блок определения 848 = «No» (Нет)), в некоторых вариантах воплощения изобретения процессор устройства CD1 может отправлять запрос синхронизации диспетчеру набора данных в добавочном блоке 852.

[0166] В некоторых вариантах воплощения изобретения после отправки запроса синхронизации процессор диспетчера наборов данных может снова выбирать элементы из эфемерного совместно используемого набора данных в блоке 812.

[0167] В некоторых вариантах воплощения изобретения после отправки запроса на синхронизацию процессоры диспетчера наборов данных, устройств CD1 и CD2, могут выполнять операции по синхронизации совместно используемого набора данных в добавочных блоках 712, 714 и 716, соответственно.

[0168] В ответ на идентификацию определения успешности расшифровки (то есть блок определения 848 = «Yes» (Да)), процессор устройства CD1

может зашифровать передаваемые данные, используя первый результат в блоке 854. Например, процессор устройства CD1 может зашифровать сообщение, для которого процессор устройства CD1 отправил указание администратору набора данных в блоке 808.

[0169] В блоке 856 процессор устройства CD1 может отправлять зашифрованное сообщение устройству CD2. В некоторых вариантах воплощения изобретения процессор устройства CD1 может затем отправлять другое указание администратору набора данных, поскольку устройство CD1 связано каналом передачи данных с устройством CD2.

[0170] В блоке 858 процессор устройства CD2 может принимать зашифрованные сообщения от устройства CD1.

[0171] В блоке 860 процессор устройства CD2 может расшифровывать передаваемые данные, используя второй результат. В некоторых вариантах воплощения изобретения процессор устройства CD2 может снова принимать инструкции извлечения от диспетчера наборов данных.

[0172] В различных вариантах воплощения процессор устройства CD1 может отправлять администратору набора данных другое указание передачи данных, предназначенной для устройства CD2, в блоке 808. В различных вариантах воплощения изобретения процессор устройства CD2 может принимать инструкции извлечения от диспетчера наборов данных в блоке 820.

[0173] Способ 800A не ограничивается отправкой сообщения из устройства CD1 устройству CD2, и в различных вариантах воплощения изобретения процессор устройства CD2 может выполнять операции, описанные выше в отношении процессора устройства CD1, и наоборот. В некоторых вариантах воплощения изобретения процессоры устройств CD1 и CD2 могут выполнять свои соответствующие операции для способа 800A, так что устройство CD1 может отправлять зашифрованное

сообщение устройству CD2, и впоследствии роли могут переключаться, чтобы устройство CD2 могло отправлять зашифрованное сообщение устройству CD1.

[0174] В различных вариантах воплощения изобретения эфемерный совместно используемый набор данных может существовать в одном состоянии в течение относительно короткого периода времени, который может составлять, например, минуты или секунды.

[0175] В различных вариантах воплощения изобретения динамическое значение может использоваться для шифрования и дешифрования только одного сообщения. Это отличается от действительной продолжительности сертификатов, выданных обычным сертифицирующим органом (такого как сертификаты PKI), который в некоторых случаях может иметь действовать в течение десятилетий. Относительно короткая полезная продолжительность и внутренняя сложность эфемерного совместно используемого набора данных и динамического значения на порядки уменьшают вероятность того, что подобная информация будет угадана, получен к ней доступ, или она будет «взломана», а затем использована в качестве средства для атаки системы.

[0176] На ФИГ. 8B проиллюстрирован способ 800B для защиты передачи данных в соответствии с различными вариантами воплощения. Со ссылкой на ФИГ. 1-8B, способ 800B может быть реализован процессором (например, процессором 202 и/или подобным) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110). В блоках 822-860 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции с одинаковым образом пронумерованными блоками с применением способа 800A.

[0177] В блоке 870 процессор диспетчера наборов данных может выполнять операции подтверждения установления передачи данных с устройства CD1 и/или устройства CD2. В блоках 872 и 874 процессор устройства CD1 и процессор устройства CD2 могут выполнять соответствующие операции установления передачи данных с диспетчером набора данных. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для установления линии передачи данных между администратором набора данных и устройством CD1 и/или между диспетчером набора данных и устройством CD2. В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций предоставления/получения эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций синхронизации для синхронизации эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для аутентификации диспетчера наборов данных, устройства CD1 и/или устройства CD2. Примеры применимых операций описаны в заявке на патент США № 15/493572, озаглавленной «Системы и

способы проверки и аутентификации устройства», поданной 21 апреля, 2017.

[0178] В некоторых вариантах воплощения изобретения после отправки запроса синхронизации (блок 852) процессор диспетчера наборов данных может снова выполнить операции подтверждения установления передачи данных в блоке 870.

[0179] В некоторых вариантах воплощения, следуя операциям блока 856, процессор устройства CD1 снова выполняют операции подтверждения установления передачи данных в блоке 872.

[0180] В некоторых вариантах воплощения изобретения, следуя операциям блока 860, процессор устройства CD2 может снова выполнять операции подтверждения установления передачи данных в блоке 874.

[0181] ФИГ. 9A иллюстрирует способ 900A для защиты передачи данных в соответствии с различными вариантами воплощения. Со ссылкой на ФИГ. 1-9, способ 900A может быть реализован процессором (например, процессором 202 и/или т.п.) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110). В блоках 818-858 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции блоков с одинаковыми номерами способа 800A.

[0182] В блоке 902 процессор устройства CD2 может выбрать один или более элементов из извлеченных элементов.

[0183] В блоке 904 процессор устройства CD2 может генерировать второй набор правил, указывающий выбранные элементы. Например, процессор устройства CD2 может выбирать один или более элементов из одной или более частей совместно используемого набора данных и может генерировать второй набор правил, идентифицирующий выбранные два

или более элементов. В некоторых вариантах воплощения процессор устройства CD2 может определять одно или более отношений между выбранными двумя или более элементами и может генерировать второй набор правил на основе определенного одного или более отношений между выбранными двумя или более элементами. В некоторых вариантах воплощения изобретения отношение(я) может быть основано на одном или более сравнительных или относительных различиях между элементами или среди них, таких как те, которые описаны выше в отношении совместно используемых наборов данных 400 и 500a-500d.

[0184] В блоке 906 процессор устройства CD1 может генерировать первый набор правил, указывающий выбранные элементы. В некоторых вариантах воплощения изобретения первый набор правил может указывать элементы, выбранные процессором устройства CD1 в операциях блока 826.

[0185] В различных вариантах воплощения первый набор правил может включать в себя инструкции для объединения результата, сгенерированного с использованием первого набора правил, и результата, сгенерированного с использованием второго набора правил. Аналогично, в различных вариантах воплощения изобретения второй набор правил может включать в себя инструкции для объединения результата, сгенерированного с использованием первого набора правил, и результата, сгенерированного с использованием второго набора правил.

[0186] В блоке 908 процессор устройства CD1 может отправлять первый набор правил устройству CD2.

[0187] В блоке 910 процессор устройства CD2 может принимать первый набор правил.

[0188] В блоке 912 процессор устройства CD2 может отправлять второй набор правил устройству CD1.

[0189] В блоке 914 процессор устройства CD1 может принимать второй набор правил.

[0190] В блоке 916 процессор устройства CD1 может генерировать первый результат на основе выбранных элементов.

[0191] В блоке 918 процессор устройства CD1 может выбирать элементы из своих извлеченных элементов, используя второй набор правил. Например, процессор устройства CD1 может использовать идентификаторы каждого из выбранных элементов (например, один или более элементов 420-428 или один или более элементов совместно используемых наборов данных 500a-500d) для выбора элементов из элементов, которые извлечены из совместно используемого набора данных, хранящихся на устройстве CD1. В качестве другого примера, процессор устройства CD1 может использовать для выбора элементов из извлеченных элементов один или более идентификаторов одного из элементов и одну или более взаимосвязей среди выбранных элементов.

[0192] В блоке 920 процессор устройства CD1 может генерировать второй результат на основе выбранных элементов.

[0193] В некоторых вариантах воплощения изобретения каждый из первого и второго результатов может включать в себя строку данных. В некоторых вариантах воплощения изобретения каждый первый результат и второй результат могут включать в себя значение, основанное на информации о выбранных элементах совместно используемого набора данных. В некоторых вариантах воплощения изобретения процессор устройства CD1 может выполнять преобразование информации выбранных элементов, например, генерировать хеш значений в информации. В некоторых вариантах воплощения процессор устройства CD1 может генерировать строку данных на основе информации выбранных элементов, и может выполнять преобразование (например, генерировать

хеш) информации выбранных элементов для генерирования каждого первого результата и второго результата.

[0194] В блоке 922 процессор устройства CD1 может объединять первый результат и второй результат. В некоторых вариантах воплощения изобретения процессор устройства CD1 может объединять первый результат и второй результат в соответствии с инструкциями в первом наборе правил. В некоторых вариантах воплощения изобретения процессор устройства CD1 может объединять первый результат и второй результат в соответствии с инструкциями во втором наборе правил.

[0195] В блоке 924 процессор устройства CD2 может генерировать третий результат на основе выбранных элементов. В некоторых вариантах воплощения изобретения процессор устройства CD2 может генерировать третий результат на основе элементов, выбранных процессором CD2 из числа извлеченных элементов (например, в операциях блока 902).

[0196] В блоке 926 процессор устройства CD2 может выбирать элементы из своих извлеченных элементов, используя первый набор правил, полученный от устройства CD1.

[0197] В блоке 928 процессор устройства CD2 может генерировать четвертый результат на основе выбранных элементов.

[0198] В некоторых вариантах воплощения изобретения каждый из третьего результата и четвертого результата может включать в себя строку данных. В некоторых вариантах воплощения изобретения каждый третий результат и четвертый результат могут включать в себя значение, основанное на информации в выбранных элементах совместно используемого набора данных. В некоторых вариантах воплощения процессор устройства CD2 может выполнять преобразование информации выбранных элементов, например, генерировать хеш значений в информации. В некоторых вариантах воплощения изобретения процессор

устройства CD2 может генерировать строку данных на основе информации относительно выбранных элементов и может выполнить преобразование (например, сгенерировать хеш) информации относительно выбранных элементов, чтобы сгенерировать каждый из третьего и четвертого результатов.

[0199] В блоке 930 процессор устройства CD2 может объединить третий и четвертый результаты. В некоторых вариантах воплощения процессор устройства CD2 может объединять третий результат и четвертый результат в соответствии с инструкциями из первого набора правил. В некоторых вариантах воплощения изобретения процессор устройства CD2 может объединять первый результат и второй результат в соответствии с инструкциями во втором наборе правил.

[0200] В блоке 932 процессор устройства CD2 может зашифровать сообщение, используя объединенный результат. В некоторых вариантах воплощения изобретения сообщение может служить в качестве тестового сообщения, чтобы дать возможность процессору устройства CD1 определять, соответствует ли комбинированный результат, сгенерированный процессором устройства CD2, комбинированному результату, сгенерированному процессором устройства CD1.

[0201] В блоке 842 процессор устройства CD2 может отправлять зашифрованное сообщение устройству CD1.

[0202] В блоке 844 процессор устройства CD1 может принять зашифрованное сообщение.

[0203] В блоке 938 процессор устройства CD1 может попытаться расшифровать сообщение, используя объединенный результат (то есть объединенный результат, сгенерированный процессором устройства CD1 в операциях в блоке 922).

[0204] IB блоке определения 940 процессор устройства CD1 может

определить, была ли успешной расшифровка сообщения, полученного от устройства CD2. В некоторых вариантах воплощения изобретения успешное дешифрование зашифрованного сообщения, полученного от устройства CD2, может указывать, что объединенный результат, определенный с помощью устройства CD1, и объединенный результат, определенный с помощью устройства CD2, совпадают.

[0205] В ответ на идентификацию безуспешности дешифрования (то есть блок определения 940 =«No» (Нет)) процессор устройства CD1 может выполнять операции блоков 850 или 852 (как проиллюстрировано на ФИГ. 8).

[0206] В ответ на определение того, что расшифровка была успешной (то есть блок определения 940 = "Yes"(Да»)) процессор устройства CD1 может зашифровать связь, используя объединенный результат в блоке 942. Например, процессор устройства CD1 может зашифровать передаваемые данные, для которых процессор устройства CD1 отправил указание администратору набора данных в блоке 808 (как проиллюстрировано на ФИГ. 8).

[0207] В блоке 944 процессор устройства CD2 может расшифровать передаваемые данные, используя объединенный результат. В некоторых вариантах воплощения изобретения, следуя операциям в блоке 944, процессор устройства CD может принимать инструкции извлечения в блоке 820.

[0208] Способ 900A не ограничивается отправкой сообщения с устройства CD1 устройству CD2, и в различных вариантах воплощения изобретения процессор устройства CD2 может выполнять операции, описанные выше в отношении процессора устройства CD1, и наоборот. В некоторых вариантах воплощения изобретения процессоры устройства CD1 и устройства CD2 могут выполнять свои соответствующие операции способа

900A, так что устройство CD1 может отправлять зашифрованное сообщение устройству CD2, и впоследствии роли могут переключаться, чтобы устройство CD2 мог направлять зашифрованное сообщение устройству CD1.

[0209] На ФИГ. 9B проиллюстрирован способ 900B для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-9B, способ 900B может быть реализован процессором (например, процессором 202 и/или т.п.) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110). В блоках 822-858 и 902-944 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции блоков с одинаковыми номерами способов 800A и 900A.

[0210] В блоке 950 процессор диспетчера наборов данных может выполнять операции установления передачи данных с первым вычислительным устройством (CD1) и/или вторым вычислительным устройством (CD2). В блоках 952 и 954 процессор устройства CD1 и процессор устройства CD2 могут выполнять соответствующие операции установления передачи данных с менеджером набора данных. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для установления линии передачи данных между администратором набора данных и устройством CD1 и/или между диспетчером набора данных и устройством CD2. В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов

данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций предоставления/получения эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций синхронизации для синхронизации эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций для аутентификации диспетчера наборов данных, устройства CD1 и/или устройства CD2. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций блоков 802-820 (например, как описано в отношении способа 800A).

[0211] В некоторых вариантах воплощения изобретения после отправки запроса синхронизации (блок 852) процессор диспетчера наборов данных может снова выполнить операции подтверждения установления передачи данных в блоке 870.

[0212] На ФИГ. 10A проиллюстрирован способ 1000A для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-10A, способ 1000A может быть реализован процессором (например, процессором 202 и/или тому подобным) вычислительного устройства (например, вычислительные

устройства 102 и 106 и сетевой элемент 110). В блоках 818-858 и 902-914 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (устройство CD1) и второго устройства передачи данных (устройство CD2) могут выполнять операции с одинаковым образом пронумерованными блокам способов 800A и 900A.

[0213] В блоке 1002 процессор устройства CD1 может объединить первый и второй наборы правил для генерации объединенного набора правил. В некоторых вариантах воплощения изобретения первый набор правил может включать в себя инструкции для объединения первого и второго набора правил. В некоторых вариантах воплощения изобретения второй набор правил может включать в себя инструкции для объединения первого и второго набора правил.

[0214] В блоке 1004 процессор устройства CD1 может выбирать элементы из своих извлеченных элементов, используя объединенный набор правил. Например, процессор устройства CD1 может использовать идентификаторы каждого из выбранных элементов (например, один или более элементов 420-428 или один или более элементов совместно используемых наборов данных 500a-500d) для выбора элементов из извлеченных элементов из совместно используемого набора данных, хранящихся на устройстве CD1. В качестве другого примера, процессор устройства CD1 может использовать один или более идентификаторов одного из элементов и одну или более взаимосвязей среди выбранных элементов для выбора элементов из извлеченных элементов.

[0215] В блоке 1006 процессор устройства CD1 может генерировать первый результат на основе выбранных элементов.

[0216] В блоке 1008 процессор устройства CD2 может объединить первый и второй наборы правил, чтобы сформировать объединенный набор правил. В некоторых вариантах воплощения изобретения первый набор

правил может включать в себя инструкции для объединения первого и второго набора правил. В некоторых вариантах воплощения изобретения второй набор правил может включать в себя инструкции для объединения первого и второго набора правил.

[0217] В блоке 1010 процессор устройства CD2 может выбирать элементы из своих извлеченных элементов, используя объединенный набор правил. Например, процессор устройства CD2 может использовать идентификаторы каждого из выбранных элементов (например, один или более элементов 420-428 или один или более элементов совместно используемых наборов данных 500a-500d) для выбора элементов из извлеченных элементов из совместно используемого набора данных, хранящихся на устройстве CD2. В качестве другого примера, процессор устройства CD2 может использовать один или более идентификаторов одного из элементов и одну или более взаимосвязей среди выбранных элементов для выбора элементов из извлеченных элементов.

[0218] В блоке 1012 процессор устройства CD2 может генерировать второй результат на основе выбранных элементов.

[0219] В блоке 1014 процессор устройства CD1 может пытаться расшифровать сообщение (с устройства CD2), используя первый результат.

[0220] В блоке 1016 определения процессор устройства CD1 может определить, была ли расшифровка сообщения от устройства CD2 успешной. В некоторых вариантах воплощения изобретения успешное дешифрование зашифрованного сообщения от устройства CD2 может указывать, что первый результат и второй результат совпадают.

[0221] В ответ на идентификацию успешности дешифрования (то есть блок определения 1016 = «Yes» (Да)), процессор устройства CD1 может зашифровать передаваемые данные, используя первый результат в блоке

1018. Например, процессор устройства CD1 может зашифровать передаваемые данные, для которых процессор устройства CD1 отправил указание менеджеру набора данных в блоке 808 (как проиллюстрировано на ФИГ. 8).

[0222] В блоке 1020 процессор устройства CD2 может расшифровать передаваемые данные, используя второй результат.

[0223] Способ 1000A не ограничивается отправкой сообщения с устройства CD1 устройству CD2, и в различных вариантах воплощения изобретения процессор устройства CD2 может выполнять операции, описанные выше в отношении процессора устройства CD1, и наоборот. В некоторых вариантах воплощения изобретения процессоры устройства CD1 и устройства CD2 могут выполнять свои соответствующие операции способа 1000A, так что устройство CD1 может отправлять зашифрованное сообщение устройству CD2, и впоследствии могут роли переключаться, чтобы устройство CD2 могло отправлять зашифрованное сообщение устройству CD1.

[0224] На ФИГ. 10B проиллюстрирован способ 1000 для защиты передачи данных в соответствии с различными вариантами воплощения. Со ссылкой на ФИГ. 1-I0B, способ 1000B может быть реализован процессором (например, процессором 202 и/или т.п.) из вычислительного устройства (например, вычислительных устройств 102 и 106 и сетевого элемента 110). В блоках 822-858, 902-914 и 1002-1020 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции одинаково пронумерованных блоков способов 800A, 900A и 1000A.

