(19) Евразийское патентное ведомство

(21) 202390945 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2023.07.18

(22) Дата подачи заявки
2021.09.22

(51) Int. Cl. ***H04L 29/06*** (2006.01)
H04W 12/64 (2021.01)

(54) УПРАВЛЕНИЕ ЗАШИФРОВАННЫМИ ФАЙЛАМИ

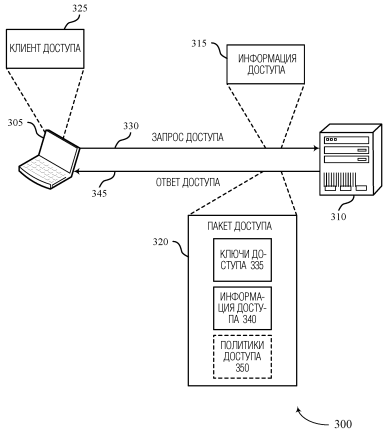
(31) **63/081,763; 17/482,010**
(32) **2020.09.22; 2021.09.22**
(33) **US**
(86) **PCT/US2021/051562**
(87) **WO 2022/066775 2022.03.31**

(71) Заявитель:
КИАВИ ДЭЙТА КОРП. (US)

(72) Изобретатель:
Ниджасуре Прашант Шрипад, Льюис Эллиот Дэниел (US)

(74) Представитель:
Медведев В.Н. (RU)

(57) Клиент доступа может передавать запрос доступа на сервер, и запрос доступа может быть примером запроса дешифрования или запроса шифрования. Запрос доступа может включать в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Сервер может валидировать информацию доступа и генерировать пакет доступа, который включает в себя набор ключей доступа и исполняемый код. Ключи доступа могут передаваться на клиент доступа. Клиент доступа может исполнять исполняемый код и дешифровать или шифровать файл. Файл может включать в себя один или более пакетов данных, которые включают в себя политики доступа к файлу, информацию о владении и логи доступа к файлам.



202390945 A1

202390945 A1

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

2420-577844EA/030

УПРАВЛЕНИЕ ЗАШИФРОВАННЫМИ ФАЙЛАМИ

Перекрестная ссылка

[0001] Настоящая заявка на патент испрашивает приоритет патентной заявки США № 17/482,010 на имя NIJASURE et al., озаглавленной "ENCRYPTED FILE CONTROL", поданной 22 сентября 2021, и предварительной патентной заявки США № 63/081,763 на имя NIJASURE et al., озаглавленной "ENCRYPTED FILE CONTROL", поданной 22 сентября 2020, каждая из которых переуступлена правообладателю настоящей заявки и каждая из которых явным образом включена в настоящий документ посредством ссылки во всей своей полноте.

ОБЛАСТЬ ТЕХНИКИ

[0002] Настоящее раскрытие в целом относится к защите данных и, более конкретно, к управлению зашифрованными файлами.

УРОВЕНЬ ТЕХНИКИ

[0003] Шифрование файлов позволяет совместно использовать файлы между компьютерами по незащищенным сетям и может предотвращать доступ третьих сторон к конфиденциальным данным. Однако шифрование файлов может быть настолько безопасным, насколько безопасны ключи, используемые для шифрования файлов.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0004] Описанные способы относятся к усовершенствованным способам, системам, устройствам и аппаратным компонентам, которые поддерживают управление зашифрованными файлами. Как правило, описанные методы обеспечивают совместное использование зашифрованных файлов без ущерба для ключей шифрования, используемых для шифрования файлов. Полезные нагрузки зашифрованных файлов ‘солят’ (модифицируют строками случайных чисел (‘солями’)) и шифруют несколькими солями и ключами, хранящимися во множестве хранилищ. В ответ на запрос доступа, чтобы шифровать или дешифровать файл, сервер генерирует пакет доступа, который включает в себя информацию (например, данные и/или код) для выполнения доступа. Например, если пакет данных включает исходный код, исходный код может быть закачан с солями и ключами, используемыми, чтобы шифровать или дешифровать полезные нагрузки зашифрованных файлов. Сервер отправляет ответ доступа с пакетом доступа на устройство доступа, которое послало запрос доступа на сервер. Устройство доступа может компилировать исходный код из пакета доступа для генерирования исполняемого кода, который может шифровать или дешифровать полезные нагрузки зашифрованных файлов. В некоторых случаях, устройство доступа может преобразовывать данные полезной нагрузки на основе данных, включенных в пакет доступа. После использования, исполняемые коды и/или пакеты доступа могут быть удалены из устройства доступа для минимизации времени, в течение которого соли и ключи находятся в памяти устройства доступа. Исключение хранения солей и ключей на устройстве доступа уменьшает влияние

и вероятность того, что устройство доступа будет скомпрометировано.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0005] Фиг. 1 иллюстрирует пример системы, которая поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0006] Фиг. 2 иллюстрирует пример зашифрованного файла, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия.

[0007] Фиг. 3 иллюстрирует пример вычислительной архитектуры, которая поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0008] Фиг. 4 иллюстрирует пример потока процесса, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия.

[0009] Фиг. 5 иллюстрирует пример потока процесса, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия.

[0010] Фиг. 6 иллюстрирует пример сценария устройства доступа, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия.

[0011] Фиг. 7 показывает блок-схему пользовательского устройства, которое поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0012] Фиг. 8 показывает схему системы, включающей в себя устройство, которое поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0013] Фиг. 9 показывает блок-схему компонента защиты данных, который поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0014] Фиг. 10 показывает схему системы, включающей в себя устройство, которое поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

[0015] Фиг. 11-23 показывают блок-схемы последовательностей операций, иллюстрирующие способы, которые поддерживают управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия.

ПОДРОБНОЕ ОПИСАНИЕ

[0016] Методы шифрования используются во множестве сред для защиты данных от неавторизованного доступа. Различные формы криптографических ключей могут использоваться для шифрования данных, дешифрования данных, безопасной передачи данных и тому подобного. Однако эти методы требуют, чтобы пользователи и системы поддерживали управление, герметизацию и видимость ключей и данных для защиты данных. Например, организации реализуют методы и системы управления устройствами, методы и системы управления идентичностями (идентификаторами), методы и системы управления хранением, технологии и системы облачной локализации, методы и системы

классификации данных, среди других методов и систем, для защиты данных. Вследствие сложностей этих систем и методов, а также количественного роста злоумышленников, потери данных и неавторизованный доступ к данным широко распространены.

[0017] Варианты осуществления, описанные в настоящем документе, поддерживают системы и методы для самозащиты, самоанализа и саморазвития данных. Описанные реализации поддерживают клиент доступа, который сконфигурирован, чтобы взаимодействовать с сервером, чтобы защищать данные с использованием способов, описанных в настоящем документе. Методы поддерживают мгновенное и динамическое управление данными. Например, если первый пользователь передал зашифрованный файл к второму пользователю, и первый пользователь больше не хочет, чтобы второй пользователь имел доступ к файлу. Первый пользователь может получать доступ к платформе для ограничения доступа второго пользователя к файлу в почти реальном времени, даже если второй пользователь уже имеет файл на своем устройстве. Эти методы поддерживаются на различных уровнях гранулярности, включая на уровне файла, групп файлов или папок файлов, на уровнях команды, уровнях организации и т.д. Кроме того, эти методы могут быть применимы к различным элементам или частям в файле. Например, файл может включать в себя один или более объектов данных (например, объектов технологии связывания и внедрения объектов (OLE), изображений), и эти объекты могут быть зашифрованы и дешифрованы (отдельно от самого файла) при применении различных методов политик доступа к файлу, описанных в настоящем документе. Кроме того, описанные методы поддерживают ограничения или политики доступа к файлу с использованием различных соображений, таких как географические местоположения, типы устройств и периоды времени, среди прочих ограничений. Например, пользователь может ограничивать доступ к файлу или группе файлов другими пользователями, которые находятся в определенной стране. Эти ограничения могут быть реализованы в почти реальном времени, даже если другие пользователи уже имеют файл на своих персональных устройствах в конкретной стране.

[0018] Чтобы поддерживать эти различные методы, сервер может генерировать и передавать пакет доступа клиенту доступа, который исполняется на пользовательском устройстве в ответ на запрос от клиента доступа. Пакет доступа может включать в себя один или более криптографических ключей и исполняемый код. Клиент доступа сконфигурирован для исполнения исполняемого кода, чтобы шифровать или дешифровать полезную нагрузку (например, файл). Зашифрованный файл может включать в себя один или более пакетов данных, которые включают в себя информацию о владении файлом, политики доступа к файлу, логи (журнал) доступа, помимо прочей информации. Эти пакеты данных обеспечивают само-интеллектуальность данных, как описано более подробно в настоящем документе. Кроме того, сервер, с которым клиент доступа имеет возможность связи, может поддерживать различные политики доступа к файлам, такие как доступ авторизованного пользователя, доступ к устройству и т.д. Сервер может поддерживать отображение файлов и политик доступа (параметры валидации). Таким образом, после

приема запроса на шифрование/дешифрование файла, сервер проверяет, что пользователь/устройство авторизован(о) выполнять шифрование/ дешифрование, идентифицирует соответствующие ключи, генерирует пакет доступа и передает пакет доступа клиенту. Таким образом, обладающая интеллектом конфигурация данных, клиент доступа и сервер функционируют, чтобы поддерживать безопасность данных динамическим образом. Эти и другие реализации описаны более подробно со ссылками на чертежи.

[0019] Аспекты раскрытия сначала описаны в контексте вычислительной среды, поддерживающей управление файлом шифрования. Аспекты раскрытия дополнительно описаны в отношении пакета доступа, который поддерживает управление зашифрованными файлами, примерного сценария управления файлами и схем потока процесса. Аспекты раскрытия дополнительно проиллюстрированы и описаны со ссылкой на схемы аппаратных компонентов, схемы систем и блок-схемы последовательностей операций, которые относятся к управлению зашифрованными файлами.

[0020] Фиг. 1 иллюстрирует пример системы 100, которая поддерживает управление зашифрованными файлами в соответствии с аспектами настоящего раскрытия. Система 100 сконфигурирована, чтобы создавать и управлять доступом к зашифрованным файлам. Система 100 включает в себя устройства 105 доступа, мобильное устройство 110, сервер 115 и репозиторий (хранилище) 120.

[0021] Устройства 105 доступа взаимодействуют с зашифрованными файлами на основе коммуникаций с сервером 115. Каждое из устройств 105 доступа во взаимосвязи с клиентами 125 доступа, исполняющимися на устройствах 105 доступа, может действовать в качестве устройства шифрования для генерирования и шифрования файлов и в качестве устройства дешифрования для дешифрования и просмотра зашифрованных файлов. В качестве примера, устройство 105-b доступа может быть устройством шифрования, которое генерирует зашифрованный файл (во взаимосвязи с сервером 115) и отправляет зашифрованный файл на устройство 105-a доступа. Устройство 105-a доступа может представлять собой устройство дешифрования, которое дешифрует (во взаимосвязи с сервером 115) и просматривает зашифрованный файл в соответствии с политиками, ассоциированными с зашифрованным файлом.

[0022] Устройства 105 доступа могут представлять собой примеры вычислительных систем в соответствии с теми, которые описаны на фиг. 8, и, например, могут представлять собой смартфоны, ноутбуки, планшеты, настольные компьютеры и тому подобное. Устройства 105 доступа могут взаимодействовать с другими устройствами 105 доступа, мобильным устройством 110 и сервером 115 с использованием проводных или беспроводных методов связи.

[0023] Устройство 105-a доступа может шифровать файлы, принимать зашифрованные файлы из других устройств доступа, взаимодействовать с сервером 115 для генерации и доступа к зашифрованным файлам, представлять информацию, дешифрованную из зашифрованных файлов, и устанавливать соединения и обновлять

данные с мобильным устройством 110. Устройство 105-a доступа включает в себя клиент 125 доступа.

[0024] Клиент 125 доступа представляет собой набор программ, работающих на устройстве 105-a доступа, которое генерирует, осуществляет доступ и просматривает зашифрованные файлы. Клиент 125 доступа может быть нативным приложением или веб-приложением, работающим через веб-браузер на устройстве 105-a доступа. Приложение доступа может включать в себя пользовательский интерфейс 130-a и исполняемый код 135-a доступа. Клиенты 125 доступа также могут быть плагинами приложений (подключаемыми модулями, программными кодами, дополняющими функционал основного приложения) для различных приложений просмотра файлов, таких как приложения для обработки слов, приложения электронных таблиц и т.п.

[0025] Пользовательский интерфейс 130-a является частью клиента 125 доступа, который обрабатывает пользовательское взаимодействие. Пользовательский интерфейс 130-a включает в себя элементы пользовательского интерфейса (кнопки, текстовые поля, окна медиа плеера и т.д.), которые обеспечивают вывод и принимают ввод от пользователя. Исполняемый код 135-a доступа представляет собой исполняемый файл, созданный устройством 105-a доступа из пакета доступа с сервера 115 для манипулирования зашифрованными файлами на устройстве 105-a доступа. В качестве примера, исполняемый код 135-a доступа может представлять собой динамически подключаемую библиотеку (DLL). Исполняемый код 135-a доступа включает в себя функцию 140-a доступа. Функция 140-a доступа является частью исполняемого кода 135-a доступа, которая выполняет функцию. Функция 140-a доступа может быть функцией шифрования, которая создает зашифрованный файл, функцией дешифрования, которая дешифрует зашифрованный файл, функцией завершения, которая удаляет зашифрованный файл, функцией ловушки и т.д. Функция ловушки может обеспечить вывод для зашифрованного файла, который подобен ожидаемому выходу из зашифрованного файла, но не включает в себя данные из полезной нагрузки зашифрованного файла.

[0026] Устройство 105-b доступа включает в себя клиент 125-b доступа, который включает в себя пользовательский интерфейс 130-b, и исполняемый код 135-b доступа. Исполняемый код 135-b доступа включает в себя функцию 140-b доступа. Аппаратные средства и компоненты устройства 105-b доступа работают аналогично таковым для устройства 105-a доступа.

[0027] Мобильное устройство 110 взаимодействует с устройством 105-a доступа для установления сетевых соединений и передачи данных. Мобильное устройство 110 представляет собой вычислительную систему в соответствии с теми, которые описаны на фиг. 8, и, например, может представлять собой смартфон, настольный компьютер, ноутбук, планшет или другой тип персонального устройства (например, карты безопасности или ключа безопасности). Мобильное устройство 110 может устанавливать беспроводное соединение персональной области с устройством 105-a доступа и переносить информацию местоположения. Мобильное устройство 110 включает в себя мобильное приложение 145.

[0028] Мобильное приложение 145 представляет собой набор программ, работающих на мобильном устройстве 110, которые устанавливают соединение с устройством 105-a доступа, собирают данные местоположения и передают данные местоположения. Мобильное приложение 145 может собирать данные местоположения из системы позиционирования мобильного устройства 110 (например, модуля системы глобального позиционирования (GPS)), которые определяют местоположение мобильного устройства и могут включать долготу, широту и высоту мобильного устройства 110.