[0225] В блоке 1030 процессор диспетчера наборов данных может выполнять операции установления передачи данных с первым вычислительным устройством (CD1) и/или вторым вычислительным

устройством (CD2). В блоках 1032 и 1034 процессор устройства CD1 и процессор устройства CD2 могут выполнять соответствующие операции установления передачи данных с диспетчером набора данных. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для установления линии передачи данных между администратором набора данных и устройством CD1 и/или между диспетчером набора данных и устройством CD2. В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций предоставления/получения эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций синхронизации для синхронизации эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для аутентификации диспетчера наборов данных, устройства CD1 и/или устройства CD2. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций

блоков 802-820 (например, как описано в отношении способа 800A).

[0226] В некоторых вариантах воплощения изобретения после расшифровки передачи данных с использованием второго результата в блоке 1020 процессор устройства CD2 может снова выполнять операции подтверждения установления передачи данных в блоке 1034.

[0227] На ФИГ. 11A проиллюстрирован способ 1100A для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-11A, способ 1100A может быть реализован процессором (например, процессором 202 и/или подобным) из вычислительного устройства (например, вычислительные устройства 102 и 106 и сетевой элемент 110). В блоках 818-858 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции одинаковым образом пронумерованных блоков способа 800A. В различных вариантах воплощения изобретения способ 1100A может быть полезен в реализациях, включающих одно или более вычислительных устройств, имеющих ограниченные ресурсы обработки и/или памяти. Один пример таких вычислительных устройств включает устройства IoT или другие подобные устройства.

[0228] В различных вариантах воплощения изобретения способ 1100A может быть полезен в реализациях, включающих в себя одно или более вычислительных устройств, имеющих ограниченные ресурсы обработки и/или памяти. Один пример таких вычислительных устройств включает устройства IoT или другие подобные устройства.

[0229] В блоке 1102 процессор устройства CD1 может зашифровать сообщение, используя первый результат. Например, процессор устройства CD1 может использовать метод шифрования, такой как MD5, SHA2, SHA256, BLAKE2 и тому подобные, вместе с первым результатом для

шифрования сообщения.

[0230] В блоке 1104 процессор устройства CD1 может отправлять зашифрованное сообщение второму вычислительному устройству.

[0231] В блоке 1106 процессор устройства CD2 может принять зашифрованное сообщение.

[0232] В блоке 1108 процессор устройства CD2 может расшифровать сообщение, используя второй результат. Например, процессор устройства CD1 может инициировать процесс дешифрования сообщения. В некоторых вариантах воплощения изобретения процессор устройства CD2 может пытаться расшифровать сообщение, используя второй результат. В различных вариантах воплощения изобретения процессор устройства CD1 может использовать формат дешифрования, такой как MD5, SHA2, SHA256, BLAKE2 и т.п., для попытки дешифрования сообщения.

[0233] В блоке 1110 процессор устройства CD2 может отправить сообщение подтверждения устройству CD1. В некоторых вариантах воплощения изобретения сообщение подтверждения может служить для указания того, что устройство CD1 возвращает процессору устройства CD2 сообщение, которое было успешно расшифровано с применением второго результата.

[0234] В блоке 1112 процессор устройства CD1 может ожидать сообщения подтверждения от устройства CD2. Например, процессор устройства CD1, отправив зашифрованное сообщение в блоке 1104, может ожидать получения сообщения подтверждения от устройства CD2.

[0235] В блоке определения 1114 процессор устройства CD1 может определить, соответствуют ли сведения сообщениям, принятым от устройства CD2.

[0236] В ответ на идентификацию получения сообщения подтверждения (то есть блок определения 1114 = «Yes» (Да)), процессор устройства CD1

может выполнять операции блока 854 (как проиллюстрировано на ФИГ.8).

[0237] В ответ на идентификацию непринятия сообщения подтверждения (то есть блок определения 1114 = «No» («Нет»)), процессор устройства CD1 может определить, истек ли период ожидания в блоке определения 1116. В некоторых вариантах воплощения изобретения процессор устройства CD1 может ожидать сообщения подтверждения от устройства CD2 за период времени (например, период ожидания).

[0238] В ответ на идентификацию того, что период ожидания не истек (то есть блок определения 1116 = «No» (Нет)), процессор устройства CD1 может снова определить, получено ли сообщение подтверждения в блоке определения 1114.

[0239] В ответ на идентификацию истечения периода ожидания (то есть блок определения 1116 = «Yes» (Да)), процессор устройства CD1 может выполнять операции блока 850 или блока 852 (как проиллюстрировано на ФИГ. 8).

[0240] На ФИГ. 11B проиллюстрирован способ 1100B для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-11B, способ 1100B может быть реализован процессором (например, процессором 202 и/или т.п.) из вычислительного устройства (например, вычислительные устройства 102 и 106 и сетевой элемент 110). В блоках 822-860 и 1102-1116 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции одинаково пронумерованных блоков способов 800A и 1100A.

[0241] В блоке 1120 процессор диспетчера наборов данных может выполнять операции установления передачи данных с первым вычислительным устройством (CD1) и/или вторым вычислительным

устройством (CD2). В блоках 1122 и 1124 процессор устройства CD1 и процессор устройства CD2 могут выполнять соответствующие операции подтверждения установления передачи данных с менеджером набора данных. В некоторых вариантах воплощения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций для установления линии передачи данных между администратором набора данных и CD1 и/или между диспетчером набора данных и устройством CD2. В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций предоставления/получения эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций синхронизации для синхронизации эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для аутентификации диспетчера наборов данных, устройства CD1 и/или устройства CD2. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, CD1 и/или CD2, могут включать в себя одну или более операций блоков 802-820

(например, как описано в отношении способа 800A).

[0242] В некоторых вариантах воплощения изобретения после отправки запроса синхронизации (блок 852) процессор диспетчера наборов данных может снова выполнить операции подтверждения установления передачи данных в блоке 870.

[0243] В некоторых вариантах воплощения изобретения, следуя операциям блока 856, процессор устройства CD1 может выполнять операции подтверждения установления передачи данных в блоке 1122.

[0244] В некоторых вариантах воплощения изобретения, следуя операциям блока 860, процессор устройства CD2 может выполнять операции подтверждения установления передачи данных в блоке 1124.

[0245] ФИГ. 12A иллюстрирует способ 1200A для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-12A, способ 1200A может быть реализован процессором (например, процессором 202 и/или т.п.) вычислительного устройства (например, вычислительными устройствами 102 и 106 и сетевым элементом 110). В блоках 818-838 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции одинаково пронумерованных блоков способа 800A.

.**[0246]** В некоторых вариантах воплощения изобретения операции способа 1200A могут использоваться в системе IoT. Например, каждое из устройств CD1 и CD2 может содержать или быть компонентом устройства IoT. В некоторых вариантах воплощения изобретения устройство CD1 может функционировать в качестве концентратора, контроллера, маршрутизатора или другого аналогичного устройства IoT. В некоторых вариантах воплощения изобретения устройство CD2 может функционировать как IoT-устройство, имеющее меньшие возможности

обработки и/или памяти, чем устройство CD1, такие как, например, смарт-лампочка или выключатель света, «умный» дверной замок или дверная ручка, или другое подобное устройство IoT. В некоторых вариантах воплощения изобретения операции устройства CD2, описанные в способе 1200A, относительно упрощены (например, по сравнению с операциями, описанными выше в отношении способов 800A и 800B), чтобы облегчить производительность устройства IoT или другого аналогичного устройства с относительно ограниченной вычислительной мощностью и/или памятью.

[0247] В блоке 1202 процессор устройства CD1 может зашифровать сообщение, используя первый результат. Например, процессор устройства CD1 может использовать метод шифрования, такой как MD5, SHA2, SHA256, BLAKE2 и тому подобное, вместе со вторым результатом для шифрования сообщения. В некоторых вариантах воплощения изобретения сообщение может служить в качестве тестового сообщения, чтобы дать возможность процессору устройства CD1 определять, соответствует ли второй результат, сгенерированный процессором устройства CD2, первому результату, сгенерированному процессором устройства CD1. В некоторых вариантах воплощения изобретения процессор устройства CD1 может генерировать относительно короткое сообщение, например, в случае, когда устройство CD2 является вычислительным устройством с относительно ограниченной вычислительной мощностью и/или памятью.

[0248] В блоке 1204 процессор устройства CD1 может отправлять зашифрованное сообщение устройству CD2.

[0249] В блоке 1206 процессор устройства CD2 может принять зашифрованное сообщение.

[0250] В блоке 1208 процессор устройства CD2 может попытаться расшифровать сообщение, используя первый результат. Например, процессор устройства CD2 может инициировать процесс дешифрования

сообщения. В различных вариантах воплощения изобретения процессор устройства CD2 может использовать формат дешифрования, такой как MD5, SHA2, SHA256, BLAKE2 и т.п., для попытки дешифрования сообщения.

[0251] В блоке 1210 процессор устройства CD2 может отправлять сообщение подтверждения устройству CD1.

[0252] В блоке определения 1212 процессор устройства CD1 может определить, принято ли сообщение подтверждения (например, сообщение подтверждения, отправленное устройством CD2 в блоке 1210).

[0253] В ответ на идентификацию приема сообщения подтверждения принято (то есть блок определения 1212 = «Yes» (Да)), процессор устройства CD1 может определить, что устройство CD2 аутентифицировано в блоке 1214. Процессор устройства CD1 затем может выполнять операции блока 808.

[0254] В ответ на идентификацию непринятия сообщения подтверждения (то есть блок определения 1212 = «No» (Нет)), процессор устройства CD1 может выполнять операции добавочных блоков 850 или 852.

[0255] На ФИГ. 12B проиллюстрирован способ 1200B для защиты передачи данных в соответствии с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-12B, способ 1200B может быть реализован процессором (например, процессором 202 и/или подобным) из вычислительного устройства (например, вычислительные устройства 102 и 106 и сетевой элемент 110). В блоках 822-852 и 1202-1214 процессоры устройств диспетчера наборов данных, первого устройства передачи данных (CD1) и второго устройства передачи данных (CD2) могут выполнять операции одинаково пронумерованных блоков способов 800A и 1200A.

[0256] В блоке 1220 процессор диспетчера наборов данных может

выполнять операции установления передачи данных с первым вычислительным устройством (CD1) и/или вторым вычислительным устройством (CD2). В блоках 1222 и 1224 процессор устройства CD1 и процессор устройства CD2 могут выполнять соответствующие операции подтверждения установления передачи данных с менеджером набора данных. В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций для установления линии передачи данных между администратором набора данных и устройством CD1 и/или между диспетчером набора данных и устройством CD2. В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций предоставления/получения эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции подтверждения установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций синхронизации для синхронизации эфемерного совместно используемого набора данных (например, как описано в отношении способа 700). В некоторых вариантах воплощения изобретения операции установления передачи данных, выполняемые процессорами диспетчера наборов данных, устройством CD1 и/или устройством CD2, могут включать в себя одну или более операций для аутентификации диспетчера наборов данных, устройства CD1 и/или устройства CD2. В некоторых вариантах воплощения изобретения операции установления передачи данных,

выполняемые процессорами диспетчера наборов данных, устройства CD1 и/или устройства CD2, могут включать в себя одну или более операций блоков 802-820 (например, как описано в отношении способа 800A).

[0257] В некоторых вариантах воплощения изобретения после отправки запроса синхронизации (блок 852) процессор диспетчера наборов данных может снова выполнить операции подтверждения установления передачи данных в блоке 870.

[0258] В некоторых вариантах воплощения, следуя операциям блока 856, процессор устройства CD1 может выполнять операции подтверждения установления передачи данных в блоке 1122.

[0259] В некоторых вариантах воплощения изобретения, следуя операциям блока 860, процессор устройства CD2 может выполнять операции подтверждения установления передачи данных в блоке 1124.

[0260] На ФИГ. 13 проиллюстрирована блок-схема компонента мобильного устройства беспроводной передачи данных 1300, подходящая для использования с различными вариантами воплощения изобретения. Со ссылкой на ФИГ. 1-13, мобильное устройство беспроводной передачи данных 1300 может содержать процессор 1302, связанный с контроллером сенсорного экрана 1306, и внутреннюю память 1304. Процессор 1302 может быть представлен одной или более многоядерными интегральными схемами, предназначенными для общих или специальных задач обработки. Внутренняя память 1304 может быть энергозависимой или энергонезависимой памятью, а также может быть защищенной и/или зашифрованной памятью, или незащищенной и/или незашифрованной памятью, или любой их комбинацией. Контроллер сенсорного экрана 1306 и процессор 1302 также могут соединяться с сенсорной панелью 1312, такой как сенсорный экран с резистивным сенсором, сенсорный экран с емкостным сенсором, сенсорный экран с инфракрасным сенсором и т.д.

Кроме того, дисплей мобильного устройства беспроводной передачи данных 1300 не обязательно имеет возможность сенсорного экрана.

[0261] Устройство мобильной беспроводной передачи данных 1300 может содержать два или более приемопередатчика радиосигнала 1308 (например, Bluetooth, Zigbee, Wi-Fi, радиочастотного диапазона и т. д.) и антенны для отправки и приема сообщений 1310, связанных друг с другом, и/или с процессором 1302. Приемопередатчики 1308 и антенны 1310 могут использоваться с вышеупомянутой схемой для реализации различных стеков и интерфейсов протокола беспроводной передачи данных. Устройство мобильной беспроводной передачи данных 1300 может содержать один или более чипов беспроводных модемов сотовой сети 1316, соединенных с процессором и антеннами 1310, которые обеспечивают связь посредством двух или более сотовых сетей, с применением двух или более технологий радиодоступа.

[0262] Устройство мобильной беспроводной передачи данных 1300 может содержать интерфейс подключения беспроводного периферийного устройства 1318, соединенный с процессором 1302. Интерфейс подключения беспроводного периферийного устройства 1318 может быть индивидуально выполнен с возможностью приема одного типа соединения или может быть выполнен с возможностью приема различных типов физических и коммуникационных соединений, обычных или фирменных, таких как USB, FireWire, Thunderbolt или PCIe. Интерфейс подключения периферийного беспроводного устройства 1318 также может быть подключен к аналогичным образом выполненному порту подключения периферийного беспроводного устройства (не показан).

[0263] Мобильное устройство беспроводной передачи данных 1300 также может содержать динамики 1310 для предоставления аудиовыходов. Устройство мобильной беспроводной передачи данных 1300 также может

содержать корпус 1320, выполненный из пластика, металла или комбинации материалов, для размещения всех или некоторых из рассматриваемых компонентов. Устройство мобильной беспроводной передачи данных 1300 может содержать источник питания 1322, связанный с процессором 1302, такой как одноразовая или перезаряжаемая (аккумуляторная) батарея. Аккумуляторная батарея также может быть подключена к порту подключения периферийного беспроводного устройства для приема зарядного тока от источника, внешнего по отношению к мобильному устройству беспроводной передачи данных 1300. Устройство мобильной беспроводной передачи данных 1300 также может включать в себя физическую кнопку 1324 для приема пользовательского ввода. Мобильное устройство беспроводной передачи данных 1300 также может содержать кнопку питания 1326 для включения и выключения мобильного устройства беспроводной передачи данных 1300.

[0264] Другие формы вычислительных устройств также могут извлекать выгоду из различных аспектов. Такие вычислительные устройства обычно содержат компоненты, проиллюстрированные на ФИГ. 14, которые иллюстрирует пример портативного компьютера 1400. Со ссылкой на ФИГ. 1-14, компьютер 1400 обычно содержит процессор 1401, связанный с энергозависимой памятью 1402, и энергонезависимую память большой емкости, такую как дисковод 1403. Компьютер 1400 также может содержать привод компакт-дисков (CD) и/или DVD-привод 1404, подключенный к процессору 1401. Компьютер 1400 также может содержать ряд портов разъема, подключенных к процессору 1401, для установления соединений для передачи данных или приема внешних устройств памяти, таких как схема сетевого соединения 1405 для соединения процессора 1401 с сетью. Компьютер 1400 также может содержать дисплей 1407, клавиатуру 1408, указательное устройство, такое как трекпад 1410 и другие подобные

устройства.

[0265] Различные варианты воплощения изобретения могут использовать вычислительное устройство в качестве сетевого элемента сети передачи данных. Такие сетевые элементы обычно могут содержать по меньшей мере компоненты, проиллюстрированные на ФИГ. 15, которая иллюстрирует пример сетевого элемента серверного устройства 1500. Со ссылкой на ФИГ. 1-15, серверное устройство 1500 обычно может содержать процессор 1501, связанный с энергозависимой памятью 1502, и энергонезависимую память большой емкости, такую как дисковод 1503. Серверное устройство 1500 также может содержать периферийное устройство доступа к памяти, такое как гибкий диск, жесткий диск, привод компакт-дисков (CD) или привод DVD 1506, соединенный с процессором 1501.Серверное устройство 1500 также может содержать порты доступа к сети (или интерфейсы) 1504, соединенные с процессором 1501, для установления соединений для передачи данных по сети, такой как Интернет и/или локальная сеть, соединенная с другими компьютерами и серверами системы. Аналогично, серверное устройство 1500 может содержать дополнительные порты доступа, такие как USB, Firewire, Thunderbolt и т.п., для подключения к периферийным устройствам, внешней памяти или другим устройствам.

[0266] Процессоры 1302, 1401, 1501 могут быть любыми программируемыми микропроцессорами, микрокомпьютерами или микросхемами или микросхемами с несколькими процессорами, которые могут быть выполнены с возможностью использования программных инструкций (приложений) для выполнения множества функций, включая функции различных аспектов, описанные ниже. В некоторых мобильных устройствах могут быть предусмотрены несколько процессоров 1302, например, один процессор, предназначенный для обеспечения функций

беспроводной передачи данных, и один процессор, предназначенный для запуска других приложений. Как правило, программные приложения могут храниться во внутренней памяти 1304, 1402, 1502 до того, как к ним осуществляется доступ, и они загружаются в процессор 1302, 1401, 1501. Процессор 1302, 1401, 1501 может содержать внутреннюю память, достаточную для хранения инструкций прикладных программ.

[0267] Различные варианты воплощения изобретения расширяют и улучшают функцию безопасности любой сети передачи данных или любой системы электронной передачи данных, улучшая безопасность передачи данных, используя динамически изменяющийся контекст совместно используемой информации. Различные варианты воплощения изобретения также расширяют и улучшают безопасность передачи данных в сети передачи данных, используя динамически генерируемый результат, основанный на динамически изменяющемся контексте совместно используемой информации. Информационный контекст может содержать, например, динамически изменяющийся совместно используемый набор данных. Различные варианты воплощения изобретения также улучшают функцию безопасности любой сети передачи данных, используя динамический совместно используемый набор данных и динамически генерируемое значение на основе динамического совместно используемого набора данных, не полагаясь на легко компрометируемую статическую идентификационную информацию (такую как, общий секрет), которая может быть уязвимой при несанкционированном доступе и копировании. Различные варианты воплощения изобретения используют динамически изменяющиеся совместно используемые данные и динамически генерируемое значение для защиты передачи данных способом, который не зависит от парадигмы общих секретов и статической информации.

[0268] Различные варианты воплощения изобретения, проиллюстрированные и описанные, представлены просто в качестве примеров, чтобы проиллюстрировать различные признаки формулы изобретения. Однако признаки, показанные и описанные в отношении любого данного варианта воплощения изобретения, не обязательно ограничены соответствующим вариантом воплощения и могут использоваться или комбинироваться с другими вариантами воплощения изобретения, которые показаны и описаны. Кроме того, пункты формулы изобретения не предназначены для ограничения каким-либо одним примером воплощения. Например, одна или более операций способов 300, 700, 800A, 800B, 900A, 900B, 1000A, 1000B, 1100A, 1100B,1200A и 1200B могут быть заменены или объединены с одной или более операций способов 300, 700, 800A, 800B, 900A, 900B, 1000A, 1000B, 1100A, 1100B, 1200A и 1200B.

[0269] Различные варианты воплощения изобретения могут быть выполнены в любом количестве однопроцессорных или многопроцессорных систем. Обычно процессы выполняются на процессоре в течение коротких временных интервалов, поэтому создается впечатление, что несколько процессов выполняются одновременно на одном процессоре. Когда процесс удаляется из процессора в конце временного интервала, информация, относящаяся к текущему рабочему состоянию процесса, сохраняется в памяти, поэтому процесс может беспрепятственно возобновить свои операции, когда возвращается к выполнению на процессоре. Эти данные рабочего состояния могут содержать адресное пространство процесса, пространство стека, пространство виртуального адреса, изображение набора регистров (например, счетчик программы, указатель стека, регистр команд, регистр состояния программы и т. д.), учетную информацию, разрешения,

ограничения доступа и информацию о состоянии.

[0270] Процесс может порождать другие процессы, и порожденный процесс (то есть, дочерний процесс) может наследовать некоторые из разрешений и ограничений доступа (то есть контекст) процесса порождения (то есть, родительского процесса). Процесс может быть тяжеловесным процессом, который содержит несколько легковесных процессов или потоков, которые являются процессами, совместно использующими весь или часть своего контекста (например, адресное пространство, стек, разрешения и/или ограничения доступа и т. д.) вместе с другими процессами/потоками. Таким образом, один процесс может содержать несколько облегченных процессов или потоков, которые совместно используют, имеют доступ и/или работают в одном контексте (то есть в контексте процессора).

[0271] Вышеприведенные описания способов и технологические схемы представлены только в качестве иллюстративных примеров и не предназначены для того, чтобы требовать или подразумевать, что блоки различных вариантов воплощения изобретения должны выполняться в представленном порядке. Как будет понятно специалисту в данной области техники, порядок следования блоков в вышеупомянутых вариантах воплощения может быть любым. Такие слова, как «после этого», «затем», «далее» и т. д. не предназначены для ограничения порядка блоков; эти слова просто используются, чтобы помочь читателю в описании способов. Далее, любую ссылку на элементы формулы в единственном числе, например, с использованием артиклей «a», «an» или «the» не следует истолковывать как ограничение элемента в единственном числе.

[0272] Различные иллюстративные логические блоки, модули, схемы и блоки алгоритмов, описанные в передачи данных с раскрытыми здесь

вариантами воплощения изобретения, могут быть реализованы как электронное аппаратное обеспечение, компьютерное программное обеспечение или их комбинации. Чтобы ясно проиллюстрировать эту взаимозаменяемость аппаратных средств и программного обеспечения, различные иллюстративные компоненты, блоки, модули, схемы и блоки алгоритмов были описаны выше в основном с точки зрения их функциональных возможностей. Реализация такого функционала аппаратного или программного обеспечения зависит от конкретного приложения и конструктивных ограничений, наложенных на всю систему. Опытные специалисты могут реализовывать описанные функциональные возможности различными способами для каждого конкретного приложения, но такие решения по реализации не должны интерпретироваться как вызывающие отклонение от объема формулы изобретения.

[0273] Аппаратные средства, используемые для реализации различных иллюстративных логических схем, логических блоков, модулей и схем, описанных в связи с раскрытыми здесь вариантами воплощения изобретения, могут быть реализованы или выполнены с процессором общего назначения, процессором цифровых сигналов (DSP), специализированной интегральной схемой (ASIC), полевой программируемой вентильной матрицей (FPGA) или другим программируемым логическим устройством, дискретным логическим вентилем или транзисторной логикой, дискретными аппаратными компонентами или любой их комбинацией, разработанной выполнять описанные здесь функции. Универсальный процессор может быть микропроцессором, но, в качестве альтернативы, процессор может быть любым обычным процессором, контроллером, микроконтроллером или конечным автоматом. Процессор также может быть реализован в виде комбинации устройств передачи данных, например, комбинации DSP и

микропроцессора, множества микропроцессоров, одного или более микропроцессоров в сочетании с ядром DSP или любой другой подобной конфигурации. Альтернативно, некоторые блоки или способы могут быть выполнены с помощью схемы, которая является определенной для данной функции.

[0274] В различных вариантах воплощения изобретения описанные функции могут быть реализованы в виде аппаратного обеспечения, программного обеспечения, встроенного программного обеспечения или любой их комбинации. При реализации в программном обеспечении функции могут храниться в виде одной или более инструкций или кода на долговременном машиночитаемом носителе или долговременном читаемом процессором носителе. Операции способа или алгоритма, раскрытого в данном документе, могут быть воплощены в исполняемом процессором программном модуле, который может находиться на долговременном машиночитаемом или постоянном читаемом процессором носителе данных. Постоянные машиночитаемые или читаемые процессором носители данных могут быть любыми носителями данных, к которым может обращаться компьютер или процессор. В качестве примера, но не ограничиваясь им, такие постоянные машиночитаемые или читаемые процессором носители данных могут содержать ОЗУ, ПЗУ, ЭСППЗУ, флэш-память, CD-ROM или другое устройство хранения данных на оптических дисках, магнитное дисковое хранилище или другие магнитные запоминающие устройства, или любой другой носитель данных, который может использоваться для хранения требуемого программного кода в форме инструкций или структур данных, и к которому может обращаться компьютер. Термин «диск», используемый в данном документе, означает компакт-диск (CD), лазерный диск, оптический диск, цифровой универсальный диск (DVD), дискету и диск Blu-ray, причем на

дискете данные записываются и воспроизводятся путем использования магнитных свойств, тогда как данные на дисках воспроизводятся оптическим путем, с помощью лазеров. Комбинации вышеупомянутого также относятся к постоянным машиночитаемым и считываемым процессором носителям данных. Кроме того, операции способа или алгоритма могут находиться в виде одной или любой комбинации или набора кодов и/или инструкций на постоянном машиночитаемом носителе данных и/или считываемых процессором носителе данных, которые могут быть включены в компьютерную программу.

[0275] Предшествующее описание раскрытых вариантов воплощения изобретения предоставлено, чтобы дать возможность любому специалисту в данной области техники создавать или использовать формулу изобретения. Различные модификации этих вариантов воплощения изобретения будут очевидны для специалистов в данной области техники, и общие принципы, определенные в данном документе, могут быть применены к другим вариантам воплощения изобретения без отступления из объема формулы изобретения. Таким образом, настоящее описание не предназначено для ограничения показанными здесь вариантами воплощения изобретения, а должно соответствовать самому широкому объему, совместимому со следующей формулой изобретения и раскрытыми здесь принципами и новыми признаками.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Устройство управления наборами данных для управления синхронизацией эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, содержащее:

память; и

процессор, связанный с памятью и имеющий схему исполняющих процессором инструкций для выполнения операций, включающих:

предоставление эфемерного совместно используемого набора данных первому вычислительному устройству и второму вычислительному устройству;

генерирование инструкции для изменения эфемерного совместно используемого набора данных; и

отправку сгенерированной инструкции первому вычислительному устройству и

второму вычислительному устройству для изменения эфемерного совместно используемого набора данных на первом и втором вычислительных устройствах в соответствии со сгенерированной инструкцией, так что эфемерный совместно используемый набор данных, сохраненный на первом вычислительном устройстве, совпадает с эфемерным совместно используемым набором данных, хранящимся на втором вычислительном устройстве.

2. Устройство управления набором данных по п. 1, отличающееся

тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, причем генерирование инструкции для изменения совместно используемого набора данных включает:

определение наличия триггера обновления набора данных; и

генерирование инструкции для изменения эфемерного совместно используемого набора данных в ответ на идентификацию наличия триггера обновления набора данных.

3. Устройство управления набором данных по п. 1, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, причем генерирование инструкции для изменения совместно используемого набора данных включает:

генерирование инструкции для замены эфемерного совместно используемого набора данных набором данных замены, определенным устройством управления набором данных.

4. Устройство управления набором данных по п. 1, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, причем генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для добавления новой части в эфемерный совместно используемый набор данных на основе входных данных, полученных устройством управления набором данных.

5. Устройство управления набором данных по п. 1, отличающееся тем, что

процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, причем генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для вычитания части совместно используемого набора данных.

6. Устройство управления набором данных по п. 1, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для исполнения операций, причем генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для переупорядочения эфемерного совместно используемого набора данных.

7. Устройство управления набором данных по п. 1, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, причем генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для преобразования эфемерного совместно используемого набора данных.

8. Устройство управления набором данных по п. 1, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, дополнительно включающих:

выполнение операции синхронизации с первым вычислительным устройством и вторым вычислительным устройством таким

образом, чтобы измененный набор данных, сохраненный в первом вычислительном устройстве, был таким же, как измененный набор данных, сохраненный во втором вычислительном устройстве.

9. Способ управления синхронизацией эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, включающий:

предоставление эфемерного совместно используемого набора данных из устройства управления наборами данных первому вычислительному устройству и второму вычислительному устройству;

генерирование инструкции для изменения эфемерного совместно используемого набора данных; и

отправку сгенерированной инструкции первому вычислительному устройству и второму вычислительному устройству для изменения эфемерного совместно используемого набора данных на первом и втором вычислительных устройствах в соответствии со сгенерированной инструкцией так, чтобы эфемерный совместно используемый набор данных, хранящийся на первом вычислительном устройстве, был таким же, что и эфемерный совместно используемый набор данных, хранящийся на втором вычислительном устройстве.

10. Способ по п. 9, отличающийся тем, что генерирование инструкции для изменения совместно используемого набора данных включает:

определение наличия триггера обновления набора данных; и

генерирование инструкции для изменения эфемерного совместно

используемого набора данных в ответ на определение наличия триггера обновления набора данных.

11. Способ по п. 9, отличающийся тем, что генерирование инструкции для изменения совместно используемого набора данных включает:

генерирование инструкции для замены эфемерного совместно используемого набора данных набором данных замены, определенным устройством управления набором данных.

12. Способ по п. 9, отличающийся тем, что генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для добавления новой части в эфемерный совместно используемый набор данных на основе входных данных, полученных устройством управления набором данных.

13. Способ по п. 9, отличающийся тем, что генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для вычитания части совместно используемого набора данных.

14. Способ по п. 9, отличающийся тем, что генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для переупорядочения эфемерного совместно используемого набора данных.

15. Способ по п. 9, отличающийся тем, что генерирование инструкции для

изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для преобразования эфемерного совместно используемого набора данных.

16. Способ по п. 9, отличающийся тем, что дополнительно включает:

выполнение операции синхронизации с первым вычислительным устройством и вторым вычислительным устройством таким образом, чтобы измененный набор данных, сохраненный в первом вычислительном устройстве, был таким же, как измененный набор данных, сохраненный во втором вычислительном устройстве.

17. Постоянный считываемый процессором носитель данных, на котором хранятся исполняемые процессором инструкции, скомпонованные с возможностью инициировать процессор устройства управления наборами данных выполнять операции, включающие:

предоставление эфемерного совместно используемого набора данных первому вычислительному устройству и второму вычислительному устройству;

генерирование инструкции для изменения эфемерного совместно используемого набора данных; и

отправку сгенерированной инструкции первому вычислительному устройству и второму вычислительному устройству для изменения эфемерного совместно используемого набора данных на первом и втором вычислительных устройствах в соответствии со сгенерированной инструкцией так, чтобы эфемерный совместно используемый набор данных, сохраненный на первом вычислительном устройстве, был

таким же, как эфемерный совместно используемый набор данных, хранящийся на втором вычислительном устройстве.

18. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции выполнены с возможностью инициировать процессор устройства управления наборами данных выполнять операции, при которых генерирование инструкции для изменения совместно используемого набора данных включает:

определение наличия триггера обновления набора данных; и

генерирование инструкции для изменения эфемерного совместно используемого набора данных в ответ на определение наличия триггера обновления набора данных.

19. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор устройства управления наборами данных выполнять операции, при которых генерирование инструкции для изменения совместно используемого набора данных включает:

генерирование инструкции для замены эфемерного совместно используемого набора данных набором данных замены, определенным устройством управления набором данных.

20. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор устройства управления наборами данных выполнять операции, при

которых генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для добавления новой части в эфемерный совместно используемый набор данных на основе входных данных, полученных устройством управления набором данных.

21. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор устройства управления наборами данных выполнять операции, при которых генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для вычитания части совместно используемого набора данных.

22. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор устройства управления наборами данных выполнять операции, при которых генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для переупорядочения эфемерного совместно используемого набора данных.

23. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор

устройства управления наборами данных выполнять операции, при которых генерирование инструкции для изменения эфемерного совместно используемого набора данных включает:

генерирование инструкции для преобразования эфемерного совместно используемого набора данных.

24. Постоянный считываемый процессором носитель данных по п. 17, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор устройства управления наборами данных выполнять операции, дополнительно включающие:

выполнение операции синхронизации с первым вычислительным устройством и вторым вычислительным устройством так, чтобы измененный набор данных, сохраненный в первом вычислительном устройстве, был таким же, как измененный набор данных, сохраненный во втором вычислительном устройстве.

25. Вычислительное устройство, содержащее:

память; и

процессор, связанный с памятью и предусматривающий исполнение процессором инструкций для выполнения операций, включающих:

выбор элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве;

генерирование набора правил, указывающего выбранные элементы;

отправка сгенерированного набора правил второму

вычислительному устройству;

генерирование результата на основе выбранных элементов;

получение зашифрованных передаваемых данных от второго вычислительного устройства;

попытку расшифровать зашифрованные передаваемые данные, используя сгенерированный результат; и

идентификацию успешности попытки расшифровки.

26. Вычислительное устройство по п. 25, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, при которых выбор элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, включает:

получение инструкций от устройства управления наборами данных для извлечения элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве; и

извлечение элементов из совместно используемого набора данных в соответствии с инструкциями.

27. Вычислительное устройство по п. 26, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, при которых выбор элементов из совместно используемого набора данных, сохраненного в первом вычислительном устройстве и втором вычислительном устройстве, включает:

выборку элементов из числа извлеченных элементов.

28. Вычислительное устройство по п. 25, отличающееся тем, что процессор сконфигурирован с возможностью исполнения процессором инструкций для выполнения операций, дополнительно включающих:

шифрование передаваемых данных с использованием первого результата в ответ на определение успешности попытки расшифровки; и

отправку зашифрованных передаваемых данных второму вычислительному устройству.

29. Способ защиты передаваемых данных, включающий:

выбор элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве;

генерирование набора правил, указывающего выбранные элементы;

отправка сгенерированного набора правил второму вычислительному устройству;

генерирование результата на основе выбранных элементов;

получение зашифрованных передаваемых данных от второго вычислительного устройства;

попытку расшифровать зашифрованные передаваемые данные, используя сгенерированный результат; и

определение успешности попытки дешифровки.

30. Способ по п. 29, отличающийся тем, что выбор элементов из эфемерного совместно используемого набора данных, сохраненных в первом вычислительном устройстве и втором вычислительном устройстве,

включает:

получение инструкций от устройства управления наборами данных для извлечения элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве; и

извлечение элементов из совместно используемого набора данных в соответствии с инструкциями.

31. Способ по п. 30, отличающийся тем, что выбор элементов из совместно используемого набора данных, сохраненных в первом вычислительном устройстве и втором вычислительном устройстве, включает:

выбор элементов из числа извлеченных элементов.

32. Способ по п. 29, отличающийся тем, что дополнительно включает:

шифрование сообщения с использованием первого результата в ответ на определение того, что попытка расшифровки прошла успешно; и

отправку зашифрованных данных второму вычислительному устройству.

33. Постоянный считываемый процессором носитель данных, на котором хранятся исполняемые процессором инструкции, скомпонованные с возможностью инициировать процессор вычислительного устройства выполнять операции, включающие:

выбор элементов из эфемерного совместно используемого набора

данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве;

генерирование набора правил, указывающего выбранные элементы;

отправку сгенерированного набора правил второму вычислительному устройству;

генерирование результата на основе выбранных элементов;

получение зашифрованных передаваемых данных от второго вычислительного устройства;

попытку расшифровать зашифрованные передаваемые данные, используя сгенерированный результат; и

определение успешности попытки дешифровки.

34. Постоянный считываемый процессором носитель данных по п. 33, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор вычислительного устройства выполнять операции таким образом, что выбор элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве, включает:

получение инструкций от устройства управления наборами данных для извлечения элементов из эфемерного совместно используемого набора данных, хранящихся в первом вычислительном устройстве и втором вычислительном устройстве; и

извлечение элементов из совместно используемого набора данных в соответствии с инструкциями.