[0029] Сервер 115 взаимодействует с другими компонентами системы 100 для управления доступом к зашифрованным файлам. Сервер 115 может представлять собой пример вычислительной системы в соответствии с теми, которые описаны на фиг. 10, и, например, может быть одним из множества серверов в одной или более облачных средах, которые хостируют серверное приложение 185.

[0030] Серверное приложение 185 представляет собой набор программ, которые обеспечивают ответы доступа на запросы доступа от устройства 105-a доступа через устройство 105-Ь доступа и могут управляться поставщиком услуг. Сервер 115 принимает запросы доступа от устройства 105-a доступа через устройство 105-b доступа для зашифрованных файлов. Серверное приложение 185 авторизует запросы доступа с использованием нескольких типов информации, включая учетные данные пользователя (идентификатор пользователя, адрес электронной почты, токен доступа и т.д.), информацию местоположения устройства доступа, информацию местоположения мобильного устройства, информацию привилегий пользователя, разрешения доступа к файлу и т.д.

[0031] Серверное приложение 185 генерирует ответы доступа для запросов доступа на основе авторизации запросов доступа. Серверное приложение 185 генерирует пакеты доступа, включенные в ответы доступа, которые возвращаются на устройство 105-a доступа через устройство 105-b доступа. Пакеты доступа включают в себя исходный код из репозитория 120, который был закачан с информацией, включая ключи от одного или более серверов 190 ключей. Пакеты доступа могут компилироваться устройствами 105 доступа для формирования соответствующих исполняемых кодов 135 доступа и соответствующих функций 140 доступа.

[0032] Серверы 190 ключей генерируют и поддерживают ключи, используемые для шифрования и дешифрования файлов в системе 100. Серверы 190 ключей осуществляют связь с сервером 115. Серверы 190 ключей могут хостироваться на различных серверах в различных облачных зонах и на различных облачных средах, чтобы препятствовать наличию в системе 100 единственной точки компрометации и повышать безопасность. Различные серверы ключей могут хранить различные типы ключей. Например, один сервер ключей может содержать ключи полезной нагрузки, другой сервер может управлять ключами микробазы данных, другой сервер ключей может управлять ключами файлов и т.п. Различные серверы ключей и наборы серверов ключей могут быть установлены для различных объектов с использованием системы 100. Например, первый объект может

использовать первый набор серверов ключей для разных типов ключей, а второй объект может иметь второй набор серверов ключей, который может отличаться от первого набора серверов ключей.

[0033] Репозиторий 120 представляет собой вычислительную систему, которая может включать в себя множество вычислительных устройств в соответствии с теми, которые описаны на фиг. 10. Репозиторий 120 может хостироваться поставщиком облачных услуг, хостирующим серверное приложение 185. Поставщик облачных услуг может предоставлять услуги хостинга, виртуализации и хранения данных, а также другие облачные услуги. Поставщик услуг, управляющий серверным приложением 185, может приводить в действие и управлять данными, программами и приложениями, которые хранят и извлекают данные из репозитория 120. Данные в репозитории 120 могут включать в себя исходный код, фильтры, базы данных и т.д. В качестве примера, репозиторий 120 включает исходный код 150 доступа, фильтры 175 маскирования и макробазу данных 180.

[0034] Исходный код 150 доступа является исходным кодом, который используется для генерирования исполняемых кодов 135 доступа после закачки с дополнительной информацией (например, ключами из одного или более серверов 190 ключей). Исходный код 150 доступа включает в себя исходный код 155 шифрования, исходный код 160 дешифрования, исходный код 165 прав пользователя и исходный код 170 завершения. Исходный код 155 шифрования включает в себя инструкции для шифрования полезных нагрузок для генерации зашифрованных файлов. Исходный код 160 дешифрования включает в себя инструкции для дешифрования зашифрованных файлов для восстановления полезных нагрузок из зашифрованных файлов. Исходный код 165 прав пользователя включает инструкции для обработки зашифрованных файлов на основе прав доступа пользователя (например, полный доступ, коллаборативный доступ и доступ только для чтения). Исходный код 170 завершения включает в себя инструкции для удаления зашифрованного файла из устройства доступа.

[0035] Права доступа пользователя к файлу могут включать в себя различные уровни, такие как полный доступ, коллаборативный доступ и доступ только для чтения. С полным доступом, пользователь может восстанавливать исходный файл, который может редактироваться внешними приложениями. Например, электронная таблица может восстанавливаться и редактироваться нативным приложением электронных таблиц. С коллаборативным доступом, пользователь может просматривать и обновлять информацию в зашифрованном файле, но не восстанавливать исходный файл. Например, пользователь может иметь возможность просматривать и редактировать информацию из полезной нагрузки зашифрованного файла в клиенте 125 доступа, но не может иметь возможность сохранять или распечатывать информацию из полезной нагрузки зашифрованного файла. С доступом только для чтения, пользователь может просматривать информацию из зашифрованного файла без возможности редактировать информацию. Например, пользователь может просматривать информацию с использованием клиента 125 доступа, но не может редактировать, распечатывать или сохранять информацию из

просматриваемого зашифрованного файла. Права доступа пользователя, которые также могут называться политиками доступа, могут исполняться в принудительном порядке клиентом 125 доступа и/или исполняемым кодом 135 доступа. В некоторых случаях, права доступа пользователя могут препятствовать совместному использованию полезной нагрузки в приложении видеоконференции.

[0036] Фильтры 175 маскирования реализуют предотвращение потери данных (DLP). Фильтры 175 маскирования идентифицируют типы и структуры данных для маскирования. В качестве примера, фильтр маскирования может использовать регулярные выражения, чтобы идентифицировать номера социального страхования с поисковой строкой “\d{3}-\d{2}-\d{4}” и замещать совпадения строкой замещения “XXX-XX-XXXX” для удаления номеров социального страхования из документа. Фильтры 175 маскирования могут применяться до шифрования полезной нагрузки, так что полезная нагрузка зашифрованного файла не включает в себя персональную идентифицирующую информацию. Дополнительно, фильтры 175 маскирования могут применяться после дешифрования зашифрованного файла для предотвращения просмотра или распространения персональной идентифицирующей информации из зашифрованного файла. Например, фильтры 175 маскирования могут исполняться в принудительном порядке как политики доступа или права пользователя.

[0037] Макробаза данных 180 хранит информацию о файлах, управляемых системой 100. Макробаза данных 180 может включать в себя супернабор информации в микробазах данных (например, также называемых пакетами данных), хранящихся в каждом зашифрованном файле системы 100. Макробаза данных 180 хранит информацию о каждом доступе для каждого зашифрованного файла. Например, макробаза данных 180 для зашифрованного файла может включать в себя таблицу информации со столбцами для даты доступа к зашифрованному файлу, типа доступа (создавать, считывать, записывать, обновлять и т.д. информацию о пользователе (например, идентификатор пользователя), информацию об устройстве доступа (идентификаторы аппаратных средств, идентификаторы программного обеспечения, идентификаторы сетевого соединения, идентификаторы адресов кодов физических адресов (MAC) и т.д.). Строки таблицы могут проводить различие между разными событиями доступа. Макробаза данных 180 документирует цепочку хранения и перемещения, которая идентифицирует пользователей и машины, которые имеют доступ к зашифрованным файлам системы 100.

[0038] Макробаза данных 180 может использовать хэш-цепочку, чтобы хранить информацию события доступа. Например, для каждого события доступа, добавленного в макробазу данных 180 для зашифрованного файла, информация события доступа комбинируется с предыдущим хэш-значением для формирования полезной нагрузки хэша. Алгоритм криптографического хэширования применяется к полезной нагрузке хэша, чтобы генерировать новое хэш-значение, которое сохраняется с информацией события доступа. Новое хэш-значение может использоваться как “предыдущее хэш-значение” для последующего события доступа для формирования постоянной цепочки хэш-значений.

Если информация в хэш-цепочке модифицируется, то последующие хэш-значения будут неверными.

[0039] Каждый из компонентов системы 100 работает во взаимосвязи, чтобы поддерживать динамическую, обладающую собственным интеллектом и самозащитой безопасность данных. Например, пользователь может осуществлять доступ к клиенту 125-a доступа, чтобы защитить файл и предоставить доступ к файлу различным пользователям. С использованием клиента 125-a доступа пользователь выбирает файл, который должен быть защищен. Файл может быть примером видеофайла, аудиофайла, файла текстового процессора, текстового файла, мультимедийного файла, PDF или тому подобного. После выбора файла для защиты, пользователю может предлагаться, клиентом 125-a доступа, выбрать параметры доступа пользователя, которые соответствуют политикам доступа к файлу. Эти параметры доступа пользователя (или политики доступа пользователя) могут включать в себя пользователей, которые авторизованы просматривать файл, местоположение (локацию) или ограничения геозонирования (например, офис или другие административные авторизованные локации), периоды времени или эмбарго, ограничения устройства, среди других типов политик и ограничений. Для выбора пользователей, клиент 125-a доступа может осуществлять доступ к локальному или удаленному перечню контактов или пользователей и предлагать пользователю производить поиск и/или выбирать пользователей, которые должны иметь доступ к файлу, и тип доступа (например, доступ только для чтения, коллаборативный или полный доступ) для каждого пользователя.

[0040] После выбора политик доступа, пользователь может выбрать компонент пользовательского интерфейса (UI), чтобы зашифровать файл. Как описано более подробно в настоящем документе, клиент 125-a доступа может принимать пакет доступа от сервера 115 в ответ на запрос зашифровать файл. Пакет доступа может включать в себя исполняемый код 135-a доступа, и клиент 125-a доступа может исполнять инструкции исполняемого кода 135-a, чтобы зашифровать файл с использованием ключей, принятых от сервера 115 в пакете доступа. Шифрование файла приводит к новому зашифрованному файлу с новым расширением файла (например, отличным от исходного файла), и новый зашифрованный файл является интеллектуальным (умным) (осведомленным об управлении (администрировании) правами) на основе политик доступа к файлу, которые встроены в сам зашифрованный файл. В некоторых реализациях, новый зашифрованный файл замещает исходный файл. В таких случаях, исходный файл автоматически удаляется после успешного создания зашифрованного файла. Этот признак может зависеть от конкретных политик организации или может активироваться после шифрования файла.

[0041] Зашифрованный файл может передаваться другим различным пользователям с использованием различных методов, таких как электронная почта, FTP, доступ к базе данных, удаленный доступ и т.д. Например, устройство 105-b доступа имеет локальный или удаленный доступ к зашифрованному файлу. Если пользователь пытается открыть файл, то клиент 125-a доступа конфигурируется, чтобы передавать запрос дешифрования на сервер 115. Запрос может включать в себя различную информацию, которая должна быть

валидирована в сервере 115. Если сервер 115 валидирует запрос, то сервер 115 передает ответ с пакетом доступа, который включает в себя исполняемый код 135-b доступа. Клиент 125-b доступа исполняет инструкции исполняемого кода 135-b доступа, чтобы дешифровать файл и его компоненты (например, пакеты данных, описанные более подробно в настоящем документе). Клиент 125-b доступа принудительно исполняет права доступа пользователя или политики доступа, которые включены в пакеты данных.

[0042] Пакеты данных, которые включены в зашифрованные файлы, включают в себя информацию о владении (например, пользователе, устройстве, организации), политики доступа к файлу (например, типы прав доступа пользователя) и логи доступа. Эта информация перемещается с зашифрованным файлом и может обновляться посредством запроса дешифрования. Так как политики доступа к файлу включены в файл, доступ к содержимому файла (например, полезной нагрузке, такой как PDF) может осуществляться, когда принудительно исполняются политики доступа к файлу.

[0043] Дополнительно, как описано в настоящем документе, сервер 115, посредством приложения 185 сервера и репозитория 120, поддерживает политики и права доступа к файлу. В общем (существуют некоторые исключения, как описано в настоящем документе), клиент 125 доступа не может расшифровать зашифрованный файл без связи с сервером. Таким образом, пользователи (например, административные пользователи или владельцы файлов) могут обновлять политики доступа к файлу, ассоциированные с различными файлами, с использованием клиента 125 доступа (например, панели инструментов, поддерживаемой клиентом 125 доступа). После приема запроса дешифрования файла, сервер 115 может определять, что политики доступа в файле являются устаревшими (например, не текущими), и передавать обновленные политики доступа с пакетом доступа на клиент 125 доступа. Например, файл доступ может динамически обновляться без необходимости сначала дешифровать файлы для включения обновленных политик доступа. Дополнительно, поскольку связь с сервером обычно происходит при запросах доступа к файлу (например, запрос дешифрования или шифрования), сервер 115 может поддерживать лог таких запросов. Лог может использоваться, чтобы поддерживать панель инструментов, используемую административными пользователями для просмотра локаций доступа, отклонений доступа, пользователей, которые запросили доступ, и тому подобного. Дополнительно, панель инструментов может использоваться, чтобы изменять политики доступа для различных пользователей, различных файлов и т.д. почти в реальном времени. Например, методы, описанные в настоящем документе, могут позволять организации иметь полный обзор в почти реальном времени своих механизмов и результатов защиты файлов.

[0044] Специалисту в данной области техники должно быть понятно, что один или более аспектов раскрытия могут быть реализованы в системе 100, чтобы дополнительно или альтернативно решать другие проблемы, чем те, которые описаны здесь. Более того, аспекты раскрытия могут обеспечивать технические усовершенствования “традиционных” систем или процессов как описано здесь. Однако описание и прилагаемые чертежи

включают в себя только примерные технические усовершенствования, вытекающие из реализации аспектов раскрытия, и соответственно не представляют все из технических усовершенствований, обеспеченных в объеме формулы изобретения.

[0045) Фиг. 2 иллюстрирует пример зашифрованного файла 200, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Зашифрованный файл 200 использует множество солей и ключей (которые не хранятся в зашифрованном файле 200), чтобы управлять доступом к полезной нагрузке 205 и защищать полезную нагрузку 205 от неавторизованного доступа. Зашифрованный файл 200 включает в себя полезную нагрузку 205, пакеты 210 данных и метаданные 215.

[0046] Полезная нагрузка 205 представляет собой электронный файл, который формирует основу зашифрованного файла 200. Полезная нагрузка 205 может включать в себя любой тип электронного файла, включая текстовые документы, электронные таблицы, слайдовые презентации, файлы исходного кода, файлы изображений, архивные файлы, видеофайлы и т.д. Зашифрованный файл 200 может включать в себя один файл в полезной нагрузке 205.