35. Постоянный считываемый процессором носитель данных по п. 34,

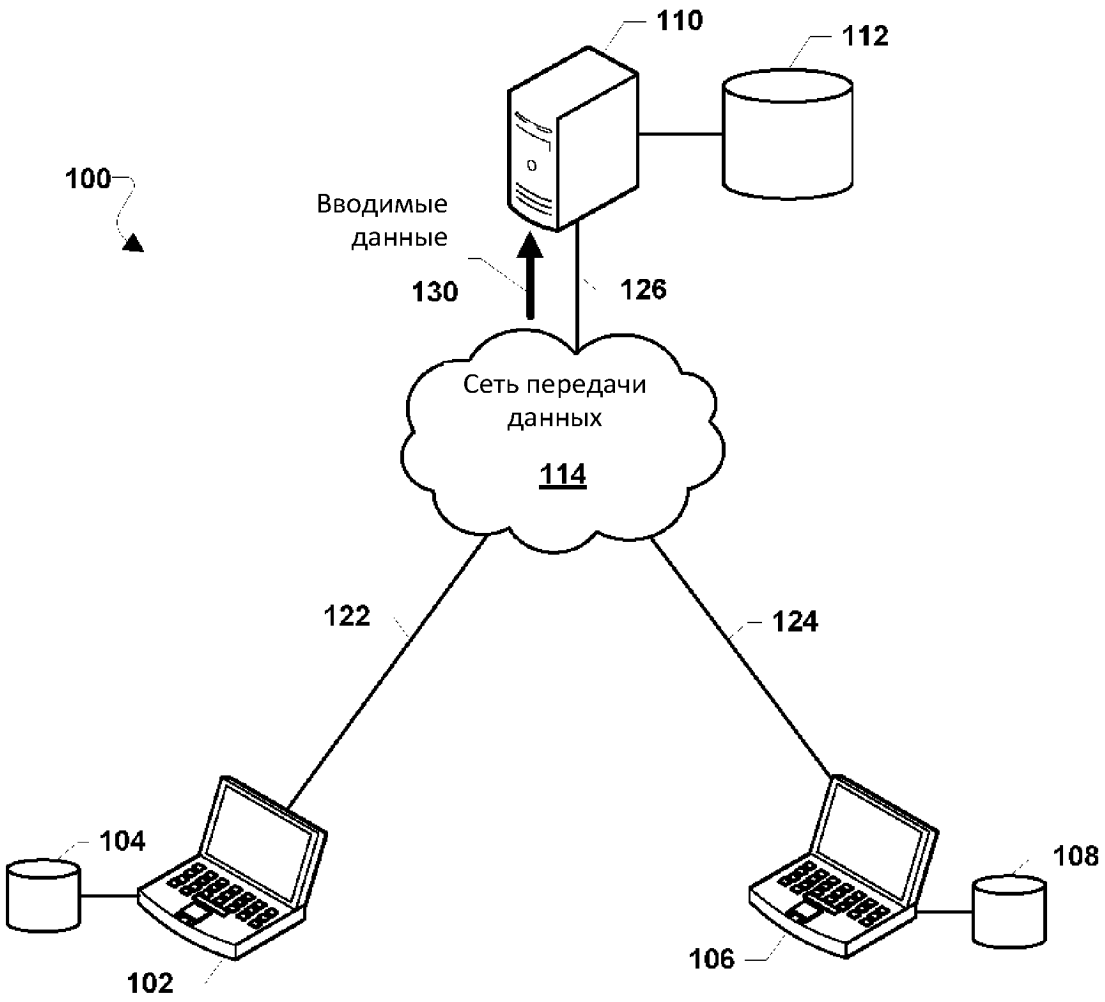
отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор вычислительного устройства выполнять операции таким образом, что выбор элементов из совместно используемого набора данных, сохраненного в первом вычислительном устройстве и втором вычислительном устройстве, включает:

выбор элементов среди извлеченных элементов.

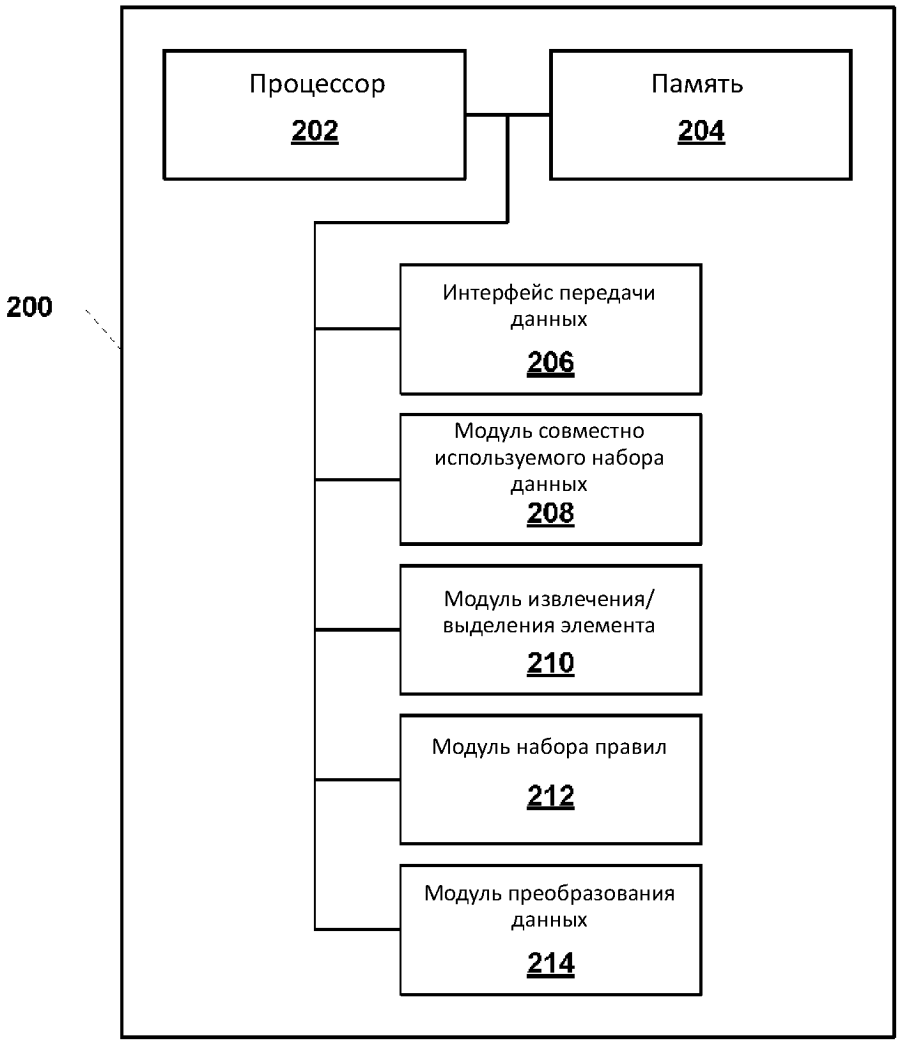
36. Постоянный считываемый процессором носитель данных по п. 33, отличающийся тем, что сохраненные исполняемые процессором инструкции скомпонованы с возможностью инициировать процессор вычислительного устройства выполнять операции, дополнительно включающие:

шифрование сообщения с использованием первого результата в ответ на определение того, что попытка расшифровки прошла успешно; и

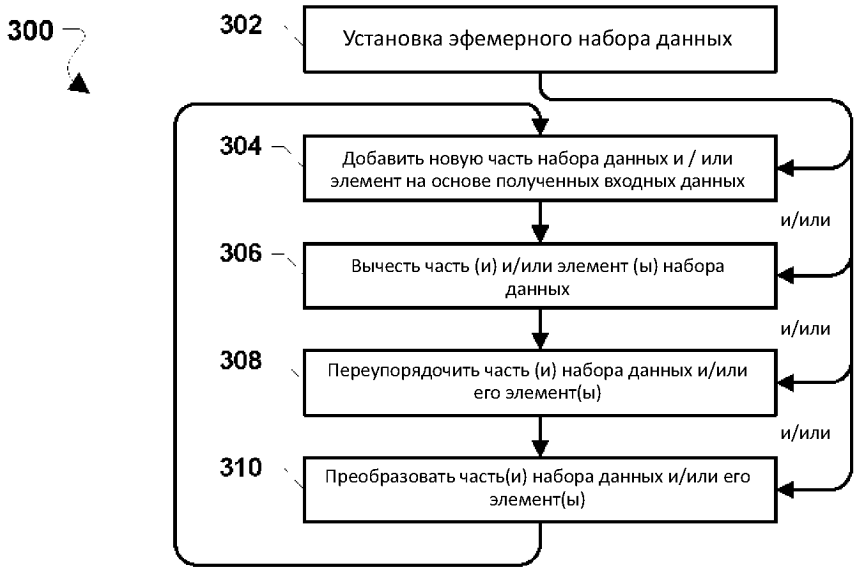
отправку зашифрованных передаваемых данных второму вычислительному устройству.


110
112
100
Вводимые
данные
130
126
Сеть передачи
данных
114
122
124
104
108
102
106

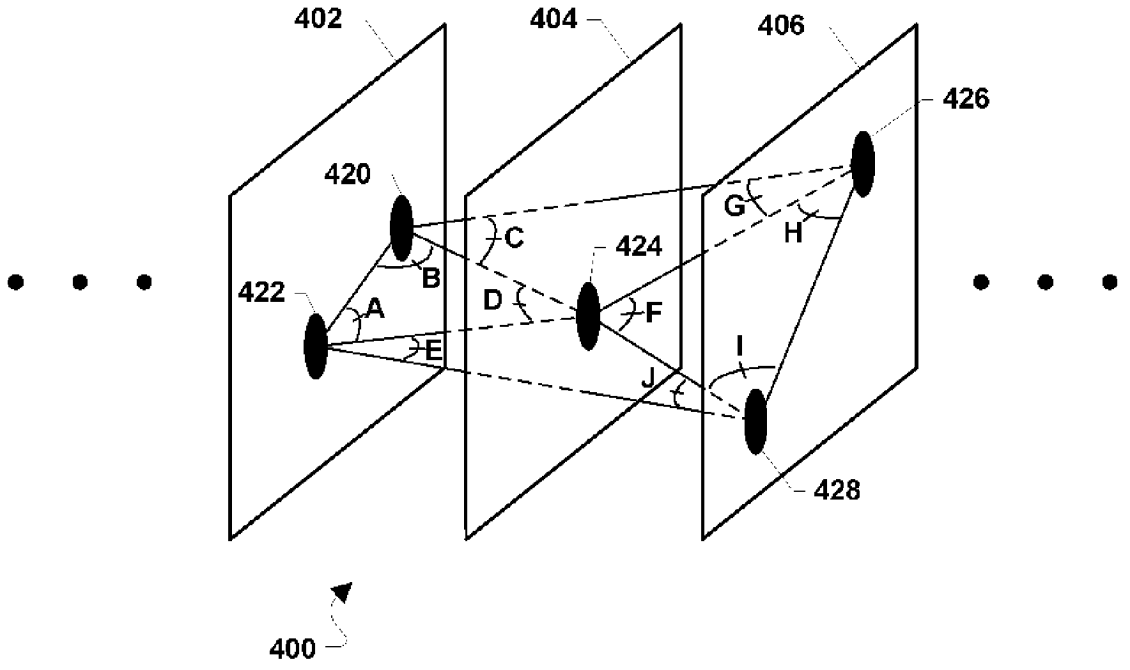
ФИГ. 1


200
Процессор
202
Память
204
Интерфейс передачи данных
206
Модуль совместно используемого набора данных
208
Модуль извлечения/ выделения элемента
210
Модуль набора правил
212
Модуль преобразования данных
214

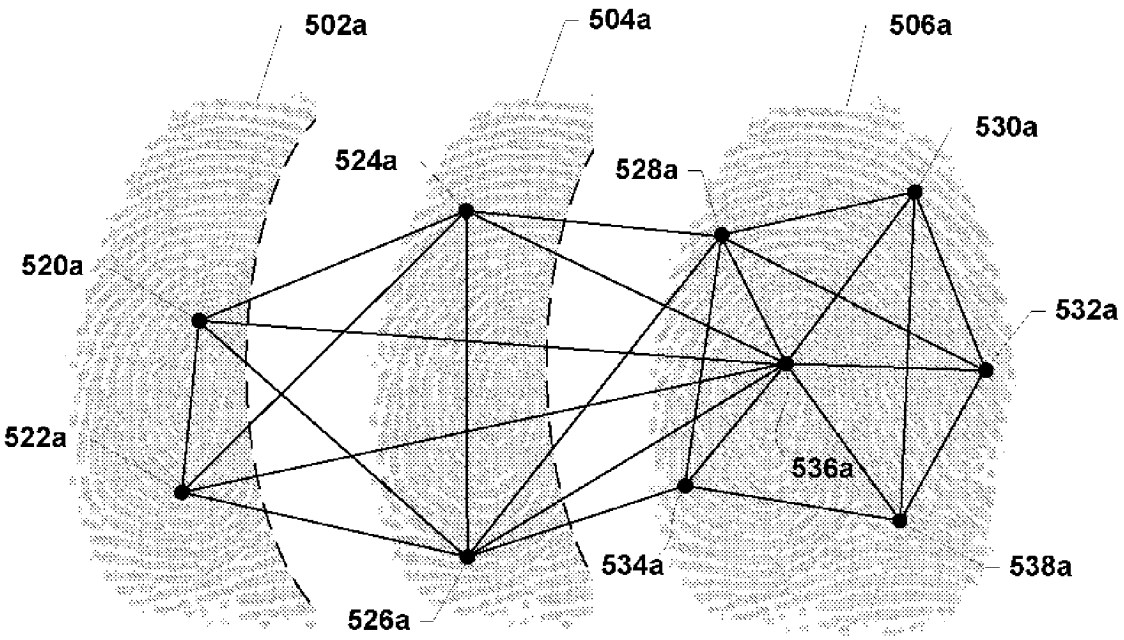
ФИГ. 2


300
302
Установка эфемерного набора данных
304
Добавить новую часть набора данных и / или элемент на основе полученных входных данных
и/или
306
Вычесть часть (и) и/или элемент (ы) набора данных
и/или
308
Переупорядочить часть (и) набора данных и/или его элемент(ы)
и/или
310
Преобразовать часть(и) набора данных и/или его элемент(ы)

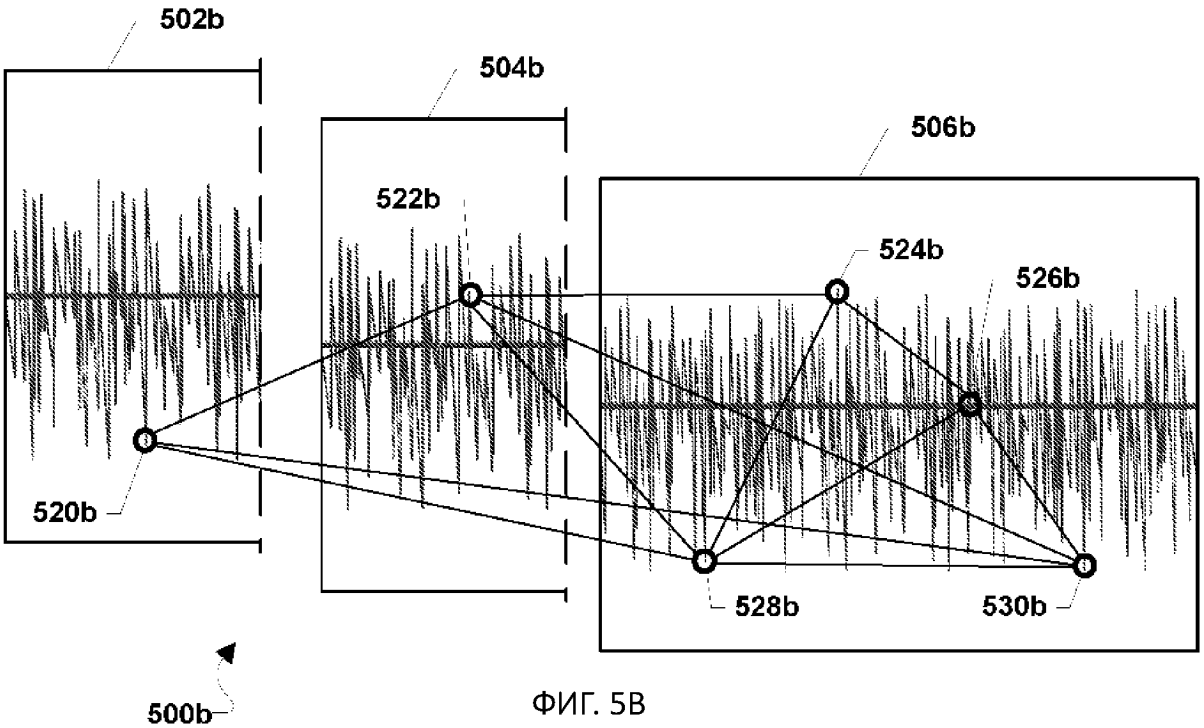
ФИГ. 3


402
404
406
426
420
424
422
A
B
C
D
E
F
G
H
I
J
428
400

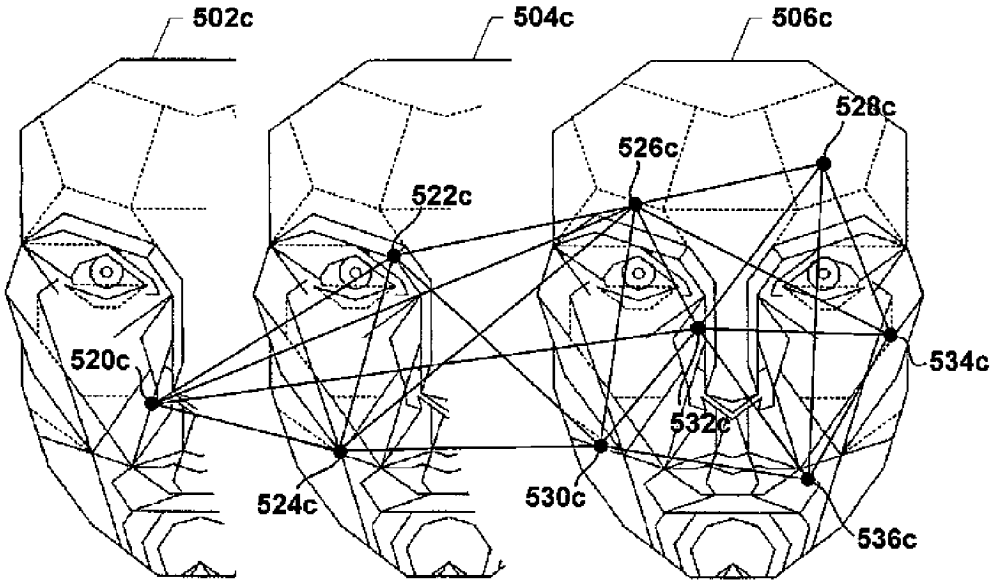
ФИГ. 4


502a
504a
506a
524a
528a
530a
520a
532a
522a
536a
534a
538a
526a
500a

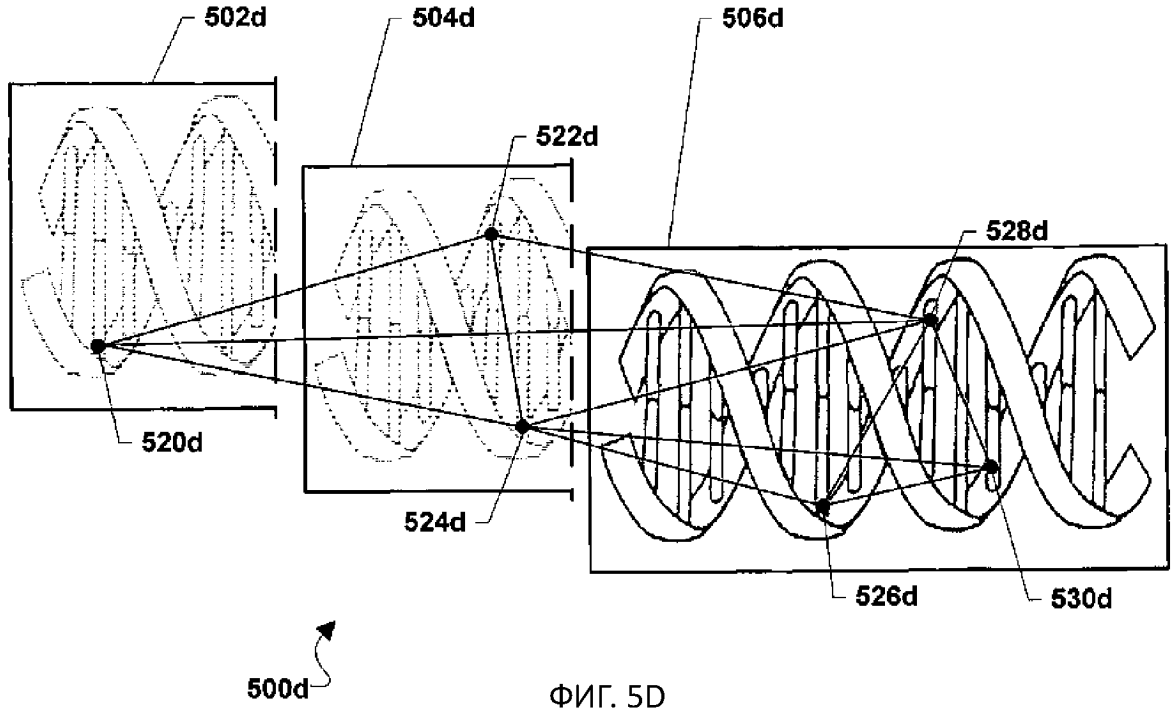
ФИГ. 5A


502b
504b
506b
522b
524b
526b
520b
528b
530b
500b

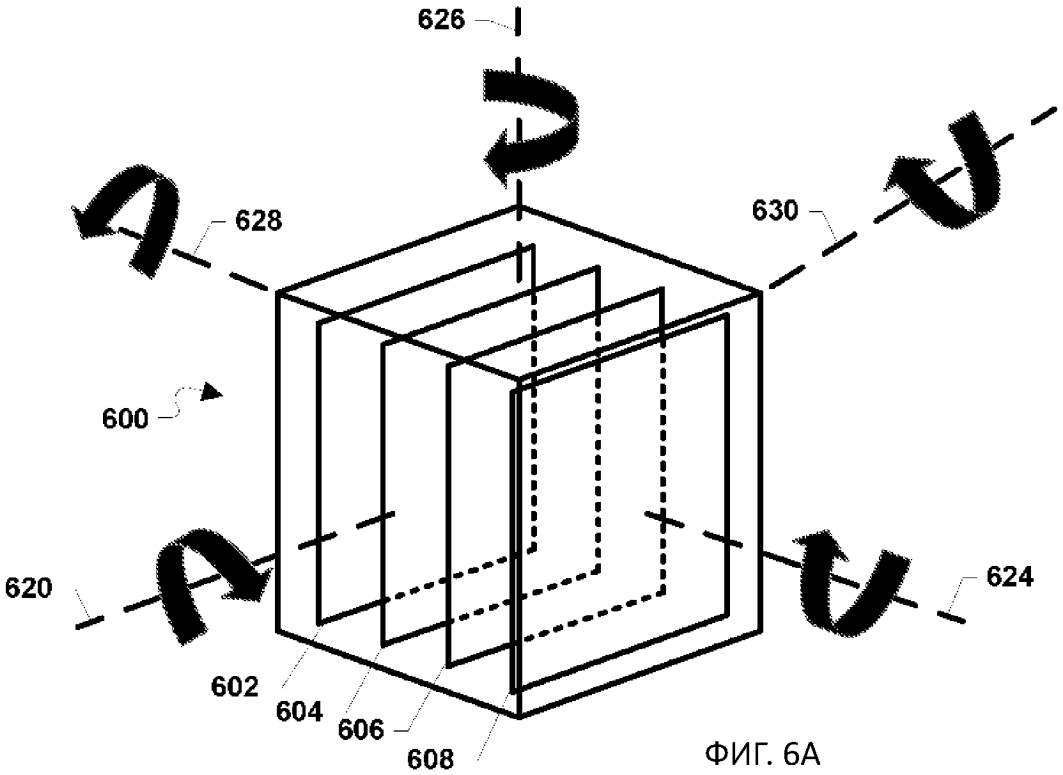
ФИГ. 5B


502c
504c
506c
528c
526c
522c
520c
534c
532c
524c
530c
536c
500c

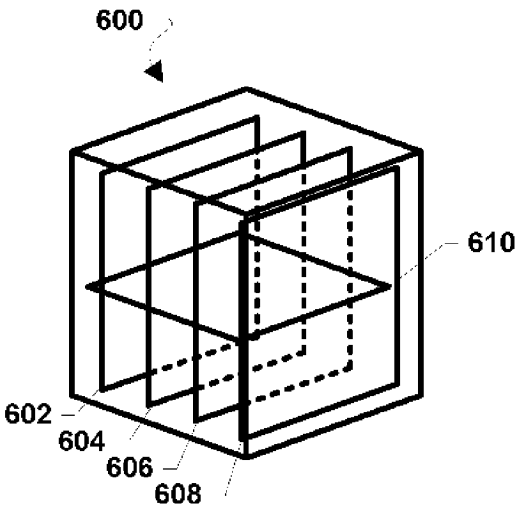
ФИГ. 5C


502d
504d
506d
522d
528d
520d
524d
526d
530d
500d

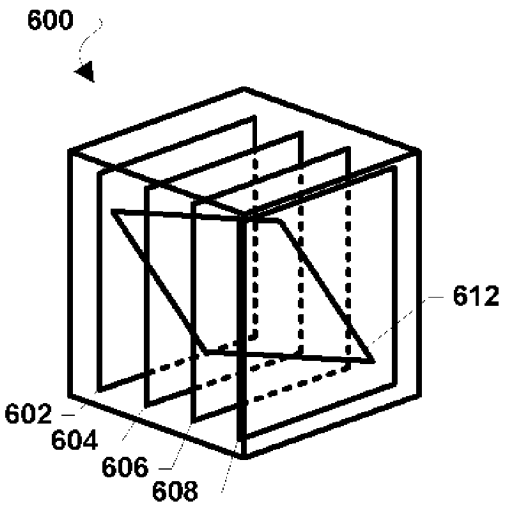
ФИГ. 5D



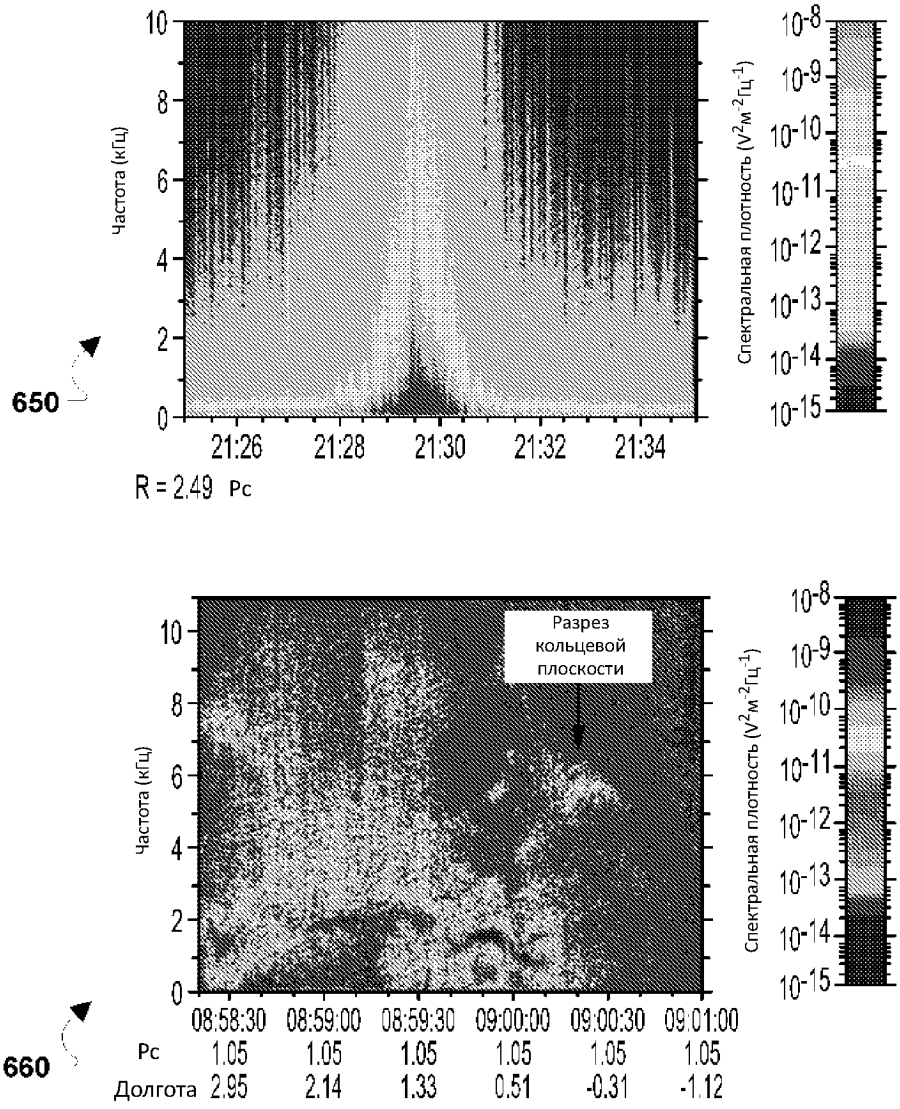
ФИГ. 6А



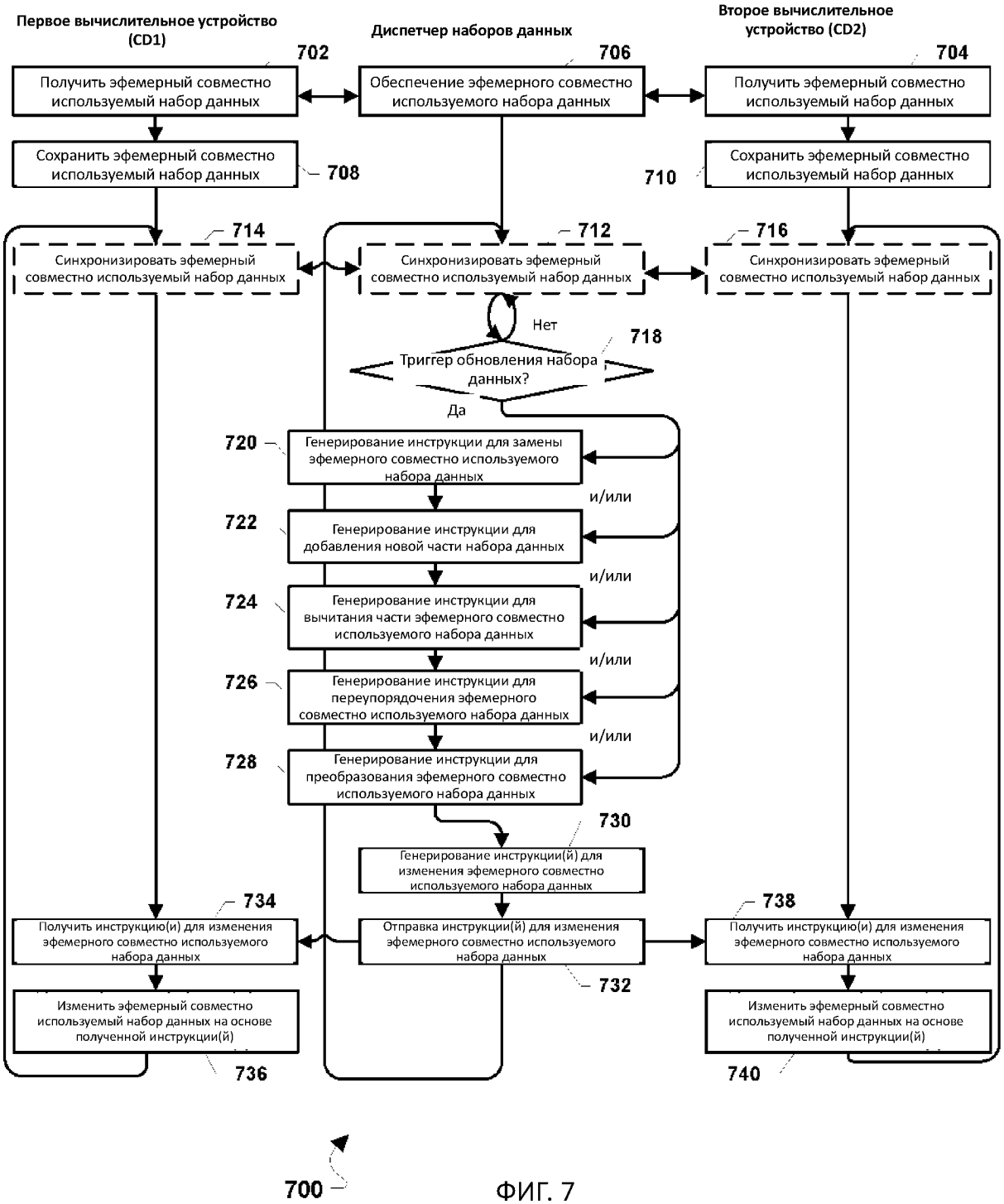
ФИГ. 6В



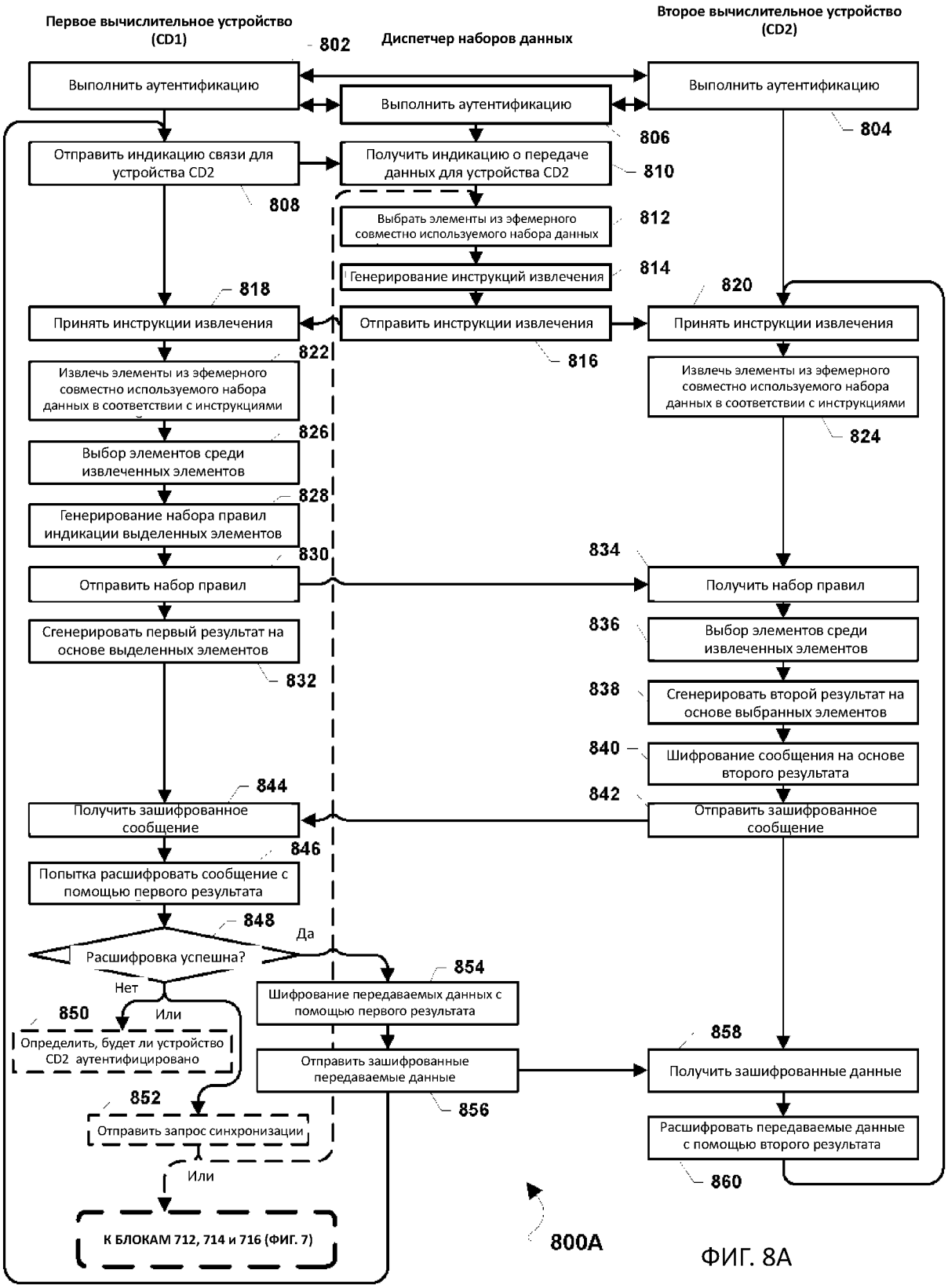
ФИГ. 6С


650
Частота (кГц)
10
8
6
4
2
0
21:26
21:28
21:30
21:32
21:34
R = 2.49 Pc
Спектральная плотность (V²м⁻²Гц⁻¹)
10⁻⁸
10⁻⁹
10⁻¹⁰
10⁻¹¹
10⁻¹²
10⁻¹³
10⁻¹⁴
10⁻¹⁵
660
Разрез кольцевой плоскости
Частота (кГц)
08:58:30
08:59:00
08:59:30
09:00:00
09:00:30
09:01:00
Pc 1.05 1.05 1.05 1.05 1.05 1.05
Долгота 2.95 2.14 1.33 0.51 -0.31 -1.12
Спектральная плотность (V²м⁻²Гц⁻¹)