[0047] Полезная нагрузка 205 может солиться солью 220 полезной нагрузки и шифроваться при помощи ключа 225 полезной нагрузки до вставки в зашифрованный файл 200. В некоторых реализациях, ключ 225 полезной нагрузки может представлять собой ключ развитого стандарта шифрования (AES) длиной 256 битов. В некоторых реализациях, соль 220 полезной нагрузки представляет собой произвольно сгенерированное восьмибайтовое значение. В некоторых реализациях, соль 220 полезной нагрузки применяется к полезной нагрузке 205 путем присоединения соли 220 полезной нагрузки к полезной нагрузке 205.

[0048] Пакеты 210 данных (которые могут также называться микробазой данных, базой данных владельца или их комбинацией) могут включать в себя поднабор информации макробазы данных (например, макробазы 180 данных на фиг. 1), которая относится к недавнему доступу к зашифрованному файлу 200, политикам доступа к файлу, ассоциированным с зашифрованным файлом 200, и информации владельца, ассоциированной с зашифрованным файлом. Пакеты 210 данных могут включать в себя информацию лога доступа (например, в логе 250 доступа), которая идентифицирует предыдущего последнего пользователя(ей) для доступа к зашифрованному файлу 200 и предыдущее устройство(а) доступа для доступа к зашифрованному файлу 200. Например, пакет данных может включать в себя лог 250 доступа, который включает в себя отпечатки (fingerprints, идентификационные признаки), ассоциированные с пользователями и устройствами, которые ранее осуществляли доступ к зашифрованному файлу 200. Информация отпечатков пользователя может включать в себя адрес электронной почты, токен доступа, хэш-значение и т.д. Информация отпечатков устройства доступа может включать в себя идентификатор аппаратных средств и/или программного обеспечения. В некоторых примерах, информация отпечатков для лога 250 доступа может включать в себя информацию сети, информацию географического местоположения, информацию клиента

доступа и т.д. В некоторых случаях, лог 250 доступа включает в себя информацию аппаратных средств, которая уникально идентифицирует компонент аппаратных средств, исполняющий клиент доступа. В качестве примера, информация аппаратных средств может представлять собой отпечаток (thumbprint, отпечаток большого пальца) пользователя, который является универсально уникальным идентификатором (UUID) из вычислительной системы пользователя. В качестве другого примера, отпечаток пользователя может представлять собой серийный номер материнской платы. Информация доступа лога 250 доступа может включать в себя временную метку доступа. Временная метка доступа может идентифицировать дату и время последнего успешного доступа к зашифрованному файлу 200.

[0049] Дополнительно, пакеты 210 данных могут включать в себя указания прав доступа (например, политики 245 доступа к файлу) для зашифрованного файла 200 и информацию о владении или объекте (также называемую базой данных владельца) для зашифрованного файла 200. Политики 245 доступа к файлу могут указывать полный доступ, коллаборативный доступ, доступ только для чтения и могут специфицироваться на глобальной основе, на групповой основе, по каждому пользователю и т.д. Политики доступа к файлу могут также включать в себя информацию администрирования цифровых прав, которая может представлять собой поднабор политик доступа к файлу, который включает в себя данные, которые идентифицируют привилегии и права доступа пользователей для зашифрованного файла 200. В качестве примера, информация администрирования цифровых прав может включать в себя значения для следующих полей: PrintAllowed, SaveAllowed, LocalCopyAllowed, ForwardAllowed, Collaborate, ReadOnly и FullAccess. Информация администрирования цифровых прав может быть сконфигурирована на глобальной основе, на групповой основе, по каждому пользователю и т.д. Права доступа могут также включать в себя ограничения отображения, которые ограничивают или разрешают доступ к файлу с использованием различных программ, например, ограничение или разрешение на совместное использование полезной нагрузки в программе видеоконференций.

[0050] Значения для PrintAllowed, SaveAllowed, LocalCopyAllowed, ForwardAllowed могут представлять собой двоичные значения. Значение для поля PrintAllowed идентифицирует, может ли пользователь распечатать информацию из полезной нагрузки 205 зашифрованного файла 200. Значение для поля SaveAllowed идентифицирует, может ли пользователь сохранить информацию из полезной нагрузки 205 зашифрованного файла 200 в устройство доступа. Значение для поля LocalCopyAllowed идентифицирует, может ли локальная копия информации из полезной нагрузки 205 зашифрованного файла 200 храниться на устройстве доступа. Значение для поля ForwardAllowed идентифицирует, может ли информация из полезной нагрузки 205 зашифрованного файла 200 направляться на другое устройство (например, как часть электронного письма).

[0051] Значения для Collaborate, ReadOnly и FullAccess могут представлять собой двоичные значения, которые могут устанавливаться независимо. Значение для поля

Collaborate идентифицирует, может ли пользователь иметь коллаборативный доступ к полезной нагрузке 205 зашифрованного файла 200. Значение для поля ReadOnly идентифицирует, может ли пользователь иметь доступ только для чтения к полезной нагрузке 205 зашифрованного файла 200. Значение для поля FullAccess идентифицирует, может ли пользователь иметь полный доступ к полезной нагрузке 205 зашифрованного файла 200.

[0052] Политики 245 доступа могут также включать в себя информацию предотвращения потери данных, которая включает в себя информацию и инструкции, которые могут идентифицировать и удалять или маскировать конфиденциальную информацию из полезной нагрузки 205 зашифрованного файла 200. Информация предотвращения потери данных может представлять собой примеры ограничений отображения, как описано в настоящем документе. Конфиденциальная информация включает в себя идентифицирующие личность сведения. Конфиденциальная информация может удаляться или маскироваться перед тем, как полезную нагрузку 205 просматривают или сохраняют на устройство доступа, действующее как устройство дешифрования. В качестве примера, информация предотвращения потери данных может включать в себя значения для следующих полей PackagelD, Rules, RuleID.

[0053] Значение для PackagelD идентифицирует пакет исходного кода, который необходимо включить в пакет доступа для удаления или маскирования конфиденциальной информации из полезной нагрузки 205. Значения для поля Rules идентифицируют группы правил, которые необходимо включить в пакет доступа для удаления или маскирования конфиденциальной информации из полезной нагрузки 205. Значение для RulelD идентифицирует конкретное правило, которое необходимо включить в пакет доступа для удаления или маскирования конфиденциальной информации из полезной нагрузки 205. Каждое правило для предотвращения потери данных включает в себя строку регулярного выражения со строкой подстановки для замещения данных в полезной нагрузке 205, которые совпадают с регулярным выражением (из потока регулярных выражений) в соответствии со строкой подстановки.

[0054] Политики 245 доступа к файлу могут также включать в себя информацию завершения. Информация завершения может включать в себя флаг завершения, который идентифицирует, была ли завершена полезная нагрузка 205 зашифрованного файла 200. Полезная нагрузка 205 могла быть завершена путем замены исходной полезной нагрузки (после шифрования) нулевыми или произвольными данными того же размера, что и исходная полезная нагрузка, для предотвращения доступа к данным в исходной полезной нагрузке. Флаг завершения может устанавливаться в “истинно”, когда неавторизованной пользователь или устройство пытается осуществить доступ к зашифрованному файлу 200.

[0055] Политики 245 доступа к файлу могут также налагать ограничения географического местоположения. Например, политика доступа к файлу может указывать, что доступ к файлу возможно осуществить только в местоположении офиса, географическом местоположении (например, в штате или стране) или тому подобное.

Таким образом, при принудительном исполнении политики, клиент доступа может использовать информацию сети, информацию GPS или другую информацию, которая может использоваться, чтобы идентифицировать географическое местоположение, чтобы определить, что доступ авторизован. Если такая информация недоступна, доступ к полезной нагрузке 205 может быть ограничен. Таким образом, политики 245 доступа к файлу могут включать в себя различные формы, включая биты, которые указывают типы прав доступа, указания правил или инструкций, принудительно обеспечивающих предотвращения потери данных, указания географических ограничений и тому подобное. В некоторых случаях, политики 245 доступа к файлу могут ограничивать пользователя от использования виртуальной частной сети (VPN) для осуществления доступа к файлам. Таким образом, если обнаружена VPN, то запрос доступа может отклоняться или пользователь может быть ограничен от просмотра файла.

[0056] Информация 255 о владении может включать в себя значение для поля Author ID, которое уникально идентифицирует пользователя, который создал зашифрованный файл 200. Значение для Author ID может представлять собой адрес электронной почты, идентификатор сотрудника, имя пользователя и т.д. Информация 255 о владении может включать в себя сигнатуру (подпись) объекта, такую как цифровая подпись. Пользователь системы может быть одним из множества сотрудников объекта. Каждый зашифрованный файл, сгенерированный пользователями для объекта, может включать в себя одну и ту же подпись объекта, которая идентифицирует объект как источник зашифрованного файла, или множество подписей объекта, которые могут идентифицировать объект как источник зашифрованного файла и пользователя, который сгенерировал зашифрованный файл.

[0057] Информация 255 о владении может также включать в себя информацию базы данных объекта, которая включает в себя указание одной или более конечных точек интерфейса программирования приложений (API) (например, унифицированные указатели ресурса (URL)), которые клиент доступа использует, чтобы верифицировать, что пользователь имеет доступ к зашифрованному файлу. Например, одна или более указанных конечных точек API может быть Verify API и Transfer API. Доступ к Verify API может осуществляться, чтобы верифицировать, что пользователь (имеющий тот же самый объект, что и зашифрованный файл 200) может осуществлять доступ к зашифрованному файлу 200. Доступ к Transfer API может осуществляться, чтобы верифицировать, что пользователь (имеющий объект, отличный от зашифрованного файла 200) может осуществлять доступ к зашифрованному файлу 200. Так как доступ к конечным точкам API может осуществляться перед дешифрованием зашифрованного файла 200, конечные точки API могут быть расположены вне всех надстроек шифрования (например, могут не быть зашифрованы одним из ключей). Например, указания конечных точек API могут быть включены в метаданные 215.

[0058] Метаданные 215 являются хранилищем информации о зашифрованном файле 200. В качестве примера, метаданные 215 могут идентифицировать тип файла в полезной нагрузке 205, имя файла в полезной нагрузке 205, длину файла в полезной нагрузке 205,

алгоритмы шифрования для полезной нагрузки 205 (включая алгоритм добавления соли), алгоритмы шифрования для пакетов 210 данных, алгоритмы шифрования для зашифрованного файла 200 и т.д. Как описано в настоящем документе, метаданные 215 могут также включать в себя указания конечных точек API. Различные аспекты метаданных 215 могут или не могут быть зашифрованы как часть зашифрованного файла 200. В некоторых случаях, аспекты метаданных 215 могут быть включены в запрос доступа (запрос шифрования или дешифровки) на сервер.

[0059] Пакеты 210 данных могут быть зашифрованы при помощи одного или более ключей 230 пакетов данных до вставки в зашифрованный файл 200. В некоторых реализациях, один или более ключей 230 пакетов данных могут представлять собой ключи развитого стандарта шифрования (AES) 128. Один или более ключей 230 пакетов данных могут быть короче, чем ключ 225 полезной нагрузки для сокращения времени, требуемого для доступа к данным в пакетах 210 данных.

[0060] Зашифрованный файл 200 может быть присолен солью 235 файла и зашифрован при помощи ключа 240 файла. В некоторых реализациях, ключ 240 файла может представлять собой ключ развитого стандарта шифрования (AES) 256. В некоторых реализациях, соль 235 файла представляет собой произвольно сгенерированное восьмибайтовое значение. Соль 235 файла может применяться к содержимому зашифрованного файла 200 (например, полезной нагрузке 205 после присаливания солью 220 полезной нагрузки и шифрования ключом 225 полезной нагрузки, пакетам 210 данных после шифрования ключами 230 пакетов данных) путем присоединения соли 235 файла к зашифрованному файлу 200.

[0061] В некоторых реализациях, соль (например, соль 235 файла) создается путем генерации первого произвольного 8-разрядного числа между 10000000 и 99999999, хранящегося в Y. Второе произвольное число между 1 и 8 затем генерируется и сохраняется в X. X-ый разряд в Y затем замещается значением X. Этапы генерации второго произвольного числа и замещения значения в Y повторяются четыре раза. Значение после последнего замещения является солью. Могут использоваться разные алгоритмы для генерации солей, используемых системой.

[0062] Различная информация, включенная в пакеты 210 данных, во взаимосвязи с коммуникациями с сервером, поддерживает динамические, обладающие собственным интеллектом и самозащитой схемы обеспечения безопасности данных, описанные в настоящем документе. Когда клиент доступа принимает пакет доступа (например, исполняемые файлы и ключи доступа) от сервера, клиент доступа исполняет исполняемый код пакета доступа, чтобы дешифровать содержимое зашифрованного файла с использованием различных ключей. Клиент доступа сконфигурирован, чтобы принудительно исполнять политики 245 доступа, которые включены в зашифрованный файл. Дополнительно, после дешифрования, исполняемый код пакета доступа может вызывать обновление лога 250 доступа информацией о клиенте доступа (например, идентификатор клиента, версия, отпечаток), устройстве, исполняющем клиент доступа

(например, идентификатор устройства, идентификатор материнской платы, идентификатор аппаратных средств), информацией пользователя и другой информацией, как описано в настоящем документе. Например, если зашифрованный файл 200 передается другому пользователю или устройству, и пользователь пытается открыть зашифрованный файл 200, содержимое лога 250 доступа может использоваться, чтобы идентифицировать цепочку хранения и перемещения зашифрованного файла 200, чтобы увидеть, кто и/или какое устройство скомпрометировало зашифрованный файл 200.

[0063] В некоторых случаях, перед дешифрованием файла, политики 245 доступа, ассоциированные с файлом, могут обновляться. В таких случаях, после того, как запрос дешифрования отправляется на сервер (например, сервер 115), сервер может отвечать обновленными политиками доступа в пакете доступа, так что после дешифрования принудительно исполняются обновленные политики доступа. Однако, поскольку политики доступа включены в файл, поддерживаются различные другие признаки, такие как офлайн-доступ.

[0064] Аспекты фиг. 2 описаны относительно полезной нагрузки 205, представляющей собой файл. Следует понимать, что методы, описанные в настоящем документе, могут быть применимы к частям файла или объектам в файле. Например, файл может включать в себя множество элементов (например, элементов OLE), изображений, графиков и т.д., которые встроены в файл. В таких случаях, полезная нагрузка 205 может быть примером одного конкретного элемента в файле или части файла (например, конкретными страницами). Таким образом, элемент или страница (например, полезная нагрузка 205) может зашифровываться и политики 245 доступа могут исполняться в принудительном порядке для элемента или страницы. Аналогично, лог 250 доступа и информация 255 о владении могут быть основаны на элементе или странице в защищаемом файле.

[0065] Фиг. 3 иллюстрирует пример вычислительной архитектуры 300, которая поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Вычислительная архитектура 300 включает в себя пользовательское устройство 305 и сервер 310. Пользовательское устройство 305 может быть примером устройства 105 доступа, как описано в отношении фиг. 1. Сервер 310 может быть примером сервера 115, как описано в отношении фиг. 1. Пользовательское устройство 305 может быть сконфигурировано, чтобы исполнять клиент 325 доступа для поддержки методов управления файлами, описанных в настоящем документе.