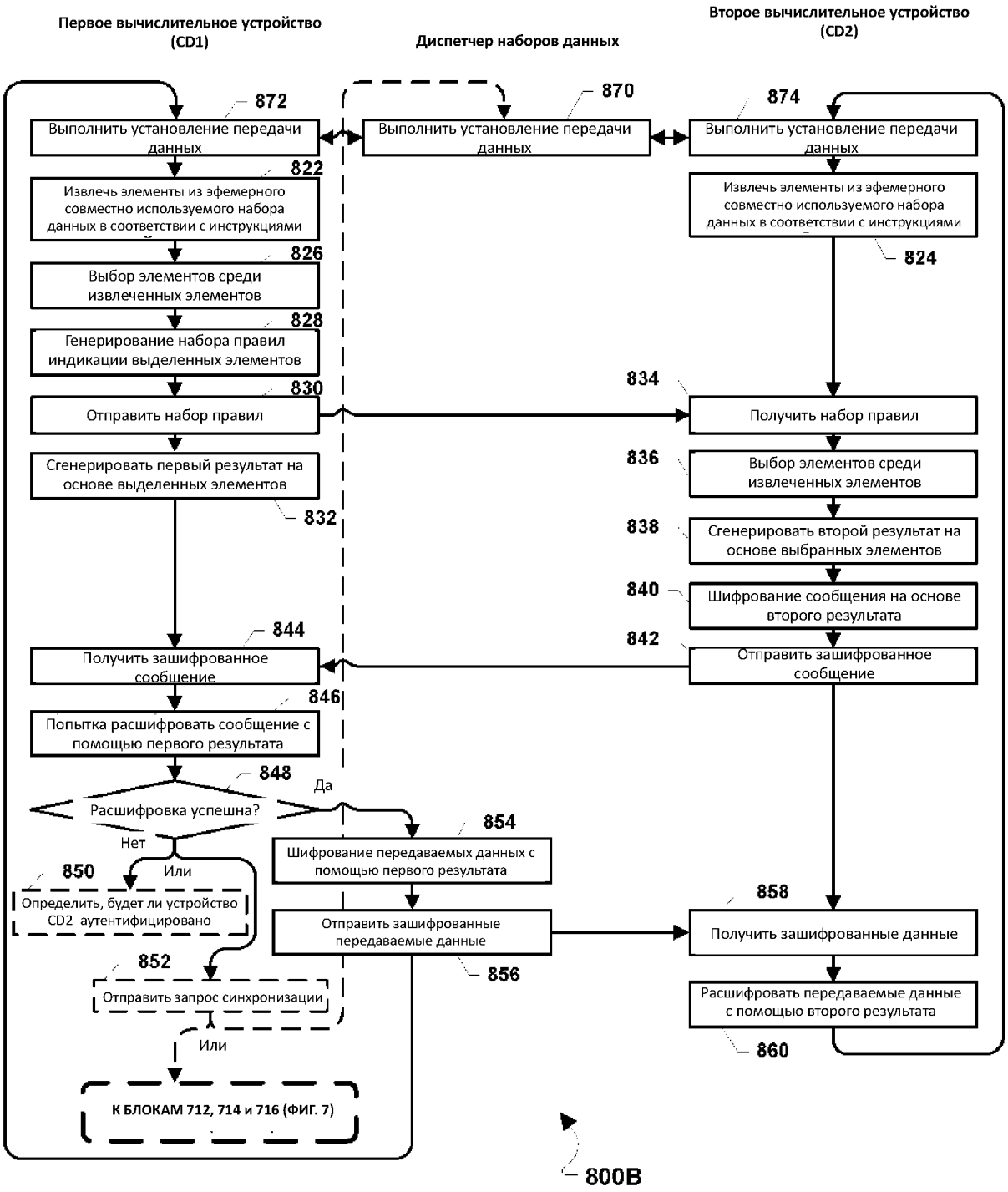
ФИГ. 6D


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
702
706
704
Получить эфемерный совместно используемый набор данных
Обеспечение эфемерного совместно используемого набора данных
Получить эфемерный совместно используемый набор данных
Сохранить эфемерный совместно используемый набор данных
708
710
Сохранить эфемерный совместно используемый набор данных
714
712
716
Синхронизировать эфемерный совместно используемый набор данных
Синхронизировать эфемерный совместно используемый набор данных
Синхронизировать эфемерный совместно используемый набор данных
Нет
718
Триггер обновления набора данных?
Да
720
Генерирование инструкции для замены эфемерного совместно используемого набора данных
и/или
722
Генерирование инструкции для добавления новой части набора данных
и/или
724
Генерирование инструкции для вычитания части эфемерного совместно используемого набора данных
и/или
726
Генерирование инструкции для переупорядочения эфемерного совместно используемого набора данных
и/или
728
Генерирование инструкции для преобразования эфемерного совместно используемого набора данных
730
Генерирование инструкции(й) для изменения эфемерного совместно используемого набора данных
734
738
Получить инструкцию(и) для изменения эфемерного совместно используемого набора данных
Отправка инструкции(й) для изменения эфемерного совместно используемого набора данных
Получить инструкцию(и) для изменения эфемерного совместно используемого набора данных
732
Изменить эфемерный совместно используемый набор данных на основе полученной инструкции(й)
Изменить эфемерный совместно используемый набор данных на основе полученной инструкции(й)
736
740
700

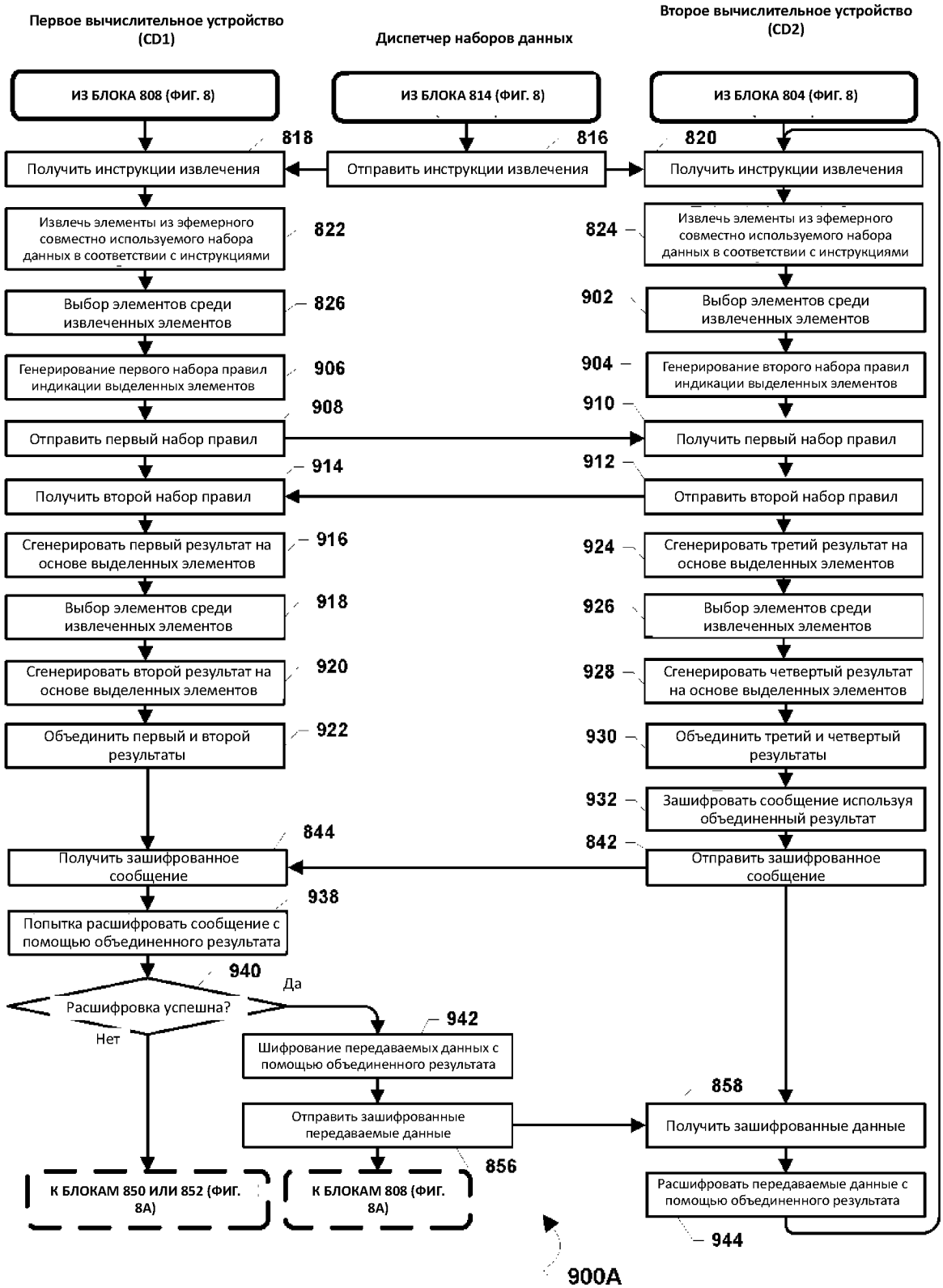
ФИГ. 7


Первое вычислительное устройство (CD1)
802
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
Выполнить аутентификацию
Выполнить аутентификацию
Выполнить аутентификацию
806
804
Отправить индикацию связи для устройства CD2
Получить индикацию о передаче данных для устройства CD2
810
808
Выбрать элементы из эфемерного совместно используемого набора данных
812
Генерирование инструкций извлечения
814
818
820
Принять инструкции извлечения
Отправить инструкции извлечения
Принять инструкции извлечения
816
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
834
830
Отправить набор правил
Получить набор правил
836
Сгенерировать первый результат на основе выделенных элементов
Выбор элементов среди извлеченных элементов
832
838
Сгенерировать второй результат на основе выбранных элементов
840
Шифрование сообщения на основе второго результата
842
844
Получить зашифрованное сообщение
Отправить зашифрованное сообщение
846
Попытка расшифровать сообщение с помощью первого результата
848
Да
Расшифровка успешна?
854
Нет
Шифрование передаваемых данных с помощью первого результата
850
Или
Определить, будет ли устройство CD2 аутентифицировано
858
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
852
856
Отправить запрос синхронизации
Расшифровать передаваемые данные с помощью второго результата
Или
860
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)
800A

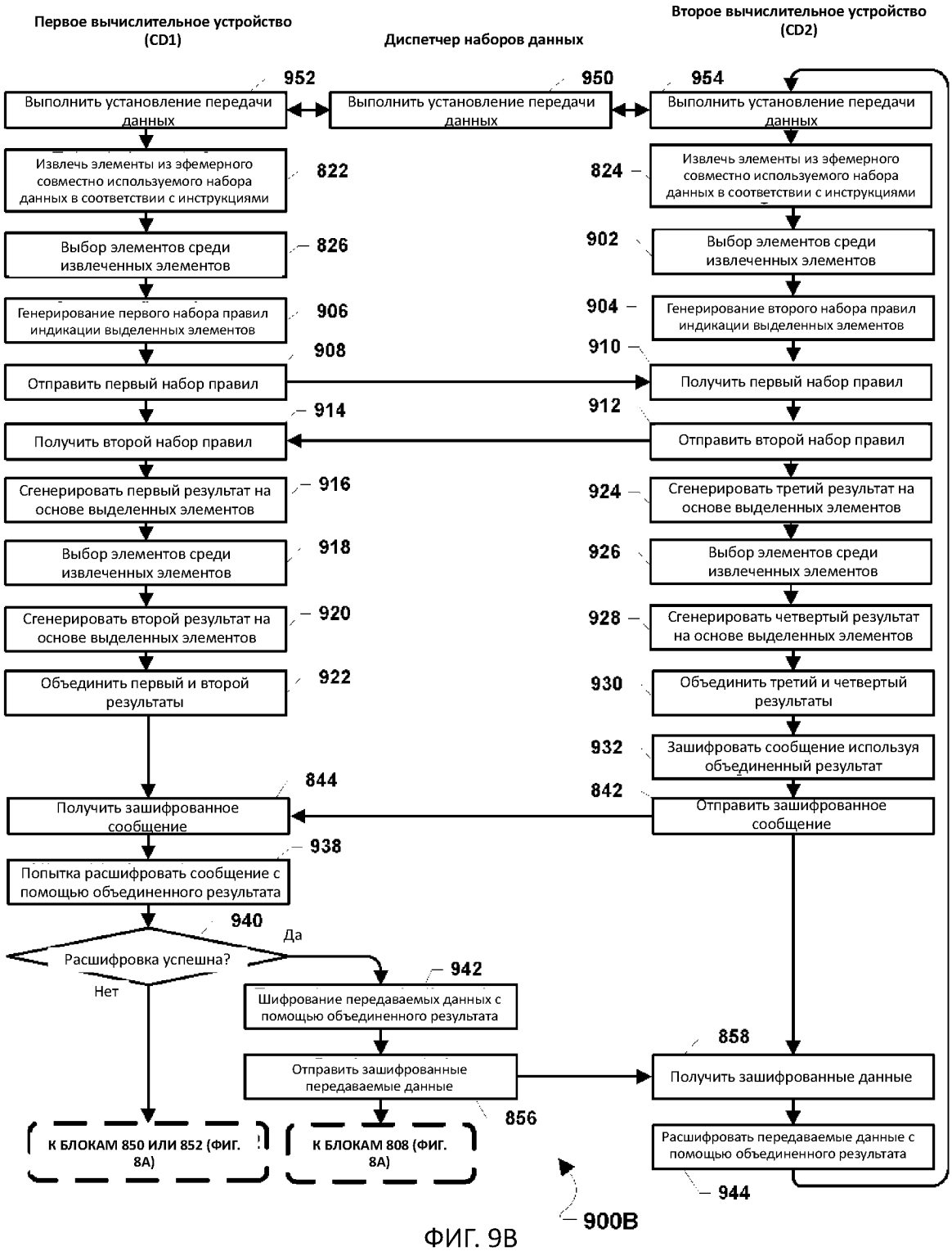
ФИГ. 8A


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
872
Выполнить установление передачи данных
870
Выполнить установление передачи данных
874
Выполнить установление передачи данных
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
830
Отправить набор правил
834
Получить набор правил
Сгенерировать первый результат на основе выделенных элементов
832
836
Выбор элементов среди извлеченных элементов
838
Сгенерировать второй результат на основе выбранных элементов
840
Шифрование сообщения на основе второго результата
842
Отправить зашифрованное сообщение
844
Получить зашифрованное сообщение
846
Попытка расшифровать сообщение с помощью первого результата
848
Расшифровка успешна?
Да
Нет
Или
854
Шифрование передаваемых данных с помощью первого результата
850
Определить, будет ли устройство CD2 аутентифицировано
Отправить зашифрованные передаваемые данные
858
Получить зашифрованные данные
856
852
Отправить запрос синхронизации
Расшифровать передаваемые данные с помощью второго результата
Или
860
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)
800B

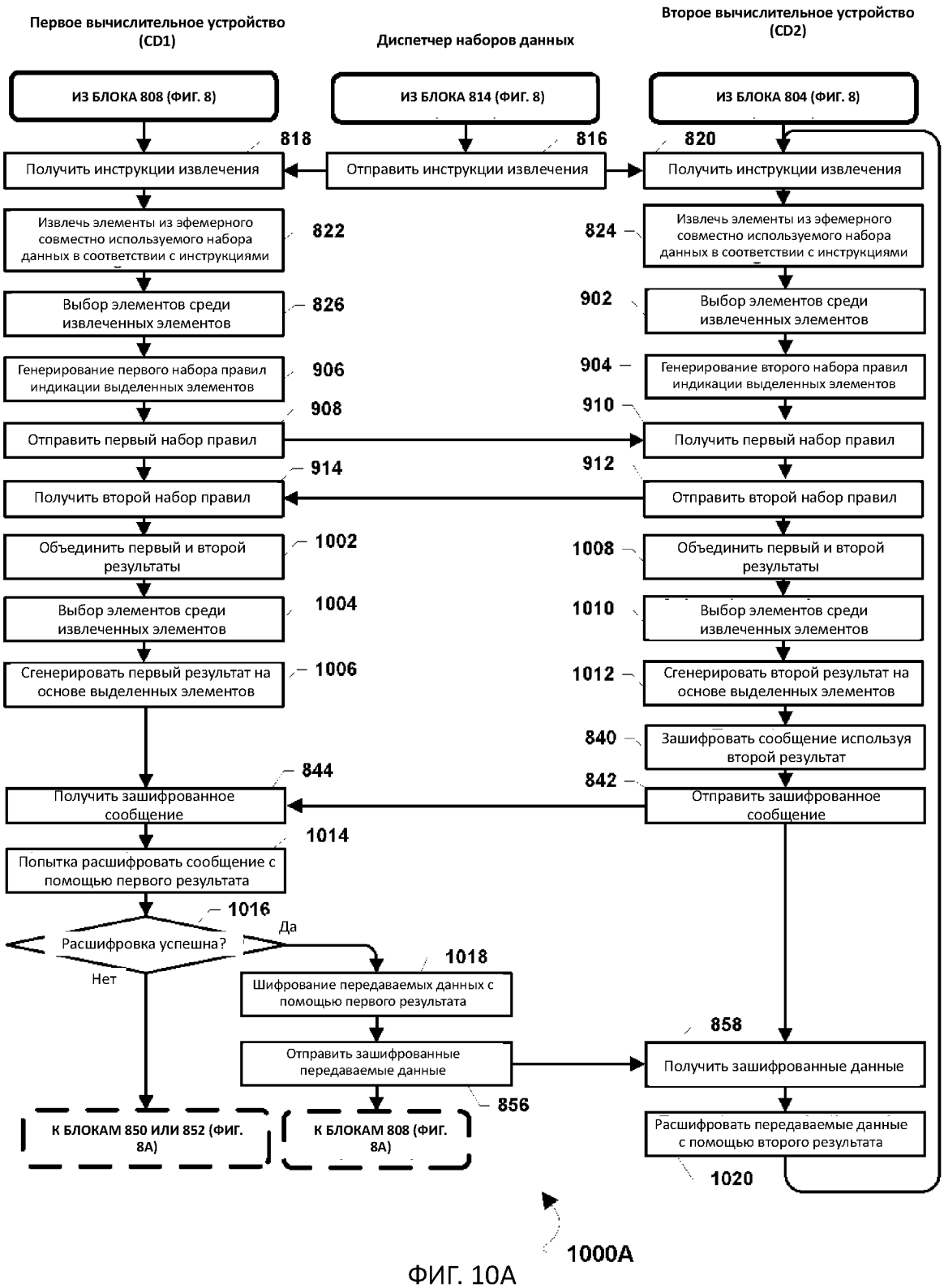
ФИГ. 8B


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
ИЗ БЛОКА 808 (ФИГ. 8)
ИЗ БЛОКА 814 (ФИГ. 8)
ИЗ БЛОКА 804 (ФИГ. 8)
818
816
820
Получить инструкции извлечения
Отправить инструкции извлечения
Получить инструкции извлечения
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
822
824
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Выбор элементов среди извлеченных элементов
826
902
Выбор элементов среди извлеченных элементов
Генерирование первого набора правил индикации выделенных элементов
906
904
Генерирование второго набора правил индикации выделенных элементов
908
910
Отправить первый набор правил
Получить первый набор правил
914
912
Получить второй набор правил
Отправить второй набор правил
Сгенерировать первый результат на основе выделенных элементов
916
924
Сгенерировать третий результат на основе выделенных элементов
Выбор элементов среди извлеченных элементов
918
926
Выбор элементов среди извлеченных элементов
Сгенерировать второй результат на основе выделенных элементов
920
928
Сгенерировать четвертый результат на основе выделенных элементов
Объединить первый и второй результаты
922
930
Объединить третий и четвертый результаты
932
Зашифровать сообщение используя объединенный результат
844
842
Получить зашифрованное сообщение
Отправить зашифрованное сообщение
938
Попытка расшифровать сообщение с помощью объединенного результата
940
Да
Расшифровка успешна?
Нет
942
Шифрование передаваемых данных с помощью объединенного результата
858
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
856
К БЛОКАМ 850 ИЛИ 852 (ФИГ. 8А)
К БЛОКАМ 808 (ФИГ. 8А)
Расшифровать передаваемые данные с помощью объединенного результата
944
900A

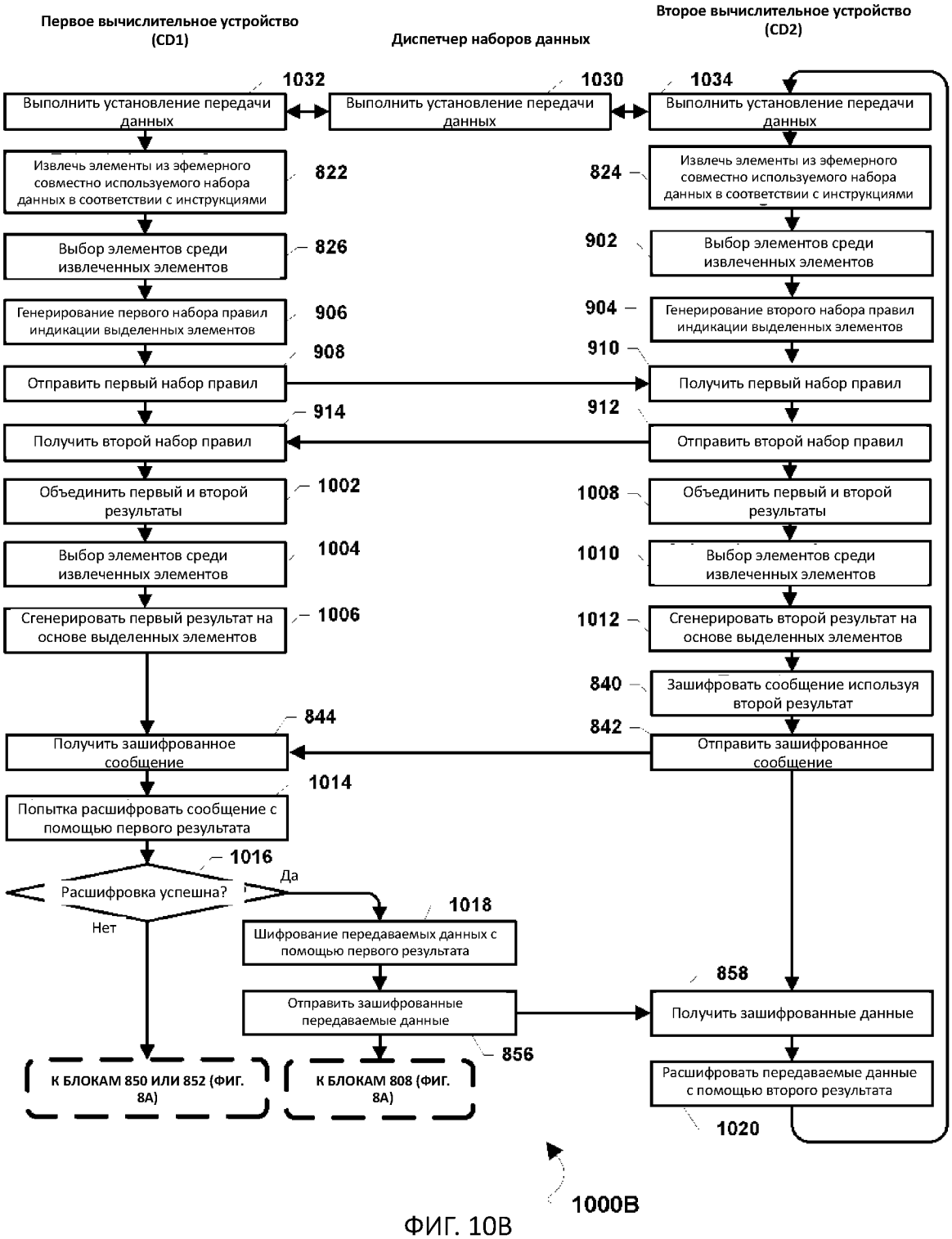
ФИГ. 9А


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
952
Выполнить установление передачи данных
950
Выполнить установление передачи данных
954
Выполнить установление передачи данных
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
822
824
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Выбор элементов среди извлеченных элементов
826
902
Выбор элементов среди извлеченных элементов
Генерирование первого набора правил индикации выделенных элементов
906
904
Генерирование второго набора правил индикации выделенных элементов
908
910
Отправить первый набор правил
Получить первый набор правил
914
912
Получить второй набор правил
Отправить второй набор правил
Сгенерировать первый результат на основе выделенных элементов
916
924
Сгенерировать третий результат на основе выделенных элементов
Выбор элементов среди извлеченных элементов
918
926
Выбор элементов среди извлеченных элементов
Сгенерировать второй результат на основе выделенных элементов
920
928
Сгенерировать четвертый результат на основе выделенных элементов
Объединить первый и второй результаты
922
930
Объединить третий и четвертый результаты
932
Зашифровать сообщение используя объединенный результат
844
842
Получить зашифрованное сообщение
Отправить зашифрованное сообщение
938
Попытка расшифровать сообщение с помощью объединенного результата
940
Да
Расшифровка успешна?
Нет
942
Шифрование передаваемых данных с помощью объединенного результата
858
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
856
К БЛОКАМ 850 ИЛИ 852 (ФИГ. 8A)
К БЛОКАМ 808 (ФИГ. 8A)
Расшифровать передаваемые данные с помощью объединенного результата
944
900B

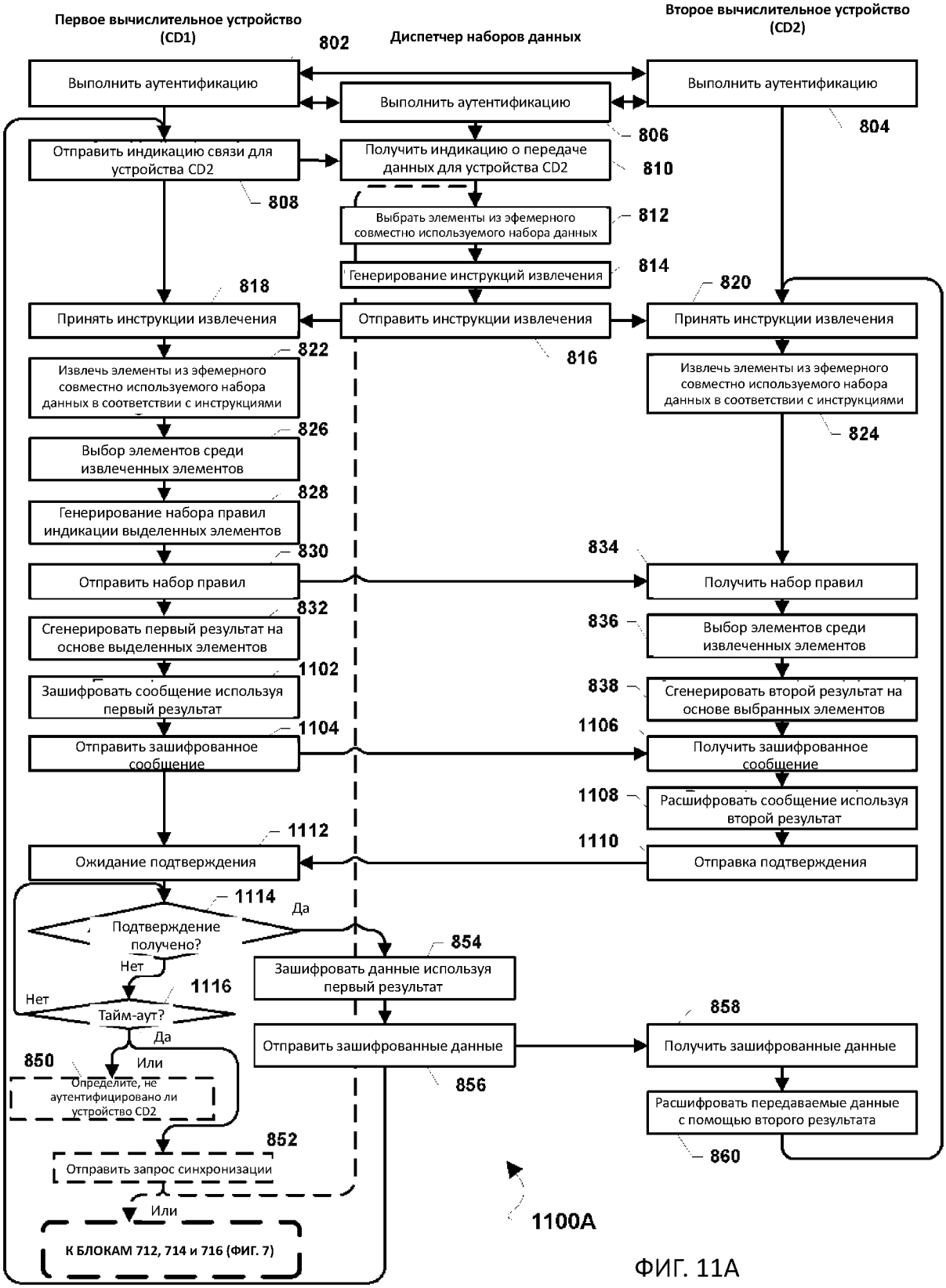
ФИГ. 9B


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
ИЗ БЛОКА 808 (ФИГ. 8)
ИЗ БЛОКА 814 (ФИГ. 8)
ИЗ БЛОКА 804 (ФИГ. 8)
818
816
820
Получить инструкции извлечения
Отправить инструкции извлечения
Получить инструкции извлечения
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
822
824
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Выбор элементов среди извлеченных элементов
826
902
Выбор элементов среди извлеченных элементов
Генерирование первого набора правил индикации выделенных элементов
906
904
Генерирование второго набора правил индикации выделенных элементов
908
910
Отправить первый набор правил
Получить первый набор правил
914
912
Получить второй набор правил
Отправить второй набор правил
Объединить первый и второй результаты
1002
1008
Объединить первый и второй результаты
Выбор элементов среди извлеченных элементов
1004
1010
Выбор элементов среди извлеченных элементов
Сгенерировать первый результат на основе выделенных элементов
1006
1012
Сгенерировать второй результат на основе выделенных элементов
840
Зашифровать сообщение используя второй результат
844
842
Получить зашифрованное сообщение
Отправить зашифрованное сообщение
1014
Попытка расшифровать сообщение с помощью первого результата
1016
Расшифровка успешна?
Да
Нет
1018
Шифрование передаваемых данных с помощью первого результата
858
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
856
К БЛОКАМ 850 ИЛИ 852 (ФИГ. 8А)
К БЛОКАМ 808 (ФИГ. 8А)
Расшифровать передаваемые данные с помощью второго результата
1020
1000A

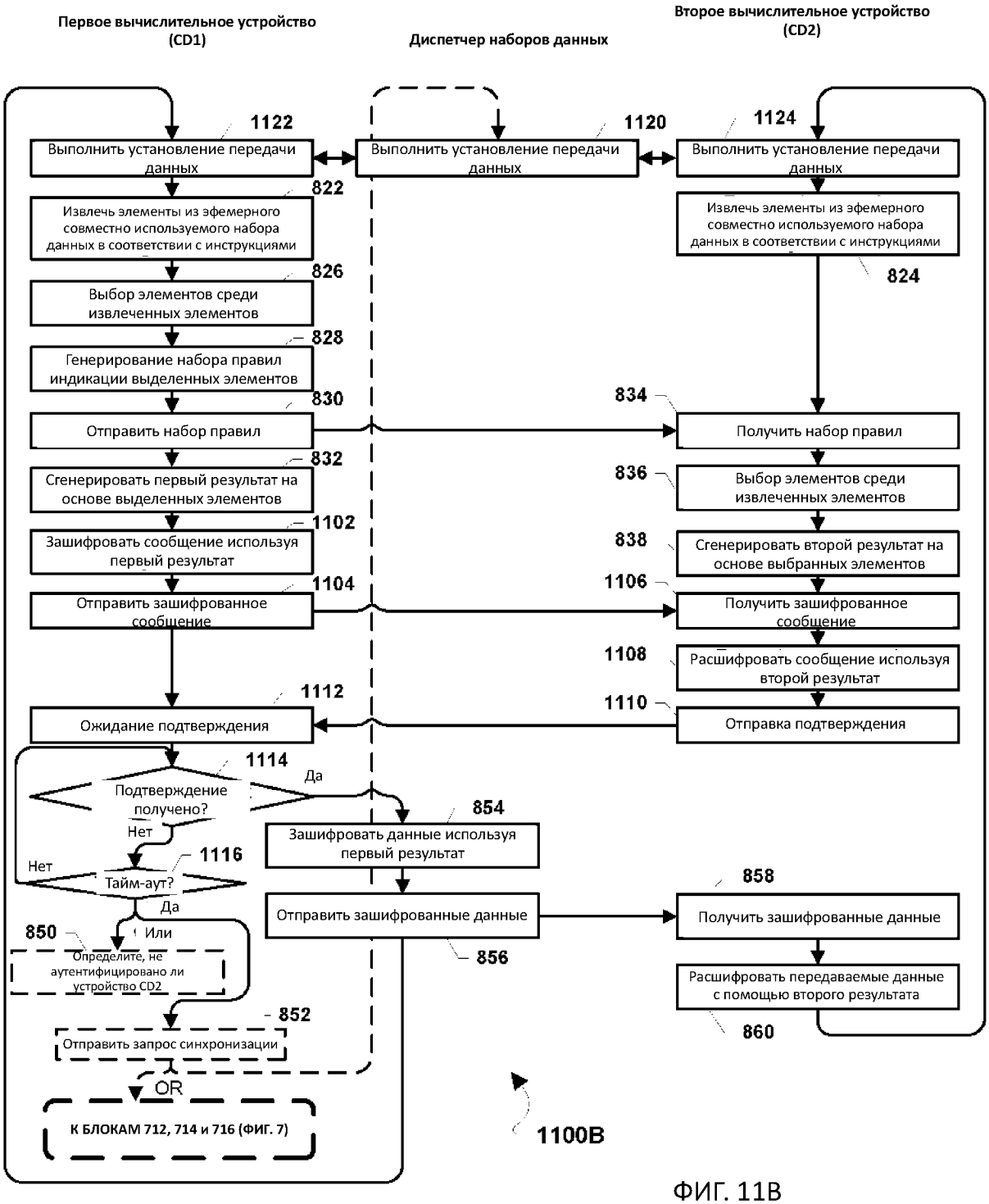
ФИГ. 10А


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
1032
1030
1034
Выполнить установление передачи данных
Выполнить установление передачи данных
Выполнить установление передачи данных
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
822
824
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Выбор элементов среди извлеченных элементов
826
902
Выбор элементов среди извлеченных элементов
Генерирование первого набора правил индикации выделенных элементов
906
904
Генерирование второго набора правил индикации выделенных элементов
908
910
Отправить первый набор правил
Получить первый набор правил
914
912
Получить второй набор правил
Отправить второй набор правил
Объединить первый и второй результаты
1002
1008
Объединить первый и второй результаты
Выбор элементов среди извлеченных элементов
1004
1010
Выбор элементов среди извлеченных элементов
Сгенерировать первый результат на основе выделенных элементов
1006
1012
Сгенерировать второй результат на основе выделенных элементов
840
Зашифровать сообщение используя второй результат
844
842
Получить зашифрованное сообщение
Отправить зашифрованное сообщение
1014
Попытка расшифровать сообщение с помощью первого результата
1016
Расшифровка успешна?
Да
Нет
1018
Шифрование передаваемых данных с помощью первого результата
858
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
856
К БЛОКАМ 850 ИЛИ 852 (ФИГ. 8А)
К БЛОКАМ 808 (ФИГ. 8А)
Расшифровать передаваемые данные с помощью второго результата
1020
1000B

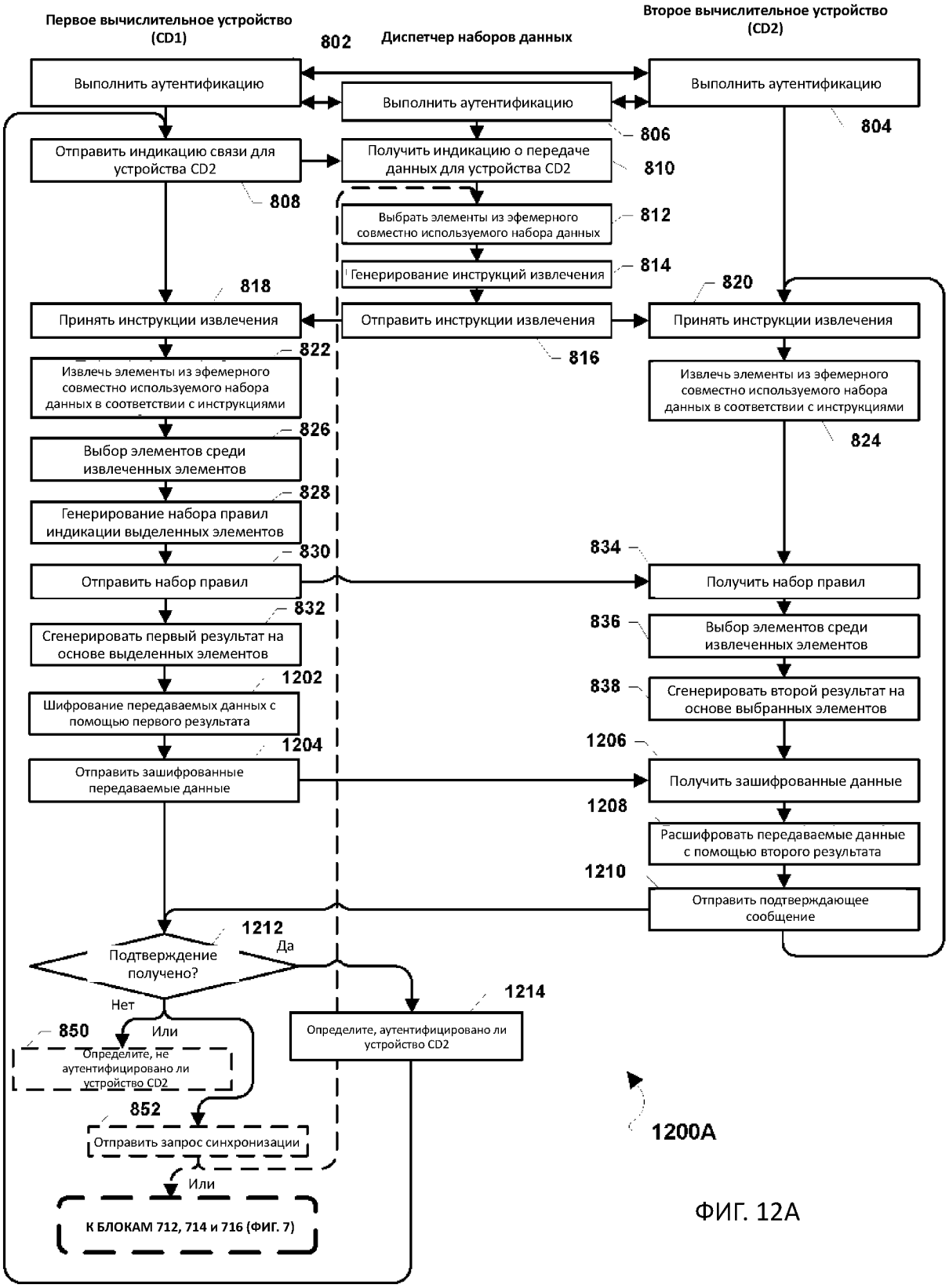
ФИГ. 10B


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
802
Выполнить аутентификацию
Выполнить аутентификацию
Выполнить аутентификацию
804
806
Отправить индикацию связи для устройства CD2
Получить индикацию о передаче данных для устройства CD2
810
808
Выбрать элементы из эфемерного совместно используемого набора данных
812
Генерирование инструкций извлечения
814
818
820
Принять инструкции извлечения
Отправить инструкции извлечения
Принять инструкции извлечения
816
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
830
834
Отправить набор правил
Получить набор правил
832
836
Сгенерировать первый результат на основе выделенных элементов
Выбор элементов среди извлеченных элементов
1102
838
Зашифровать сообщение используя первый результат
Сгенерировать второй результат на основе выбранных элементов
1104
1106
Отправить зашифрованное сообщение
Получить зашифрованное сообщение
1108
Расшифровать сообщение используя второй результат
1112
1110
Ожидание подтверждения
Отправка подтверждения
1114
Да
Подтверждение получено?
854
Нет
Зашифровать данные используя первый результат
1116
Нет
Тайм-аут?
858
Да
Отправить зашифрованные данные
Получить зашифрованные данные
850
Или
Определите, не аутентифицировано ли устройство CD2
856
Расшифровать передаваемые данные с помощью второго результата
852
Отправить запрос синхронизации
860
Или
1100A
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)