[0066] Пользователь пользовательского устройства 305 может осуществлять доступ к клиенту 325 доступа, чтобы шифровать и/или дешифровать файлы или части файлов в соответствии с методами, описанными в настоящем документе. В некоторых случаях, пользователю требуется входить в систему клиента доступа ежедневно, периодически и т.д. Вход в систему клиента 325 доступа может запускать связь с сервером 310, включая установку безопасного соединения. Дополнительно, токен может генерироваться при входе в систему, и токен может использоваться для безопасной связи с сервером 325. В некоторых

примерах, пользователь может регистрировать географическое местоположение, идентификатор сети и т.д. при входе в систему, и такая информация используется для генерации токена, безопасной связи с сервером, принудительного исполнения политик доступа к файлу (например, геозонирования данных) и т.д.

[0067] В примере использования клиента 325 доступа, пользователь может использовать клиент доступа, чтобы защитить файл или часть файла перед его передачей группе пользователей. Пользователь может выбрать файл и затем выбрать политики доступа к файлу для файла посредством клиента 325 доступа. После выбора файла и политик доступа к файлу, клиент 325 доступа может отправлять запрос на 330 доступ на сервер 310. В случае запроса шифрования, сервер 310 может быть идентифицирован на основе URL (например, конечной точки API), сконфигурированного в клиенте 325 доступа. Запрос 330 доступа может включать в себя информацию 315 доступа, а также информацию файла, ассоциированную с файлом (размер файла, тип, метаданные файла). Информация 315 доступа может индивидуально оптимизироваться на основе клиента 325 доступа. В зависимости от реализации (например, конфигураций организации, персональных конфигураций) клиента 325 доступа, информация доступа может включать в себя различную информацию, такую как адрес Интернет-протокола (IP), информация сети, идентификатор материнской платы, универсально уникальный (UU) идентификатор, идентификаторы пользователей, идентификаторы клиентов (например, идентификатор лицензии клиента), версия клиента, информация географического местоположения, информация браузера (например, в случае браузерного клиента), информация приложения (например, в случае плагина клиента). Информация 315 доступа может также включать в себя токен доступа.

[0068] Информация доступа может включать в себя информацию о пользователе, вычислительной системе пользователя, местоположении вычислительной системы и типе запрашиваемого доступа. Информация о пользователе может включать в себя имя пользователя, токены пользовательского доступа, цифровую подпись пользователя, открытый ключ пользователя и т.д. Информация о вычислительной системе пользователя может включать в себя идентификаторы аппаратных средств и программного обеспечения компонентов аппаратных средств и программного обеспечения вычислительной системы. Информация о местоположении компьютерной системы может включать в себя IP-адрес для компьютерной системы, который может отображаться на географическое местоположение. Информация доступа может быть частью заголовка запроса доступа и может форматироваться в соответствии со стандартом записи объектов JavaScript (JSON).

[0069] Сервер 310 может проверять достоверность (валидировать) информации 315 доступа. Валидации могут включать в себя валидирование местоположений, валидирование сетей, валидирование устройства, валидирование токена (например, что токен активен) и другую информацию. В некоторых случаях, организация может быть ассоциирована с политиками организации, которые указывают, что необходимо представить определенную информацию, чтобы использовать функцию шифрования.

Например, глобальная политика может указывать, что сотрудники или пользователи могут иметь возможность шифровать файл только при присутствии в офисе. Например, используются различные валидации для обеспечения удовлетворения организационных политик. Валидации могут настраиваться для различных условий и сценариев.

[0070] Информация 315 доступа, запрос 330 доступа или другая коммуникация от клиента 325 доступа может также включать в себя указания политик доступа к файлу для файла, подлежащего шифрованию. Таким образом, выбранные политики, включая политики чтения, записи, коллаборации, географического ограничения, авторизованных пользователей и другие политики могут сообщаться на сервер 310. Сервер 310 может поддерживать запись информации файла и политик доступа (например, в макробазе 180 данных на фиг. 1) в безопасном репозитории.

[0071] Если запрос 330 доступа валидирован, информация доступа может сохраняться как описано в настоящем документе, и сервер 310 может генерировать пакет 320 доступа. Чтобы сгенерировать пакет 320 доступа, сервер 310 может запросить (например, передать запрос) безопасное хранилище ключей сгенерировать ключи шифрования с использованием сервиса ключей. Безопасное хранилище ключей может представлять собой пример услуги администрирования ключей третьей стороной. Безопасное хранилище ключей может возвращать произвольную строку, которая используется, чтобы генерировать ключи. Сервер 310 может быть сконфигурирован, чтобы разделять строку на один или более ключей 335 доступа, и, например, безопасное хранилище ключей может не иметь возможности идентифицировать ключи 335 доступа. В некоторых примерах, запрос в хранилище ключей может включать в себя информацию идентификации файла, которая может использоваться в последующем запросе дешифрования для приема строки ключей. Каждый запрос шифрования может приводить к разному набору ключей.

[0072] Сервер 310 может также генерировать информацию 340 доступа для пакета 320 доступа. Информация доступа может включать в себя код (например, исполняемый код) из различных типов библиотек шифрования или дешифрования. Например, схемы и ключи шифрования/дешифровки могут настраиваться в зависимости от желаний организации, реализующей методы, описанные в настоящем документе. Информация 340 доступа может включать в себя инструкции для шифрования файла, включающего в себя полезную нагрузку и пакеты данных. В некоторых случаях, пакет 320 доступа может включать в себя указание политик доступа к файлу и/или информацию о владении, так что политики и информация о владении могут быть зашифрованы с файлом. Информация 340 доступа может извлекаться из репозитория инструкций (например, репозитория 120 на фиг. 1). Репозиторий инструкций может конфигурироваться для каждого арендатора или организации, которые реализуют систему, описанную в настоящем документе, и, например, может использовать настраиваемые или выбираемые методы шифрования/дешифрования, форматы ключей и тому подобное.

[0073] В некоторых случаях, как описано в настоящем документе, информация 340

доступа компилируется устройством 305, чтобы сгенерировать машиноисполняемый код, который используется, чтобы выполнять операции (например, шифровать, дешифровать, обеспечивать выполнение политик). В некоторых случаях, информация 340 доступа может включать в себя значения или полезные нагрузки данных, которые используются, чтобы преобразовывать данные полезной нагрузки/файла в другой вид, или используются, чтобы применять операции для изменения значений в данных, или то и другое. В некоторых примерах, инструкции преобразования данных могут указываться в пакете 320 доступа или могут конфигурироваться в клиенте 325 доступа. Например, когда информация 320 доступа включает в себя значения или полезную нагрузку данных, информация 320 доступа (и пакет 320 доступа) могут не включать в себя компилируемый или исполняемый код.

[0074] Пакет 320 доступа передается на устройство 305 (например, клиент 325 доступа) в ответе 345 доступа. Клиент 325 доступа сконфигурирован, чтобы использовать информацию 340 доступа для генерации зашифрованного файла (например, с использованием ключей 335 доступа). Использование информации доступа может включать в себя исполнение кода, включенного в информацию 340 доступа, что вызывает создание и шифрование пакетов данных, шифрование полезной нагрузки (например, файла, подлежащего шифрованию) и шифрование пакетов данных и файла вместе. Например, в зависимости от конфигурации, может существовать множество уровней шифрования в зашифрованном файле. Зашифрованный файл может затем передаваться различным другим пользователям и устройствам с использованием методов переноса файлов или связи.

[0075] Если запрос 330 доступа представляет собой запрос дешифрования, то могут использоваться аналогичные методы. Аналогичная информация 315 доступа может сообщаться на сервер 310. Сервер 310 может выполнять различные валидации. Валидации для дешифрования могут отличаться от валидации шифрования. Например, сервер 310 может определять, авторизован ли пользователь и/или устройство, запрашивающее дешифрование, осуществлять доступ к файлу, на основе информации, сохраненной в ассоциации с идентификатором файла. В некоторых случаях, валидация включает в себя определение, что местоположение запрашивающего пользовательского устройства 305 удовлетворяет политике местоположения (географического местоположения, местоположения сети).

[0076] Если запрос 330 доступа валидирован, то сервер 310 может генерировать пакет 320 доступа. Генерация пакета доступа может включать в себя передачу запроса на сервис хранения ключей для ассоциированной строки ключа. Например, запрос на сервис хранения ключей может включать в себя указание идентификатора файла для файла, подлежащего дешифрованию. Сервер 310 может принимать строку ключа и генерировать ключ 335 доступа и информацию 340 доступа. В этом случае, исполняемый код может включать в себя инструкцию дешифрования для дешифрования всего файла, пакетов данных и полезной нагрузки зашифрованного файла.

[0077] В некоторых случаях, информация 340 доступа может вызывать шифрование файла и затем пакетов данных. Политики доступа к файлу пакетов данных могут затем

исполняться в принудительном порядке до дешифрования полезной нагрузки. Например, если политика представляет собой политику географического местоположения и политика не удовлетворена на основе информации, идентифицированной клиентом 325 доступа, то исполнение информации 340 доступа может завершаться, пока политика не будет удовлетворена. Таким образом, доступ к полезной нагрузке не осуществляется, хотя даже части файла были дешифрованы.

[0078] Чтобы исполнить информацию 340 доступа, клиент 325 доступа может создать объект, ассоциированный с кодом в памяти, и использовать ключи 335 доступа, чтобы зашифровать или дешифровать файл. После того, как файл успешно зашифрован или дешифрован, код разрушается (например, удаляется из памяти). Таким образом, объект содержится в памяти устройства 305 во время работы и удаляется после исполнения. Таким образом, клиент 325 доступа сконфигурирован, только чтобы исполнять код, и не сконфигурирован (без кода), чтобы дешифровать или дешифровать файлы.

[0079] В некоторых примерах, сервер 310 определяет, что запрос 330 доступа является недействительным, на основе информации 315 доступа. Например, сервер 310 может определять, что запрос пришел из неавторизованного местоположения, сети, устройства, клиента, пользователя и т.д. В таких случаях, сервер 310 может выполнять различные действия. Одно действие может включать в себя передачу оповещения административному пользователю (например, посредством электронной почты, оповещения или тому подобного). Другое действие может включать в себя генерацию пакета 320 доступа с информацией 340 доступа, которая сконфигурирована, чтобы перезаписывать содержимое полезной нагрузки. Дополнительно или альтернативно, информация 340 доступа может запускать метку завершения в политиках доступа к файлу. Например, после неавторизованного запроса, пользователь не может осуществить доступ к файлу, и содержимое файла может быть перезаписано.

[0080] В некоторых случаях, сервер 310 может определять, что запрос 330 доступа является достоверным, но сервер 310 может также определять, что политики доступа 350, ассоциированные с файлом, являются устаревшими. Чтобы произвести такое определение, сервер 310 может сравнивать информацию (например, информацию файла, хэш-значения, версии), включенную в информацию 315 доступа, с информацией (например, информацией файла, хэш-значениями, версиями), поддерживаемой сервером 310. Если политики устарели, пакет 320 доступа может включать в себя обновленные или текущие политики доступа 350, выполнение которых принудительно обеспечивается клиентом 325 доступа.

[0081] Как описано в настоящем документе, пакет доступа может представлять собой пакет шифрования, пакет дешифрования, пакет ловушки или пакет завершения. Пакет шифрования может включать в себя исходный код с функциями для шифрования данных, но не включает в себя исходный код с функциями для дешифрования данных. Пакет дешифрования может включать в себя исходный код с функциями для дешифрования данных, но не для шифрования данных. Пакет завершения может включать в себя исходный код с функциями, чтобы скрывать или удалять зашифрованные файлы. Пакет ловушки

может включать в себя исходный код с функциями для отображения данных, которые выглядят аналогично данным из зашифрованного файла, но которые не включают в себя данные из зашифрованного файла. Пакет завершения и пакет ловушки не могут включать в себя исходный код, ключи или соли, используемые, чтобы шифровать или дешифровать данные.

[0082] Пакет завершения может скрывать данные путем отображения пользователю сообщения, указывающего, что данные из зашифрованного файла не могут быть дешифрованы. Пакет завершения может удалять данные путем перезаписи данных в зашифрованном файле произвольными данными в ответ на авторизацию доступа, указывающую, что вычислительная система, которая отправила запрос доступа, расположена в запрещенной области геозоны. Запрещенные области геозоны могут включать в себя определенные страны.

[0083] В некоторых случаях, клиент 325 доступа сконфигурирован с доступом к структурам папок в устройстве 305 пользователя, в веб-сервисе хранения файлов, в удаленном сервере или тому подобном. Клиент 325 доступа может также быть сконфигурирован, чтобы шифровать любой файл, который сохранен в назначенную папку или местоположение. Например, когда файл сохраняется в папку, клиент 325 доступа может запускать передачи запросов 330 доступа (запроса шифрования) на сервер 310. Таким образом, с использованием этих методов, схемы защиты на уровне папок могут исполняться в принудительном порядке.

[0084] Фиг. 4 иллюстрирует пример потока 400 процесса, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Конкретно, поток 400 процесса иллюстрирует операции для шифрования файлов в соответствии с методами, описанными в настоящем документе. Поток 400 процесса включает в себя устройства 405 доступа и сервер 410, которые могут служить примерами соответствующих устройств, описанных в отношении фиг. 1-3.

[0085] В 415, выбирается полезная нагрузка. Полезная нагрузка может выбираться пользователем при помощи пользовательского интерфейса клиента доступа, исполняющегося на устройстве 405-а доступа. В 420, клиент доступа устройства 405-а доступа может получать информацию доступа. Информация доступа может включать в себя информацию о пользователе и устройстве 405-а доступа. В качестве примера, информация может включать в себя идентификатор компонента аппаратных средств из устройства 405-а доступа и адрес Интернет-протокола устройства 405-а доступа.

[0086] В 425, устройство 405-а доступа передает запрос доступа на сервер 410. Запрос представляет собой запрос шифрования для шифрования полезной нагрузки. Запрос доступа включает в себя информацию доступа, полученную с использованием устройства 405-а доступа. Сервер может идентифицироваться на основе конфигурации в клиенте доступа. Например, запрос доступа может передаваться на сервер посредством конечной точки API, которая сконфигурирована в клиенте доступа.

[0087] В 430, сервер 410 может авторизовать или валидировать запрос. Авторизация

запроса включает в себя проверку местоположения устройства 405-a доступа и верификацию, что пользователь авторизован использовать систему и выполнять запрошенное действие. Местоположение может проверяться путем идентификации географического местоположения устройства 405-a доступа из IP-адреса устройства 405-a доступа и сравнения географического местоположения с набором геозон, который может идентифицировать набор стран, в которых система не может использоваться. В этом примере, пользователь верифицируется из данных в информации доступа. Например, может обеспечиваться токен доступа пользователя, который указывает, что пользователь авторизован использовать систему и выполнять запрошенное действие.

[0088] Идентификация вычислительной системы, которая отправила запрос, может удовлетворяться путем приема идентификаторов компонентов аппаратных средств или программного обеспечения, которые могут включать в себя MAC-адреса, международный идентификатор мобильного оборудования (IMEI), серийные номера и номера моделей для компонентов (материнской платы, процессора, памяти, графической карты и т.д.), номера версии программного обеспечения для операционной системы и базовой системы ввода/вывода (BIOS) и т.д. Идентификаторы для компонентов аппаратных средств и программного обеспечения вычислительной системы могут верифицироваться путем сравнения принятых идентификаторов с идентификаторами компонентов вычислительной системы, которые были ранее приняты и привязаны к пользователю, выполняющему запрос доступа.

[0089] Местоположение вычислительной системы может проверяться путем отображения IP-адреса вычислительной системы на географическое местоположение. Отображенное географическое местоположение может сравниваться с геозоной, которая идентифицирует разрешенные географические местоположения для типа доступа, специфицированного в запросе доступа. В некоторых реализациях, геозона может идентифицировать определенные страны, в которых доступ не обеспечивается. Местоположение вычислительной системы может также идентифицироваться на основе позиционирования беспроводной локальной сети (WLAN) или беспроводной глобальной сети (WWAN) (например, сотового позиционирования).

[0090] Привилегии доступа могут зависеть от типа запрашиваемого доступа. Для запроса шифрования, политики привилегий доступа к системе, которые могут применяться к каждому пользователю системы, могут проверяться, чтобы гарантировать, что пользователю, запрашивающему шифрование, разрешено это делать, на основе политик привилегий доступа к системе. Для запроса дешифрования, политики системы, которые применяются к каждому пользователю системы, политики группы, которые применяются к группам пользователей системы, политики пользователей, которые применяются к отдельным пользователям, и политики файлов, которые применяются к отдельным файлам, проверяются для верификации того, что конкретный пользователь может осуществлять доступ к конкретному файлу с конкретным уровнем привилегии. Уровни привилегий могут включать в себя полный доступ, коллаборативный доступ и доступ только для чтения.

Каждый из разных типов политик может специфицировать уровень доступа к отдельному файлу или их группам.

[0091] Авторизация запроса доступа может включать в себя сравнение информации местоположения устройства доступа из информации доступа с правилом местоположения устройства доступа, чтобы определить авторизацию доступа. Информация местоположения устройства доступа может включать в себя адрес Интернет-протокола (IP) вычислительной системы, которая отправила запрос доступа, и географическое местоположение, в которое отображается IP-адрес. Правило местоположения устройства может определять геозону, в которой доступ может быть авторизован. Геозона идентифицирует географические местоположения, где доступ может быть авторизован или может быть ограничен. В качестве примера, когда географическое местоположение для вычислительной системы сравнивается с геозоной, которая определяет область географического местоположения здания, и определено, что вычислительная система находится в пределах геозоны, доступ может указываться как авторизованный в авторизации доступа. Когда сравнение указывает, что вычислительная система не находится в пределах геозоны, авторизация доступа может указывать, что доступ не авторизован. В другом примере авторизации запроса доступа, сервер может определять, использует ли устройство доступа VPN, чтобы определить, что извлеченное отображение IP не маскирует местоположение пользователя. Таким образом, в некоторых случаях, пользователь и запрос доступа могут отклоняться, когда используется VPN.

[0092] Авторизация запроса доступа может также включать в себя сравнение информации местоположения мобильного устройства из информации доступа с правилом местоположения мобильного устройства для определения авторизации доступа. Информация местоположения мобильного устройства может включать в себя информацию спутникового позиционирования. Дополнительно или альтернативно, информация местоположения мобильного устройства может идентифицировать тип соединения между мобильным устройством и устройством доступа. Мобильное устройство может быть соединено с устройством доступа по проводному или беспроводному соединению.

[0093] Когда информация местоположения мобильного устройства включает в себя информацию спутникового позиционирования, географическое местоположение, соответствующее информации спутникового позиционирования, может сравниваться с географическим местоположением, отвечающим на IP-адрес вычислительной системы. Если географические местоположения информации спутникового позиционирования и IP-адрес согласованы, то запрос доступа может быть авторизован. В противном случае, запрос доступа может отклоняться.

[0094] Когда информация местоположения мобильного устройства включает в себя информацию соединения (которая идентифицирует тип соединения), запрос доступа может быть авторизован, когда соединение между вычислительной системой мобильного устройства было установлено и поддерживается. В качестве примера, кабель последовательной шины может использоваться для соединения мобильного устройства с

вычислительным устройством и установки проводного соединения. В качестве другого примера, беспроводное соединение может устанавливаться напрямую или опосредованно. Прямое беспроводное соединение включает в себя беспроводное сетевое соединение персональной области. Опосредованное беспроводное соединение может устанавливаться через точку беспроводного доступа, с которой соединены как мобильное устройство, так и вычислительная система.

[0095] Множество серверов могут использоваться для авторизации аспектов запроса доступа. Когда используются множество серверов, сервер может отправлять следующий запрос на следующий сервер для авторизации пользователя, идентифицированного из информации доступа. В некоторых реализациях, один сервер может авторизовать доступ к зашифрованному файлу, в то время как другой сервер может генерировать пакет доступа на основе авторизации доступа.

[0096] В 435, сервер 410 может генерировать пакет доступа. Когда он авторизован, сервер 410 генерирует пакет шифрования в ответ на запрос шифрования от устройства 405-а доступа. Пакет шифрования может генерироваться путем извлечения исходного кода для функции шифрования, генерации и хранения солей и ключей для файла, подлежащего шифрованию устройством 405-а доступа, и вставки в исходный код информации, включающей в себя соли и ключи. Генерация пакета доступа может дополнительно или альтернативно включать в себя идентификацию полезных нагрузок данных или значений, которые используются, чтобы преобразовывать данные полезной нагрузки файла.

[0097] Сервер может генерировать пакет доступа путем извлечения файлов исходного кода и вставки информации в файлы исходного кода. Вставленная информация может включать в себя соли и ключи для шифрования или дешифрования данных. Соли и ключи хранятся по отдельности и отделены от исходного кода для уменьшения влияния компрометации безопасности разных частей системы. Например, если неавторизованный пользователь имел ключ для зашифрованного файла, неавторизованный пользователь все равно не имел бы других ключей, солей или алгоритма дешифровки, требуемых для доступа к зашифрованному файлу.

[0098] В качестве примера, пакет доступа для запроса шифрования (например, пакет шифрования) может генерироваться путем получения исходного кода шифрования, модификации исходного кода шифрования при помощи набора солей и ключей для формирования модифицированного исходного кода шифрования и генерации пакета доступа при помощи модифицированного исходного кода шифрования. Аналогично, пакет доступа для запроса дешифрования (например, пакет дешифрования) может генерироваться путем получения исходного кода дешифрования, модификации исходного кода дешифрования при помощи набора солей и ключей для формирования модифицированного исходного кода дешифрования и генерации пакета доступа при помощи модифицированного исходного кода дешифрования.

[0099] В 440, пакет доступа (который представляет собой пакет шифрования) отправляется от сервера 410 на устройство 405-а доступа. Пакет доступа (как и предыдущий

запрос) отправляется по безопасной линии связи между сервером 410 и устройством 405-a доступа.

[0100] В 445, устройство 405-a доступа (посредством клиента доступа) может компилировать пакет доступа. Устройство 405-a доступа может компилировать исходный код из пакета доступа для генерации исполняемого кода, который может представлять собой динамически подключаемую библиотеку (DLL). Пакет доступа может удаляться с устройства 405-a доступа (например, из памяти устройства) после создания исполняемого кода. Пакет доступа может включать в себя исходный код, написанный на множестве языков, и использовать множество компиляторов, ассемблеров, генераторов связей и т.д. для генерации исполняемого кода из пакета доступа. В некоторых случаях, в 445, устройство 405-a доступа, вместо компиляции пакета доступа, может использовать полезную нагрузку или значения данных в пакете доступа для преобразования данных файла или полезной нагрузки, подлежащих шифрованию.

[0101] В 450, устройство 405-a доступа (посредством клиента доступа) может генерировать пакеты данных. Пакеты данных могут генерироваться как часть процесса шифрования. Пакеты данных могут включать в себя политики доступа к файлу, информацию о владении, логи доступа и тому подобное. Как описано выше, пакеты данных могут включать в себя несколько элементов информации, которые были вставлены в исходный код пакета доступа и затем сохранены в пакетах данных. В качестве примера, подпись объекта (или набор информации о владении) может вставляться в исходный код и компилироваться в исполняемый код, который сохраняет подпись объекта в пакеты данных зашифрованного файла. Аналогично, политики доступа к файлу могут вставляться в исходный код и компилироваться в исполняемый код, который сохраняет политики доступа к файлу в пакеты данных зашифрованного файла.

[0102] В 455, устройство 405-a доступа может шифровать полезную нагрузку. Полезная нагрузка может шифроваться как часть процесса шифрования, который сгенерировал пакеты данных. Зашифрованный файл генерируется из зашифрованной полезной нагрузки и пакетов данных с использованием множества солей и ключей шифрования.

[0103] В 460, устройство 405-a доступа может удалять файлы, включая исполняемый файл, после создания зашифрованного файла.

[0104] В 465, устройство 405-a доступа может передавать зашифрованный файл на устройство 405-b доступа.

[0105] Фиг. 5 иллюстрирует пример потока 500 процесса, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Конкретно, поток 500 процесса иллюстрирует операции для дешифрования файлов в соответствии с методами, описанными в настоящем документе. Поток 500 процесса включает в себя устройства 505 доступа и сервер 510, которые могут служить примерами соответствующих устройств, описанных в отношении фиг. 1-4. Например, поток 500 процесса может быть продолжением потока 400 процесса.

[0106] В 515, зашифрованный файл выбирается в устройстве 505-b доступа. Зашифрованный файл может выбираться на устройстве 505-b доступа пользователем устройства 505-b доступа. Зашифрованный файл может представлять собой файл, который был передан на устройство доступа, как описано на фиг. 4.

[0107] В 520, устройство доступа (например, посредством клиента приложения) отправляет запрос доступа на сервер 510. Запрос, также называемый запросом дешифрования, может включать в себя информацию доступа, которая идентифицирует зашифрованный файл, пользователя устройства 505-b доступа и устройство 505-b доступа. Запрос может включать в себя идентификатор зашифрованного файла, который привязан к информации прав доступа, хранящейся в пакетах данных и в макробазе данных сервера. Идентификатор зашифрованного файла может использоваться сервером для расположения информации о зашифрованном файл (включая права доступа пользователя) в макробазе данных, поддерживаемой сервером. В некоторых случаях, информация о файле может идентифицироваться из метаданных, ассоциированных с файлом. Сервер может идентифицироваться посредством конечной точки API, которая ассоциирована с файлом (например, в метаданных), или посредством конфигурации в клиенте доступа (например, клиент доступа предварительно сконфигурирован с конечной точкой API).

[0108] В 525, сервер 510 может авторизовать или валидировать запрос доступа. Сервер может авторизовать запрос доступа на основе информации, включенной в информацию запроса, поддерживаемую сервером, в ассоциации с файлом, такой как политики доступа (например, идентификаторы пользователей, которые авторизованы осуществлять доступ к файлу).

[0109] В 530, сервер 510 может генерировать пакет доступа на основе авторизации или валидации запроса доступа. Пакет доступа может представлять собой пакет дешифрования, когда запрос доступа авторизован, или может представлять собой пакет завершения или ловушки, когда запрос не авторизован.

[0110] В 535, сервер 510 может передавать пакет доступа на устройство 505-b доступа. Пакет доступа (как и предыдущий запрос) может передаваться по безопасной линии связи между сервером 510 и устройством 505-b доступа.

[0111] В 540, устройство 505-b доступа может компилировать пакет доступа. Устройство 505-b доступа (например, посредством клиента доступа) может компилировать исходный код из пакета доступа для генерации исполняемого модуля, который может представлять собой DLL. Пакет доступа может удаляться с устройства 505-b доступа после создания исполняемого модуля. В некоторых случаях, в 540, устройство 405-a доступа, вместо компиляции пакета доступа, может использовать полезную нагрузку или значения данных в пакете доступа для преобразования данных файла или полезной нагрузки, подлежащих дешифрованию.

[0112] В 545, устройство 505-b доступа может обновлять пакеты данных файла. Пакеты данных могут обновляться устройством 505-b доступа как часть процесса дешифрования путем модификации логов доступа (например, добавления информации

устройства и информации пользователя, ассоциированных с устройством 505-b доступа). В некоторых случаях, обновление пакетов данных может включать в себя обновление логов доступа к файлу на основе информации, включенной в пакет доступа. Таким образом, пакеты данных могут дешифроваться и обновляться при помощи информации доступа, которая идентифицирует дату и время доступа, и идентификатора аппаратных средств вычислительной системы, которая выполнила доступ. После обновления пакетов данных, процесс шифрования может исполняться, чтобы заново сгенерировать зашифрованный файл с обновленными пакетами данных.

[0113] В 550, устройство 505-b доступа может дешифровать полезную нагрузку зашифрованного файла. Полезная нагрузка может дешифроваться с использованием исполняемого кода как часть процесса дешифрования, который обновил пакеты данных. Зашифрованный файл дешифруется, чтобы восстановить исходную полезную нагрузку, с использованием множества солей и ключей шифрования в соответствии с исполняемым кодом пакета доступа.

[0114] В 565, устройство 505-b доступа осуществляет доступ к полезной нагрузке. Доступ к полезной нагрузке может осуществляться для представления информации из полезной нагрузки в соответствии с политиками доступа к файлу (например, правами пользователя и привилегиями) для зашифрованного файла, включенного в пакеты данных. Политики доступа к файлу могут ограничивать редактирование, сохранение, печать и просмотр информации из зашифрованного файла.

[0115] В 560, устройство 505-b доступа может удалять файлы, такие как исполняемый код, из памяти устройства 505-b доступа.

[0116] В некоторых примерах, запрос доступа в 520 передается на сервер, ассоциированный с клиентом доступа, исполняющимся на устройстве 505-b доступа. В таких случаях, сервер, ассоциированный с клиентом доступа, может указывать, что он не может валидировать запрос (например, не имеет доступа к информации файла). В таких случаях, сервер может отвечать откликом, указывающим URL для корректного сервера (например, сервера 510). В других случаях, сервер может осуществлять связь с корректным сервером 510, чтобы транслировать пакет доступа на устройство 505-b доступа.

[0117] Фиг. 6 иллюстрирует пример сценария 600 устройства доступа, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Сценарий 600 устройства доступа включает в себя устройство 605 доступа, которое может служить примером устройств доступа, описанных в отношении фиг. 1-5. Устройство 605 доступа включает в себя дисплей 610. Дисплей 610 представляет пользовательский интерфейс 615. Пользовательский интерфейс может служить примером пользовательского интерфейса, ассоциированного с клиентом доступа, который исполняется на устройстве 605 доступа.