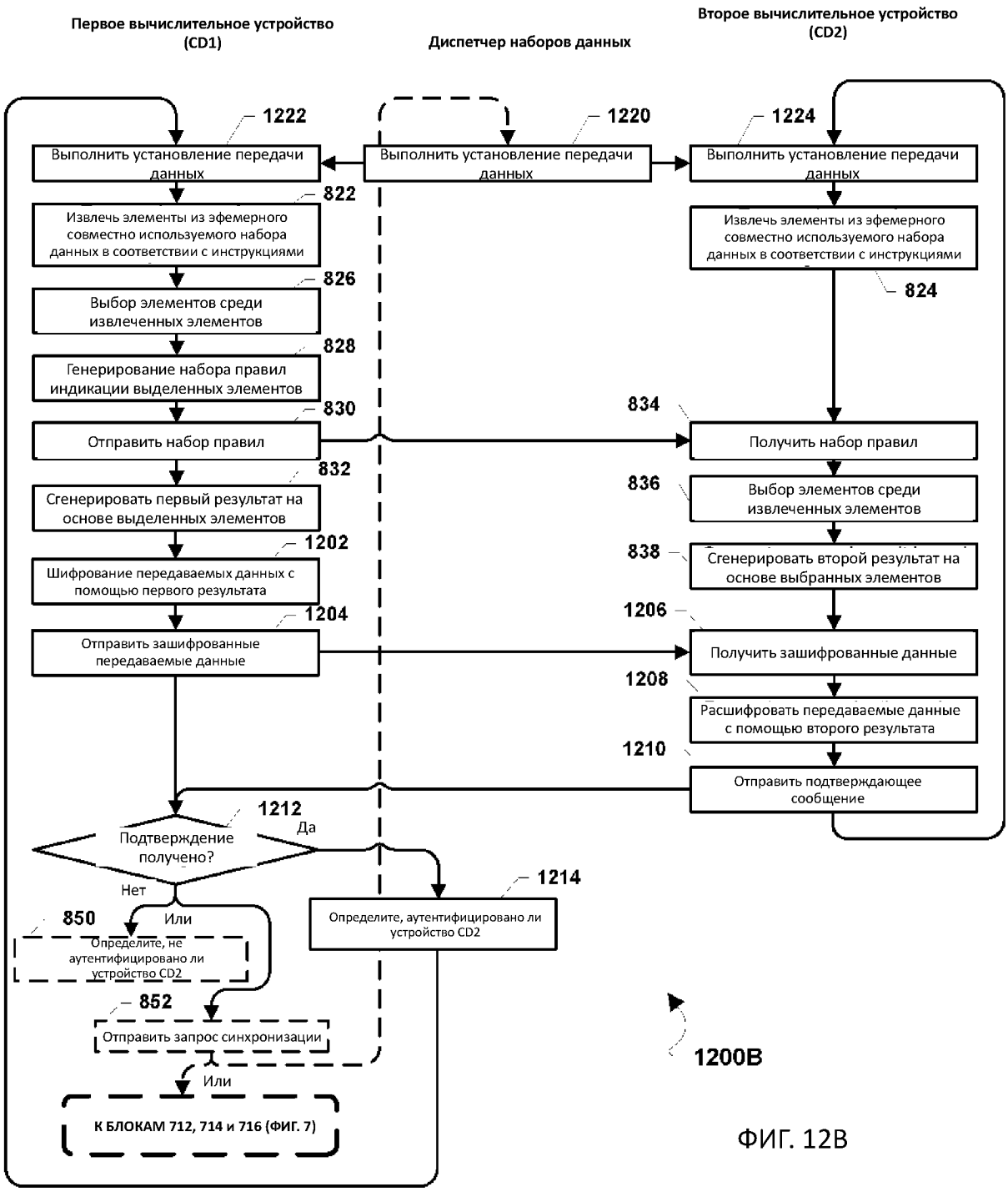
ФИГ. 11A


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
1122
Выполнить установление передачи данных
1120
Выполнить установление передачи данных
1124
Выполнить установление передачи данных
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
830
Отправить набор правил
834
Получить набор правил
832
Сгенерировать первый результат на основе выделенных элементов
836
Выбор элементов среди извлеченных элементов
1102
Зашифровать сообщение используя первый результат
838
Сгенерировать второй результат на основе выбранных элементов
1104
Отправить зашифрованное сообщение
1106
Получить зашифрованное сообщение
1108
Расшифровать сообщение используя второй результат
1112
Ожидание подтверждения
1110
Отправка подтверждения
1114
Подтверждение получено?
Да
Нет
854
Зашифровать данные используя первый результат
Нет
1116
Тайм-аут?
Да
858
Отправить зашифрованные данные
Получить зашифрованные данные
850
Или
Определите, не аутентифицировано ли устройство CD2
856
Расшифровать передаваемые данные с помощью второго результата
852
Отправить запрос синхронизации
860
OR
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)
1100B

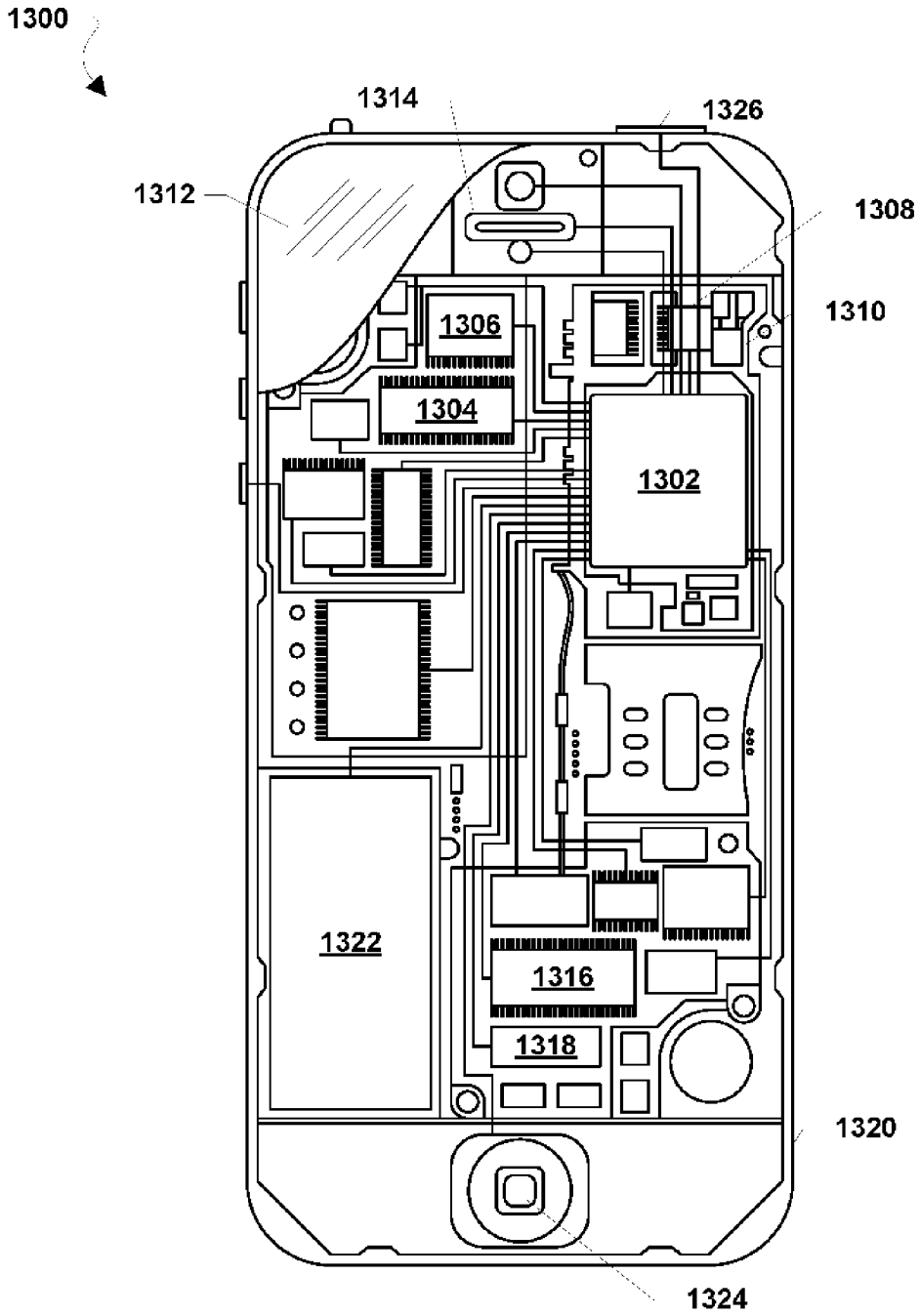
ФИГ. 11B


Первое вычислительное устройство (CD1)
802
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
Выполнить аутентификацию
Выполнить аутентификацию
Выполнить аутентификацию
804
806
Отправить индикацию связи для устройства CD2
Получить индикацию о передаче данных для устройства CD2
810
808
Выбрать элементы из эфемерного совместно используемого набора данных
812
Генерирование инструкций извлечения
814
818
820
Принять инструкции извлечения
Отправить инструкции извлечения
Принять инструкции извлечения
816
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
834
830
Отправить набор правил
Получить набор правил
832
836
Выбор элементов среди извлеченных элементов
Сгенерировать первый результат на основе выделенных элементов
838
Сгенерировать второй результат на основе выбранных элементов
1202
Шифрование передаваемых данных с помощью первого результата
1206
1204
Отправить зашифрованные передаваемые данные
Получить зашифрованные данные
1208
Расшифровать передаваемые данные с помощью второго результата
1210
Отправить подтверждающее сообщение
1212
Подтверждение получено?
Да
Нет
1214
Или
850
Определите, не аутентифицировано ли устройство CD2
Определите, аутентифицировано ли устройство CD2
852
Отправить запрос синхронизации
Или
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)
1200A

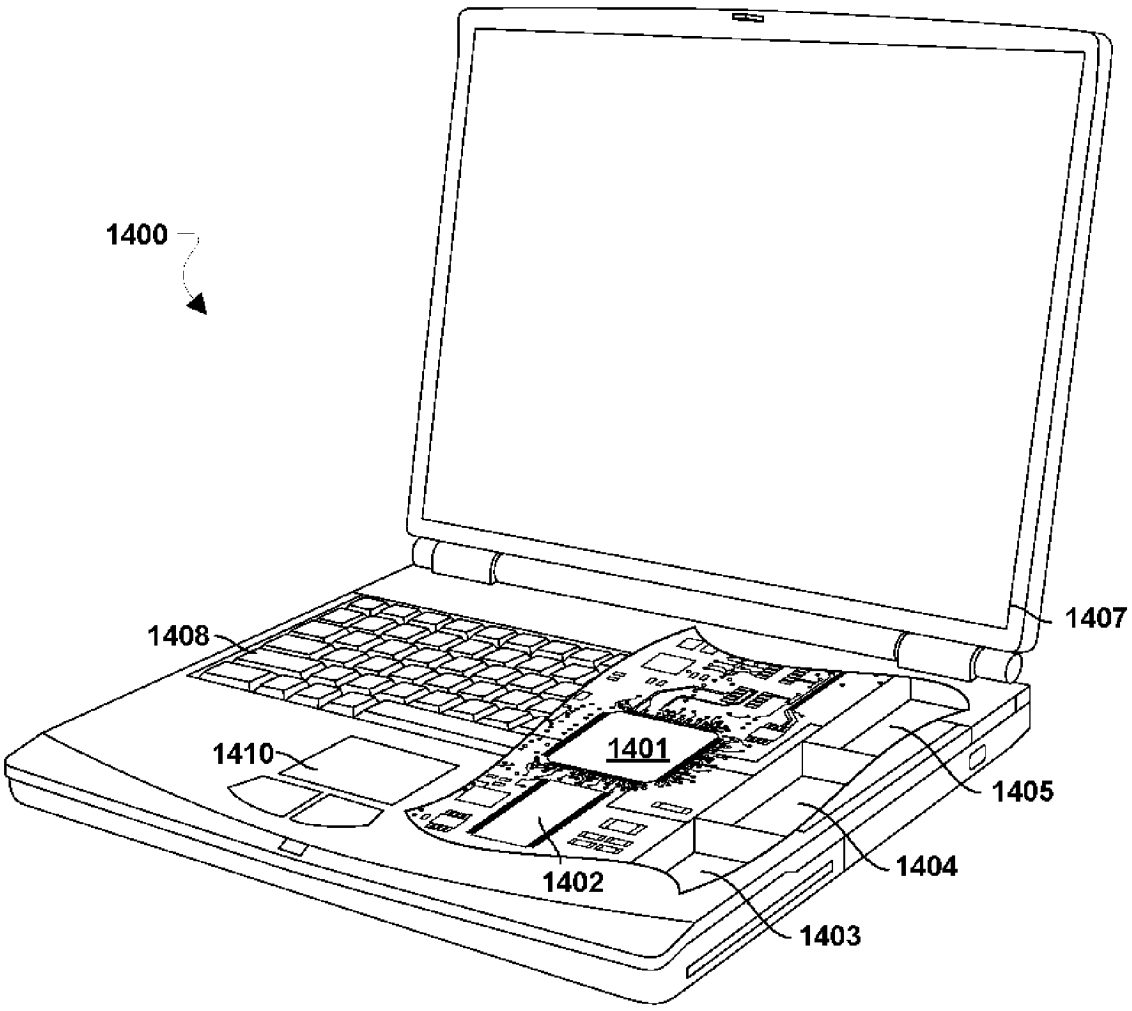
ФИГ. 12A


Первое вычислительное устройство (CD1)
Диспетчер наборов данных
Второе вычислительное устройство (CD2)
1222
Выполнить установление передачи данных
1220
Выполнить установление передачи данных
1224
Выполнить установление передачи данных
822
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
Извлечь элементы из эфемерного совместно используемого набора данных в соответствии с инструкциями
824
826
Выбор элементов среди извлеченных элементов
828
Генерирование набора правил индикации выделенных элементов
830
Отправить набор правил
834
Получить набор правил
832
Сгенерировать первый результат на основе выделенных элементов
836
Выбор элементов среди извлеченных элементов
1202
Шифрование передаваемых данных с помощью первого результата
838
Сгенерировать второй результат на основе выбранных элементов
1204
Отправить зашифрованные передаваемые данные
1206
Получить зашифрованные данные
1208
Расшифровать передаваемые данные с помощью второго результата
1210
Отправить подтверждающее сообщение
1212
Подтверждение получено?
Да
Нет
1214
Определите, аутентифицировано ли устройство CD2
850
Или
Определите, не аутентифицировано ли устройство CD2
852
Отправить запрос синхронизации
Или
К БЛОКАМ 712, 714 и 716 (ФИГ. 7)
1200B

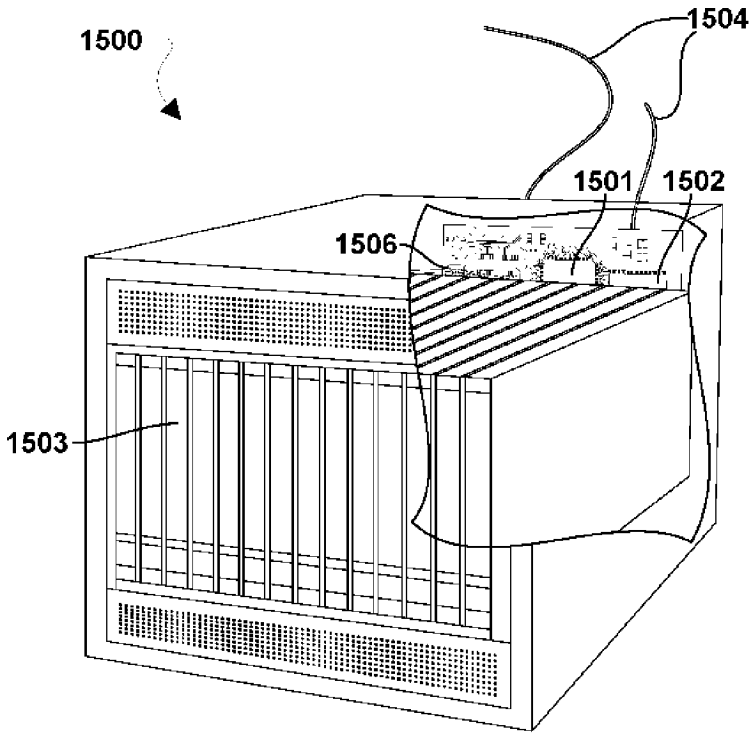
ФИГ. 12B


1300
1314
1326
1312
1308
1310
1306
1304
1302
1322
1316
1318
1320
1324

ФИГ. 13



ФИГ. 14



ФИГ. 15