[0118] В примере Фиг. 6, клиент доступа осуществляет доступ к файлу (например, файл дешифруется в соответствии с методами, описанными в настоящем документе). Пакет данных, ассоциированный с файлом, включает в себя политику доступа к файлу, которая

представляет собой политику доступа близости мобильного устройства, которая указывает, что мобильное пользовательское устройство должно иметь соединение с устройством 605 доступа, чтобы пользователь мог просмотреть полезную нагрузку. Таким образом, клиент доступа принудительно обеспечивает выполнение политики доступа близости мобильного устройства на фиг. 6.

[0119] В 625, пользовательский интерфейс 615 отображает информацию (например, полезную нагрузку) из зашифрованного файла, когда присутствует соединение данных с мобильным устройством 620. Когда соединение с мобильным устройством 620 потеряно, информация больше не отображается устройством 605 доступа. В качестве примера, устройство 605 доступа может представлять собой стационарный компьютер, и мобильное устройство 620 может представлять собой смартфон. Устройство 605 доступа и мобильное устройство 620 расположены достаточно близко для соединения с использованием одного из множества стандартов соединения устройств (универсальная последовательная шина (USB), Wi-Fi, Bluetooth и т.д.). Затем мобильное устройство помещается достаточно далеко от устройства 605 доступа, так что соединение больше не может поддерживаться. После нарушения соединения, информация, которая была представлена, может исчезать с дисплея, поскольку клиент доступа обеспечивает принудительное выполнение политики доступа к файлу на основе близости мобильного устройства. Дополнительно, зашифрованный файл может закрываться, и исполняемый код, используемый для дешифрования зашифрованного файла, может удаляться из устройства 605 доступа. В некоторых случаях, соединение периодически проверяется (например, каждую секунду), чтобы обеспечить выполнение политики, включенной в ассоциированный пакет данных. Таким образом, методы согласно фиг. 6 могут включать в себя дополнительные защитные механизмы.

[0120) Фиг. 7 показывает блок-схему 700 пользовательского устройства 720, которое поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Пользовательское устройство 720 может служить примером аспектов устройства доступа (например, пользовательского устройства), как описано со ссылкой на фиг. 1-6. Пользовательское устройство 720 или его различные компоненты могут служить примером средства для выполнения различных аспектов управления зашифрованным файлом как описано в настоящем документе. Например, пользовательское устройство 720 может включать в себя интерфейс 725 запроса доступа, интерфейс 730 пакета доступа, компонент 735 исполнения, компонент 740 удаления пакета доступа, компонент 745 шифрования, компонент 750 дешифрования, компонент 755 политики, компонент 760 информации валидации, компонент 765 метаданных файла, компонент 770 лога доступа или любую их комбинацию. Каждый из этих компонентов может осуществлять связь, напрямую или опосредованно, друг с другом (например, посредством одной или более шин).

[0121] Пользовательское устройство 720 может поддерживать защиту данных в клиенте доступа в соответствии с примерами, как раскрыто в настоящем документе.

Интерфейс 725 запроса доступа может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Интерфейс 730 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для приема, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Компонент 735 исполнения может быть сконфигурирован, чтобы поддерживать средство для исполнения, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Компонент 740 удаления пакета доступа может быть сконфигурирован, чтобы поддерживать средство для удаления пакета доступа из памяти, ассоциированной с клиентом доступа.

[0122] В некоторых примерах, чтобы поддерживать передачу запроса доступа, компонент 745 шифрования может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, запроса шифрования и информации файла.

[0123] В некоторых примерах, чтобы поддерживать прием пакета доступа, интерфейс 730 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для приема пакета доступа, который включает в себя пакет данных, содержащий указание одной или более политик доступа к файлу, ассоциированных с файлом, причем пакет данных зашифрован с файлом с использованием одного или более ключей доступа. В некоторых примерах, одна или более политик доступа к файлу включают в себя доступ для чтения, доступ для записи, ограничения на отображение или их комбинацию.

[0124] В некоторых примерах, чтобы поддерживать прием пакета доступа, интерфейс 730 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для приема пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем пакет данных зашифрован с файлом с использованием одного или более ключей доступа.

[0125] В некоторых примерах, чтобы поддерживать передачу запроса шифрования, компонент 755 политики может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, указания одной или более политик доступа к файлу, ассоциированных с файлом.

[0126] В некоторых примерах, чтобы поддерживать исполнение исполняемого кода, компонент 745 шифрования может быть сконфигурирован, чтобы поддерживать средство для шифрования, с использованием исполняемого кода, полезной нагрузки и одного или более пакетов данных с использованием одного или более ключей доступа для генерации зашифрованного файла.

[0127] В некоторых примерах, чтобы поддерживать шифрование одного или более пакетов данных, компонент 745 шифрования может быть сконфигурирован, чтобы поддерживать средство для шифрования одного или более пакетов данных, которые включают в себя указание одной или более политик доступа к файлу, информацию о

владении файлом, лог аудита доступа к файлу или их комбинацию.

[0128] В некоторых примерах, чтобы поддерживать передачу запроса доступа, компонент 750 дешифрования может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл.

[0129] В некоторых примерах, чтобы поддерживать прием пакета доступа, интерфейс 730 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для приема пакета доступа, который включает в себя пакет данных, содержащий одну или более обновленных политик доступа к файлу.

[0130] В некоторых примерах, компонент 760 информации валидации может быть сконфигурирован, чтобы поддерживать средство для идентификации, в клиенте доступа, информации валидации, которая включает в себя информацию клиента доступа, информацию компьютера, информацию устройства, информацию географического местоположения, токен аутентификации или их комбинацию, причем запрос дешифрования включает в себя указание информации валидации.

[0131] В некоторых примерах, компонент 765 метаданных файла может быть сконфигурирован, чтобы поддерживать средство для идентификации, что файл ассоциирован с клиентом доступа, на основе, по меньшей мере частично, метаданных, ассоциированных с файлом, причем файл включает в себя полезную нагрузку, зашифрованную с использованием первого ключа из одного или более ключей доступа, и один или более зашифрованных пакетов данных, которые зашифрованы с использованием по меньшей мере одного второго ключа из одного или более ключей доступа, причем запрос дешифрования передается на сервер на основе того, по меньшей мере частично, что файл ассоциирован с клиентом доступа.

[0132] В некоторых примерах, чтобы поддерживать исполнение исполняемого кода, компонент 750 дешифрования может быть сконфигурирован, чтобы поддерживать средство для дешифрования файла с использованием одного или более ключей доступа.

[0133] В некоторых примерах, компонент 750 дешифрования может быть сконфигурирован, чтобы поддерживать средство для отображения, в клиенте доступа, полезной нагрузки файла в соответствии с одной или более политиками доступа, ассоциированными с файлом.

[0134] В некоторых примерах, одна или более политик доступа включают в себя доступ для чтения, доступ для записи, ограничения на отображение или их комбинацию. В некоторых примерах, одна или более политик доступа включены в пакет данных, который был дешифрован с файлом с использованием одного или более ключей доступа.

[0135] В некоторых примерах, компонент 770 лога доступа может быть сконфигурирован, чтобы поддерживать средство для обновления лога аудита доступа к файлу, чтобы он включал в себя информацию устройства, ассоциированную с клиентом доступа, информацию пользователя, информацию географического местоположения или их комбинацию.

[0136] В некоторых примерах, компонент 750 дешифрования может быть сконфигурирован, чтобы поддерживать средство для идентификации, на основе, по меньшей мере частично, дешифрования файла, полезной нагрузки и одного или более пакетов данных в файле, причем один или более пакетов данных включают в себя указание одной или более политик доступа к файлу, информацию о владении, лог аудита доступа к файлу или их комбинацию.

[0137] В некоторых примерах, компонент 735 исполнения может быть сконфигурирован, чтобы поддерживать средство для создания, в памяти, ассоциированной с клиентом доступа и на основе, по меньшей мере частично, исполнения исполняемого кода, объекта доступа, который используется, чтобы дешифровать или шифровать файл, причем объект доступа удаляется из памяти, ассоциированной с клиентом доступа, после дешифрования или шифрования файла.

[0138] В некоторых примерах, компонент 750 дешифрования может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы перезаписывать содержимое файла.

[0139] В некоторых примерах, чтобы поддерживать передачу запроса доступа, интерфейс 725 запроса доступа может быть сконфигурирован, чтобы поддерживать средство для передачи запроса доступа, который включает в себя информацию доступа, содержащую географическое местоположение пользовательского устройства, исполняющего клиент доступа, информацию устройства, ассоциированную с пользовательским устройством, информацию сети, ассоциированную с пользовательским устройством, токен аутентификации, ассоциированный с клиентом доступа, или их комбинацию.

[0140] Фиг. 8 показывает диаграмму системы 800, включающей в себя устройство 805, которое поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Устройство 805 может включать в себя компоненты для двунаправленной голосовой связи и передачи данных, включая компоненты для передачи и приема коммуникаций, такие как менеджер 820 защиты данных, модуль 810 связи, антенну 815, компонент 825 пользовательского интерфейса, базу данных (данные приложения) 830, память 835 и процессор 840. Эти компоненты могут быть в электронной коммуникации или иным образом соединены (например, операционно, коммуникативно, функционально, электронно, электрически) посредством одной или более шин (например, шины 845). Устройство 805 может служить примером пользовательского устройства, которое исполняет клиент доступа, как описано в настоящем документе. В некоторых случаях, клиент доступа может соответствовать менеджеру 820 защиты данных.

[0141] Модуль 810 связи может управлять сигналами ввода и вывода для устройства 805 посредством антенны 815. Модуль 810 связи может включать в себя пример модуля 810 связи пользовательского устройства 106, показанного и описанного на фиг. 2. В этом отношении, модуль 810 связи может управлять связью с сервером 110, как

проиллюстрировано на фиг. 2. Модуль 810 связи может также управлять периферийными устройствами, не интегрированными в устройство 805. В некоторых случаях, модуль 810 связи может представлять физическое соединение или порт во внешнее периферийное устройство. В некоторых случаях, модуль 810 связи может использовать операционную систему, такую как iOS®, ANDROID®, MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, LINUX® или другую известную операционную систему. В других случаях, модуль 810 связи может представлять или взаимодействовать с модемом, клавиатурой, мышью, тачскрином или аналогичным устройством. В некоторых случаях, модуль 810 связи может быть реализован как часть процессора 840. В некоторых примерах, пользователь может взаимодействовать с устройством 805 посредством модуля 810 связи, компонента 825 пользовательского интерфейса или посредством компонентов аппаратных средств, которыми управляет модуль 810 связи.

[0142] В некоторых случаях, устройство 805 может включать в себя одну антенну 815. Однако, в некоторых других случаях, устройство 805 может иметь более одной антенны 815, которые могут одновременно передавать или принимать множество беспроводных передач. Модуль 810 связи может осуществлять связь двунаправленно, посредством одной или более антенн 815, проводных или беспроводных линий связи, как описано в настоящем документе. Например, модуль 810 связи может представлять беспроводной приемопередатчик и может осуществлять связь двунаправленно с другим беспроводным приемопередатчиком. Модуль 810 связи может также включать в себя модем для модулирования пакетов, для подачи модулированных пакетов на одну или более антенн 815 для передачи и для демодуляции пакетов, принятых от одной или более антенн 815.

[0143] Компонент 825 пользовательского интерфейса может управлять хранением и обработкой данных в базе данных 830. В некоторых случаях, пользователь может взаимодействовать с компонентом 825 пользовательского интерфейса. В других случаях, компонент 825 пользовательского интерфейса может работать автоматически без взаимодействия пользователя. База данных 830 может служить примером единичной базы данных, распределенной базы данных, множества распределенных баз данных, хранилища данных, озера данных или базы данных аварийных резервных копий.

[0144] Память 835 может включать в себя память с произвольным доступом (RAM) и постоянную память (ROM). Память 835 может хранить считываемое компьютером, исполняемое компьютером программное обеспечение, включающее в себя инструкции, которые, при исполнении, побуждают процессор 840 выполнять различные функции, описанные в настоящем документе. В некоторых случаях, память 835 может содержать, помимо прочего, BIOS, который может управлять работой базовых аппаратных средств или программного обеспечения, такой как взаимодействие с периферийными компонентами или устройствами.

[0145] Процессор 840 может включать в себя умное аппаратное устройство (например, универсальный процессор, DSP, CPU, микроконтроллер, ASIC, FPGA, программируемое логическое устройство, дискретный компонент вентильной или

транзисторной логики, дискретный аппаратный компонент или любую их комбинацию). В некоторых случаях, процессор 840 может быть сконфигурирован, чтобы управлять массивом памяти с использованием контроллера памяти. В других случаях, контроллер памяти может быть интегрирован в процессор 840. Процессор 840 может быть сконфигурирован, чтобы исполнять считываемые компьютером инструкции, хранящиеся в памяти 835, чтобы выполнять различные функции (например, функции или задачи, поддерживающие способ и систему для алгоритмов определения стадий сна).

[0146] Менеджер 820 защиты данных может поддерживать защиту данных в клиенте доступа в соответствии с примерами, как раскрыто в настоящем документе. Например, менеджер 820 защиты данных может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Менеджер 820 защиты данных может быть сконфигурирован, чтобы поддерживать средство для приема, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Менеджер 820 защиты данных может быть сконфигурирован, чтобы поддерживать средство для исполнения, клиентом доступа, исполняемого кода, чтобы осуществлять доступ к файлу с использованием одного или более ключей доступа. Менеджер 820 защиты данных может быть сконфигурирован, чтобы поддерживать средство для удаления пакета доступа из памяти, ассоциированной с клиентом доступа.

[0147] Менеджер 820 защиты данных может включать в себя приложение (например, “app”), программу, программное обеспечение или другой компонент, который сконфигурирован, чтобы обеспечивать методы защиты данных, описанные в настоящем документе, посредством связи с сервером, другими пользовательскими устройствами и тому подобным.

[0148] Фиг. 9 показывает блок-схему 900 сервера 920, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Сервер 920 может служить примером аспектов сервера, как описано со ссылкой на фиг. 1-6. Сервер 920, или различные его компоненты, может служить примером средства для выполнения различных аспектов управления зашифрованным файлом, как описано в настоящем документе. Например, сервер 920 может включать в себя интерфейс 925 запроса доступа, компонент 930 валидации запроса, компонент 935 пакета доступа, интерфейс 940 пакета доступа, компонент 945 шифрования, компонент 950 дешифрования, компонент 955 идентификации ключа, компонент 960 политики файла, компонент 965 действия, компонент 970 уведомления или любую их комбинацию. Каждый из этих компонентов может осуществлять связь, напрямую или опосредованно, друг с другом (например, посредством одной или более шин).

[0149] Сервер 920 может поддерживать защиту данных в сервере в соответствии с примерами, как раскрыто в настоящем документе. Интерфейс 925 запроса доступа может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа,

запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Компонент 930 валидации запроса может быть сконфигурирован, чтобы поддерживать средство для валидации запроса доступа с использованием информации доступа. Компонент 935 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для генерации, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Интерфейс 940 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для передачи, на клиент доступа, пакета доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется, чтобы осуществлять доступ к файлу.

[0150] В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 945 шифрования может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа, запроса шифрования для шифрования файла, причем пакет доступа включает в себя исполняемый код для шифрования файла с использованием одного или более ключей доступа.

[0151] В некоторых примерах, чтобы поддерживать передачу пакета доступа, интерфейс 940 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий указание одной или более политик доступа к файлу, ассоциированных с файлом, причем исполняемый код сконфигурирован, чтобы шифровать пакет данных с файлом с использованием одного или более ключей доступа. В некоторых примерах, одна или более политик доступа к файлу содержат доступ для чтения, доступ для записи, ограничения отображения или их комбинацию.

[0152] В некоторых примерах, чтобы поддерживать передачу пакета доступа, компонент 935 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий исполняемый код, который сконфигурирован, чтобы генерировать лог аудита, ассоциированный с файлом, и шифровать лог аудита с файлом с использованием одного или более ключей доступа.

[0153] В некоторых примерах, чтобы поддерживать передачу пакета доступа, компонент 935 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем исполняемый код сконфигурирован, чтобы шифровать пакет данных с файлом с использованием одного или более ключей доступа.

[0154] В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 960 политики файла может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа, указания одной или более политик доступа к файлу, ассоциированных с файлом. В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 960 политики файла может быть сконфигурирован, чтобы

поддерживать средство для хранения, в ассоциации с идентификатором файла для файла, одной или более политик доступа к файлу.

[0155] В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 960 политики файла может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа, указания одного или более пользователей, которые авторизованы осуществлять доступ к файлу. В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 960 политики файла может быть сконфигурирован, чтобы поддерживать средство для хранения, в ассоциации с идентификатором файла для файла, указания одного или более пользователей, которые авторизованы осуществлять доступ к файлу.

[0156) В некоторых примерах, чтобы поддерживать прием запроса доступа, компонент 950 дешифрования может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа, запроса дешифрования для дешифрования файла, причем пакет доступа включает в себя исполняемый код для дешифрования файла с использованием одного или более ключей доступа.

[0157] В некоторых примерах, компонент 960 политики файла может быть сконфигурирован, чтобы поддерживать средство для определения, что пакет данных, который содержит одну или более политик доступа к файлу для файла, является устаревшим. В некоторых примерах, компонент 960 политики файла может быть сконфигурирован, чтобы поддерживать средство для передачи, на основе, по меньшей мере частично, определения, что пакет данных является устаревшим, обновленного пакета данных, который включает в себя одну или более обновленных политик доступа к файлу для файла.

[0158] В некоторых примерах, компонент 930 валидации запроса может быть сконфигурирован, чтобы поддерживать средство для сравнения, в сервере, информации пользователя, которая включена в информацию доступа, принятую в запросе дешифрования, с записью доступа, ассоциированной с файлом. В некоторых примерах, компонент 930 валидации запроса может быть сконфигурирован, чтобы поддерживать средство для определения, что пользователь, ассоциированный с клиентом доступа, авторизован осуществлять доступ к файлу, на основе, по меньшей мере частично, результата сравнения, причем пакет доступа передается на клиент доступа на основе, по меньшей мере частично, определения, что пользователь авторизован осуществлять доступ к файлу.

[0159] В некоторых примерах, компонент 930 валидации запроса может быть сконфигурирован, чтобы поддерживать средство для определения, что клиент доступа не авторизован дешифровать файл, на основе, по меньшей мере частично, информации доступа, принятой в запросе дешифрования. В некоторых примерах, компонент 965 действия может быть сконфигурирован, чтобы поддерживать средство для запуска, в сервере, действия на основе, по меньшей мере частично, определения, что клиент доступа не авторизован дешифровать файл.

[0160] В некоторых примерах, чтобы поддерживать запуск действия, компонент 970 уведомления может быть сконфигурирован, чтобы поддерживать средство для генерации оповещения или сообщения, указывающего, что клиент доступа передал неавторизованной запрос доступа.

[0161] В некоторых примерах, чтобы поддерживать запуск действия, компонент 935 пакета доступа может быть сконфигурирован, чтобы поддерживать средство для передачи пакета доступа, который включает в себя исполняемый код для перезаписи содержимого файла.

[0162] В некоторых примерах, компонент 955 идентификации ключа может быть сконфигурирован, чтобы поддерживать средство для передачи, на сервис хранения ключей и на основе, по меньшей мере частично, приема запроса доступа, запроса строки ключа и идентификатора файла, ассоциированного с файлом. В некоторых примерах, компонент 955 идентификации ключа может быть сконфигурирован, чтобы поддерживать средство для приема, от сервиса хранения ключей, строки ключа, ассоциированной с идентификатором файла. В некоторых примерах, компонент 955 идентификации ключа может быть сконфигурирован, чтобы поддерживать средство для генерации одного или более ключей доступа с использованием строки ключа.

[0163] В некоторых примерах, чтобы поддерживать валидацию запроса доступа, компонент 930 валидации запроса может быть сконфигурирован, чтобы поддерживать средство для валидации информации доступа, которая включает в себя географическое местоположение пользовательского устройства, исполняющего клиент доступа, информации устройства, ассоциированной с пользовательским устройством, информации сети, ассоциированной с пользовательским устройством, токена аутентификации, ассоциированного с клиентом доступа, или их комбинации.

[0164] Фиг. 10 показывает диаграмму системы 1000, включающей в себя устройство 1005, которое поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Устройство 1005 может включать в себя компоненты для двунаправленной голосовой связи и передачи данных, включая компоненты для связи передачи и приема, такие как компонент 1020 защиты данных, контроллер 1010 I/O, контроллер 1015 базы данных, память 1025, процессор 1030 и базу данных 1035. Эти компоненты могут состоять в электронной коммуникации или иным образом соединены (например, оперативно, коммуникативно, функционально, электронно, электрически) посредством одной или более шин (например, шины 1040).

[0165] Контроллер 1010 I/O может управлять сигналами 1045 ввода и сигналами 1050 вывода для устройства 1005. Контроллер 1010 I/O может также администрировать периферийные устройства, не интегрированные в устройство 1005. В некоторых случаях, контроллер 1010 I/O может представлять физическое соединение или порт для внешнего периферийного устройства. В некоторых случаях, контроллер 1010 I/O может использовать операционную систему, такую как iOS®, ANDROID®, MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, LINUX® или другую известную операционную систему. В других случаях,

контроллер 1010 I/O может представлять или взаимодействовать с модемом, клавиатурой, мышью, тачскрином или аналогичным устройством. В некоторых случаях, контроллер 1010 I/O может быть реализован как часть процессора 1030. В некоторых примерах, пользователь может взаимодействовать с устройством 1005 посредством контроллера 1010 I/O или посредством аппаратных компонентов, которыми управляет контроллер 1010 I/O.

[0166] Контроллер 1015 базы данных может управлять хранением и обработкой данных в базе данных 1035. В некоторых случаях, пользователь может взаимодействовать с контроллером 1015 базы данных. В других случаях, контроллер 1015 базы данных может работать автоматически без взаимодействия пользователя. База данных 1035 может служить примером одиночной базы данных, распределенной базы данных, множества распределенных баз данных, хранилища данных, озера данных или базы данных аварийных резервных копий.

[0167] Память 1025 может включать в себя RAM и ROM. Память 1025 может хранить считываемое компьютером, исполняемое компьютером программное обеспечение, включающее в себя инструкции, которые, при исполнении, побуждают процессор 1030 выполнять различные функции, описанные в настоящем документе. В некоторых случаях, память 1025 может содержать, помимо прочего, BIOS, который может управлять работой базовых аппаратных средств или программного обеспечения, такой как взаимодействие с периферийными компонентами или устройствами.

[0168] Процессор 1030 может включать в себя умное аппаратное устройство (например, универсальный процессор, DSP, CPU, микроконтроллер, ASIC, FPGA, программируемое логическое устройство, дискретный компонент вентильной или транзисторной логики, дискретный аппаратный компонент или любую их комбинацию). В некоторых случаях, процессор 1030 может быть сконфигурирован, чтобы управлять массивом памяти с использованием контроллера памяти. В других случаях, контроллер памяти может быть интегрирован в процессор 1030. Процессор 1030 может быть сконфигурирован, чтобы исполнять считываемые компьютером инструкции, хранящиеся в памяти 1025, для выполнения различных функций (например, функций или задач, поддерживающих управление зашифрованным файлом).

[0169] Компонент 1020 защиты данных может поддерживать защиту данных в сервере в соответствии с примерами, как раскрыто в настоящем документе. Например, компонент 1020 защиты данных может быть сконфигурирован, чтобы поддерживать средство для приема, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Компонент 1020 защиты данных может быть сконфигурирован, чтобы поддерживать средство для валидации запроса доступа с использованием информации доступа. Компонент 1020 защиты данных может быть сконфигурирован, чтобы поддерживать средство для генерации, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Компонент 1020 защиты данных может быть сконфигурирован,

чтобы поддерживать средство для передачи, на клиент доступа, пакета доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется, чтобы осуществлять доступ к файлу.

[0170] Фиг. 11 показывает блок-схему последовательности операций, иллюстрирующую способ 1100, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1100 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1100 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0171] В 1105, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1105 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1105 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0172] В 1110, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1110 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1110 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7. В некоторых примерах, пакет доступа включает в себя один или более ключей доступа и/или информацию доступа, такую как данные или значения, а не исполняемый код.

[0173] В 1115, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1115 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1115 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7. В примерах, когда пакет доступа включает в себя один или более ключей доступа и/или информацию доступа, устройство доступа может использовать информацию доступа, чтобы осуществлять доступ к данным полезной нагрузки путем преобразования данных, которое может соответствовать шифрованию или дешифрованию данные. В некоторых случаях, этот процесс может включать в себя исполнение инструкций, доступ к которым осуществляется клиентом доступа. Эти инструкции могут или не могут быть включены в пакет доступа.

[0174] В 1120, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1120 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1120 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0175] Фиг. 12 показывает блок-схему последовательности операций, иллюстрирующую способ 1200, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1200 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1200 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0176] В 1205, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1205 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1205 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0177] В 1210, способ может включать в себя передачу, на сервер, запроса шифрования и информации файла. Операции 1210 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1210 могут выполняться компонентом 745 шифрования, как описано со ссылкой на фиг. 7.

[0178] В 1215, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1215 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1215 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0179] В 1220, способ может включать в себя прием пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем пакет данных зашифрован с файлом с использованием одного или более ключей доступа. Операции 1220 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1220 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0180] В 1225, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1225 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1225 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0181] В 1230, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1230 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1230 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0182] Фиг. 13 показывает блок-схему последовательности операций, иллюстрирующую способ 1300, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1300 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1300 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0183] В 1305, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1305 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1305 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0184] В 1310, способ может включать в себя передачу, на сервер, запроса шифрования и информации файла. Операции 1310 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1310 могут выполняться компонентом 745 шифрования, как описано со ссылкой на фиг. 7.

[0185] В 1315, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1315 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1315 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0186] В 1320, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более

ключей доступа. Операции 1320 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1320 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0187] В 1325, способ может включать в себя шифрование, с использованием исполняемого кода, полезной нагрузки и одного или более пакетов данных с использованием одного или более ключей доступа для генерации зашифрованного файла. Операции 1325 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1325 могут выполняться компонентом 745 шифрования, как описано со ссылкой на фиг. 7.

[0188] В 1330, способ может включать в себя шифрование одного или более пакетов данных, которые включают в себя указание одной или более политик доступа к файлу, информацию о владении файлом, лог аудита доступа к файлу или их комбинацию. Операции 1330 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1330 могут выполняться компонентом 745 шифрования, как описано со ссылкой на фиг. 7.

[0189] В 1335, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1335 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1335 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0190] Фиг. 14 показывает блок-схему последовательности операций, иллюстрирующую способ 1400, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1400 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1400 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0191] В 1405, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1405 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1405 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0192] В 1410, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1410 могут

выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1410 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0193] В 1415, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1415 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1415 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0194] В 1420, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1420 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1420 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0195] В 1425, способ может включать в себя передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл. Операции 1425 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1425 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0196] Фиг. 15 показывает блок-схему последовательности операций, иллюстрирующую способ 1500, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1500 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1500 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0197] В 1505, способ может включать в себя идентификацию, в клиенте доступа, информации валидации, которая включает в себя информацию клиента доступа, информацию компьютера, информацию устройства, информацию географического местоположения, токен аутентификации или их комбинацию, причем запрос дешифрования включает в себя указание информации валидации. Операции 1505 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1505 могут выполняться компонентом 760 информации валидации, как описано со ссылкой на фиг. 7.

[0198] В 1510, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому

необходимо осуществить доступ. Операции 1510 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1510 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0199] В 1515, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1515 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1515 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0200] В 1520, способ может включать в себя прием пакета доступа, который включает в себя пакет данных, содержащий одну или более обновленных политик доступа к файлу. Операции 1520 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1520 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0201] В 1525, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1525 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1525 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0202] В 1530, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1530 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1530 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0203] В 1535, способ может включать в себя передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл. Операции 1535 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1535 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0204] Фиг. 16 показывает блок-схему последовательности операций, иллюстрирующую способ 1600, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1600 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1600 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может

выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0205] В 1605, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1605 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1605 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0206] В 1610, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1610 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1610 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг 7.

[0207] В 1615, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1615 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1615 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0208] В 1620, способ может включать в себя дешифрование файла с использованием одного или более ключей доступа. Операции 1620 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1620 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0209] В 1625, способ может включать в себя отображение, в клиенте доступа, полезной нагрузки файла в соответствии с одной или несколькими политиками доступа, ассоциированными с файлом. Операции 1625 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1625 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0210] В 1630, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1630 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1630 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0211] В 1635, способ может включать в себя передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл. Операции 1635 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1635 могут выполняться компонентом 750 дешифрования, как описано

со ссылкой на фиг. 7.

[0212] Фиг. 17 показывает блок-схему последовательности операций, иллюстрирующую способ 1700, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1700 могут быть реализованы пользовательским устройством или его компонентами, как описано в настоящем документе. Например, операции способа 1700 могут выполняться пользовательским устройством, как описано со ссылкой на фиг. 1-8. В некоторых примерах, пользовательское устройство может исполнять набор инструкций, чтобы управлять функциональными элементами пользовательского устройства для выполнения описанных функций. Дополнительно или альтернативно, пользовательское устройство может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0213] В 1705, способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1705 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1705 могут выполняться интерфейсом 725 запроса доступа, как описано со ссылкой на фиг. 7.

[0214] В 1710, способ может включать в себя прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1710 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1710 могут выполняться интерфейсом 730 пакета доступа, как описано со ссылкой на фиг. 7.

[0215] В 1715, способ может включать в себя исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа. Операции 1715 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1715 могут выполняться компонентом 735 исполнения, как описано со ссылкой на фиг. 7.

[0216] В 1720, способ может включать в себя дешифрование файла с использованием одного или более ключей доступа. Операции 1720 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1720 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0217] В 1725, способ может включать в себя обновление лога аудита доступа к файлу, чтобы он включал в себя информацию устройства, ассоциированную с клиентом доступа, информацию пользователя, информацию географического местоположения или их комбинацию. Операции 1725 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1725 могут выполняться компонентом 770 лога доступа, как описано со ссылкой на фиг. 7.

[0218] В 1730, способ может включать в себя удаление пакета доступа из памяти, ассоциированной с клиентом доступа. Операции 1730 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1730 могут выполняться компонентом 740 удаления пакета доступа, как описано со ссылкой на фиг. 7.

[0219] В 1735, способ может включать в себя передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл. Операции 1735 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1735 могут выполняться компонентом 750 дешифрования, как описано со ссылкой на фиг. 7.

[0220] Фиг. 18 показывает блок-схему последовательности операций, иллюстрирующую способ 1800, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1800 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 1800 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0221] В 1805, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1805 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1805 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0222] В 1810, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 1810 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1810 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0223] В 1815, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1815 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1815 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9. В некоторых примерах, генерация пакета доступа может включать в себя идентификацию одного или более ключей доступа и/или информации доступа, такой как данные или значения, а не исполняемый код.

[0224] В 1820, способ может включать в себя передачу, на клиент доступа, пакета

доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 1820 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1820 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9. Когда пакет доступа включает в себя информацию доступа, клиент доступа может использовать информацию доступа, чтобы осуществлять доступ к данным полезной нагрузки путем преобразования данных, которое может соответствовать шифрованию или дешифрованию данных. В некоторых случаях, этот процесс может включать в себя исполнение инструкций, доступ к которым осуществляется клиентом доступа. Эти инструкции могут или не могут быть включены в пакет доступа.

[0225] Фиг. 19 показывает блок-схему последовательности операций, иллюстрирующую способ 1900, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 1900 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 1900 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0226] В 1905, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 1905 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1905 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0227] В 1910, способ может включать в себя прием, от клиента доступа, запроса шифрования для шифрования файла, причем пакет доступа включает в себя исполняемый код для шифрования файла с использованием одного или более ключей доступа. Операции 1910 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1910 могут выполняться компонентом 945 шифрования, как описано со ссылкой на фиг. 9.

[0228] В 1915, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 1915 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1915 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0229] В 1920, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 1920 могут выполняться в

соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1920 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0230] В 1925, способ может включать в себя передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется клиентом доступа в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 1925 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1925 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9.

[0231] В 1930, способ может включать в себя передачу, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий указание одной или нескольких политик доступа к файлу, ассоциированных с файлом, причем исполняемый код сконфигурирован, чтобы шифровать пакет данных с файлом с использованием одного или более ключей доступа. Операции 1930 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1930 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг 9.

[0232] В 1935, способ может включать в себя передачу, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий исполняемый код, который сконфигурирован, чтобы генерировать лог аудита, ассоциированный с файлом, и шифровать лог аудита с файлом с использованием одного или более ключей доступа. Операции 1935 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 1935 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0233] Фиг. 20 показывает блок-схему последовательности операций, иллюстрирующую способ 2000, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 2000 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 2000 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0234] В 2005, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 2005 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2005 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0235] В 2010, способ может включать в себя прием, от клиента доступа, запроса шифрования для шифрования файла, причем пакет доступа включает в себя исполняемый

код для шифрования файла с использованием одного или более ключей доступа. Операции 2010 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2010 могут выполняться компонентом 945 шифрования, как описано со ссылкой на фиг. 9.

[0236] В 2015, способ может включать в себя прием, от клиента доступа, указания одной или более политик доступа к файлу, ассоциированных с файлом. Операции 2015 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2015 могут выполняться компонентом 960 политики файла, как описано со ссылкой на фиг. 9.

[0237] В 2020, способ может включать в себя хранение, в ассоциации с идентификатором файла для файла, одной или более политик доступа к файлу. Операции 2020 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2020 могут выполняться компонентом 960 политики файла, как описано со ссылкой на фиг. 9.

[0238] В 2025, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 2025 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2025 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0239] В 2030, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 2030 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2030 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0240] В 2035, способ может включать в себя передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется клиентом доступа в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 2035 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2035 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9.

[0241] Фиг. 21 показывает блок-схему последовательности операций, иллюстрирующую способ 2100, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 2100 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 2100 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0242] В 2105, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 2105 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2105 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0243] В 2110, способ может включать в себя прием, от клиента доступа, указания одного или более пользователей, которые авторизованы осуществлять доступ к файлу. Операции 2110 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2110 могут выполняться компонентом 960 политики файла, как описано со ссылкой на фиг. 9.

[0244] В 2115, способ может включать в себя прием, от клиента доступа, запроса шифрования для шифрования файла, причем пакет доступа включает в себя исполняемый код для шифрования файла с использованием одного или более ключей доступа. Операции 2115 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2115 могут выполняться компонентом 945 шифрования, как описано со ссылкой на фиг. 9.

[0245] В 2120, способ может включать в себя хранение, в ассоциации с идентификатором файла для файла, указания одного или более пользователей, которые авторизованы осуществлять доступ к файлу. Операции 2120 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2120 могут выполняться компонентом 960 политики файла, как описано со ссылкой на фиг. 9.

[0246] В 2125, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 2125 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2125 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0247] В 2130, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 2130 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2130 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0248] В 2135, способ может включать в себя передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется клиентом доступа в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 2135 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2135 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9.

[0249] Фиг. 22 показывает блок-схему последовательности операций, иллюстрирующую способ 2200, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 2200 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 2200 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0250] В 2205, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 2205 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2205 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0251] В 2210, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 2210 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2210 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0252] В 2215, способ может включать в себя сравнение, на сервере, информации пользователя, которая включена в информацию доступа, принятую в запросе дешифрования, с записью доступа, ассоциированной с файлом. Операции 2215 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2215 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0253] В 2220, способ может включать в себя определение, что пользователь, ассоциированный с клиентом доступа, авторизован осуществлять доступ к файлу, на основе, по меньшей мере частично, результата сравнения, причем пакет доступа передается на клиент доступа на основе, по меньшей мере частично, определения, что пользователь авторизован осуществлять доступ к файлу. Операции 2220 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2220 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0254] В 2225, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 2225 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2225 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0255] В 2230, способ может включать в себя передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется клиентом доступа в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 2230 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2230 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9.

[0256] В 2235, способ может включать в себя прием, от клиента доступа, запроса дешифрования для дешифрования файла, причем пакет доступа включает в себя исполняемый код для дешифрования файла с использованием одного или более ключей доступа. Операции 2235 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2235 могут выполняться компонентом 950 дешифрования, как описано со ссылкой на фиг. 9.

[0257] Фиг. 23 показывает блок-схему последовательности операций, иллюстрирующую способ 2300, который поддерживает управление зашифрованным файлом в соответствии с аспектами настоящего раскрытия. Операции способа 2300 могут быть реализованы сервером или его компонентами, как описано в настоящем документе. Например, операции способа 2300 могут выполняться сервером, как описано со ссылкой на фиг. 1-6 и 9 и 10. В некоторых примерах, сервер может исполнять набор инструкций, чтобы управлять функциональными элементами сервера для выполнения описанных функций. Дополнительно или альтернативно, сервер может выполнять аспекты описанных функций с использованием специализированных аппаратных средств.

[0258] В 2305, способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ. Операции 2305 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2305 могут выполняться интерфейсом 925 запроса доступа, как описано со ссылкой на фиг. 9.

[0259] В 2310, способ может включать в себя валидацию запроса доступа с использованием информации доступа. Операции 2310 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2310 могут выполняться компонентом 930 валидации запроса, как описано со ссылкой на фиг. 9.

[0260] В 2315, способ может включать в себя генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа. Операции 2315 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2315 могут выполняться компонентом 935 пакета доступа, как описано со ссылкой на фиг. 9.

[0261] В 2320, способ может включать в себя передачу, на сервис хранения ключей и на основе, по меньшей мере частично, приема запроса доступа, запроса строки ключа и

идентификатора файла, ассоциированного с файлом. Операции 2320 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2320 могут выполняться компонентом 955 идентификации ключа, как описано со ссылкой на фиг. 9.

[0262] В 2325, способ может включать в себя прием, от сервиса хранения ключей, строки ключа, ассоциированной с идентификатором файла. Операции 2325 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2325 могут выполняться компонентом 955 идентификации ключа, как описано со ссылкой на фиг. 9.

[0263] В 2330, способ может включать в себя генерацию одного или более ключей доступа с использованием строки ключа. Операции 2330 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2330 могут выполняться компонентом 955 идентификации ключа, как описано со ссылкой на фиг. 9.

[0264] В 2335, способ может включать в себя передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется, чтобы осуществлять доступ к файлу. Операции 2335 могут выполняться в соответствии с примерами, как раскрыто в настоящем документе. В некоторых примерах, аспекты операций 2335 могут выполняться интерфейсом 940 пакета доступа, как описано со ссылкой на фиг. 9.

[0265] Описан способ для защиты данных в клиенте доступа. Способ может включать в себя передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа, исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа и удаление пакета доступа из памяти, ассоциированной с клиентом доступа.

[0266] Описан аппаратный компонент для защиты данных в клиенте доступа. Аппаратный компонент может включать в себя процессор, память, связанную с процессором, и инструкции, хранящиеся в памяти. Инструкции могут исполняться процессором, чтобы побуждать аппаратный компонент передавать, на сервер, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, принимать, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа, исполнять, клиентом доступа, исполняемый код для осуществления доступа к файлу с использованием одного или более ключей доступа и удалять пакет доступа из памяти, ассоциированной с клиентом доступа.

[0267] Описан другой аппаратный компонент для защиты данных в клиенте доступа. Аппаратный компонент может включать в себя средство для передачи, на сервер, запроса

доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, средство для приема, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа, средство для исполнения, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа и средство для удаления пакета доступа из памяти, ассоциированной с клиентом доступа.

[0268] Описан долговременный считываемый компьютером носитель, хранящий код для защиты данных в клиенте доступа. Код может включать в себя инструкции, исполняемые процессором, чтобы передавать, на сервер, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, принимать, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа, исполнять, клиентом доступа, исполняемый код для осуществления доступа к файлу с использованием одного или более ключей доступа и удалять пакет доступа из памяти, ассоциированной с клиентом доступа.

[0269] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, способ, аппаратные компоненты и долговременный считываемый компьютером носитель могут включать в себя дополнительные операции, признаки, средства или инструкции для передачи, на сервер, запроса шифрования и информации файла.

[0270] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием пакета доступа может включать в себя операции, признаки, средства или инструкции для приема пакета доступа, который включает в себя пакет данных, содержащий указание одной или более политик доступа к файлу, ассоциированных с файлом, причем пакет данных может быть зашифрован с файлом с использованием одного или более ключей доступа.

[0271] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, одна или более политик доступа к файлу включают в себя доступ для чтения, доступ для записи, ограничения отображения или их комбинацию.

[0272] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием пакета доступа может включать в себя операции, признаки, средства или инструкции для приема пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем пакет данных может быть зашифрован с файлом с использованием одного или более ключей доступа.

[0273] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача запроса шифрования может включать в себя операции, признаки, средства или инструкции

для передачи, на сервер, указания одной или более политик доступа к файлу, ассоциированных с файлом.

[0274] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, исполнение исполняемого кода может включать в себя операции, признаки, средства или инструкции для шифрования, с использованием исполняемого кода, полезной нагрузки и одного или более пакетов данных с использованием одного или более ключей доступа для генерации зашифрованного файла.

[0275] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, шифрование одного или более пакетов данных может включать в себя операции, признаки, средства или инструкции для шифрования одного или более пакетов данных, которые включают в себя указание одной или более политик доступа к файлу, информацию о владении файлом, лог аудита доступа к файлу или их комбинацию.

[0276] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача запроса доступа может включать в себя операции, признаки, средства или инструкции для передачи, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который может использоваться для дешифрования файла.

[0277] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием пакета доступа может включать в себя операции, признаки, средства или инструкции для приема пакета доступа, который включает в себя пакет данных, содержащий одну или более обновленных политик доступа к файлу.

[0278] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для идентификации, в клиенте доступа, информации валидации, которая включает в себя информацию клиента доступа, информацию компьютера, информацию устройства, информацию географического местоположения, токен аутентификации или их комбинацию, причем запрос дешифрования включает в себя указание информации валидации.

[0279] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для идентификации, что файл может быть ассоциирован с клиентом доступа, на основе, по меньшей мере частично, метаданных, ассоциированных с файлом, причем файл включает в себя полезную нагрузку, зашифрованную с использованием первого ключа из одного или более ключей доступа, и один или более зашифрованных пакетов данных, которые могут быть зашифрованы с использованием по меньшей мере одного второго ключа из одного

или более ключей доступа, причем запрос дешифрования может передаваться на сервер на основе того, по меньшей мере частично, что файл ассоциирован с клиентом доступа.

[0280] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, исполнение исполняемого кода может включать в себя операции, признаки, средства или инструкции для дешифрования файла с использованием одного или более ключей доступа.

[0281] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для отображения, в клиенте доступа, полезной нагрузки файла в соответствии с одной или более политиками доступа, ассоциированными с файлом.

[0282] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, одна или более политик доступа включают в себя доступ для чтения, доступ для записи, ограничения отображения или их комбинацию.

[0283] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, одна или более политик доступа могут быть включены в пакет данных, который был дешифрован с файлом с использованием одного или более ключей доступа.

[0284] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для обновления лога аудита доступа к файлу, чтобы включать информацию устройства, ассоциированную с клиентом доступа, информацию пользователя, информацию географического местоположения или их комбинацию.

[0285] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для идентификации, на основе, по меньшей мере частично, дешифрования файла, полезной нагрузки и одного или более пакетов данных в файле, причем один или более пакетов данных включают в себя указание одной или более политик доступа к файлу, информацию о владении, лог аудита доступа к файлу или их комбинацию.

[0286] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для создания, в памяти, ассоциированной с клиентом доступа, и на основе, по меньшей мере частично, исполнения исполняемого кода, объекта доступа, который может использоваться для дешифрования или шифрования файла, причем объект доступа может удаляться из памяти, ассоциированной с клиентом доступа, после дешифрования или шифрования файла.

[0287] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для передачи, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который может использоваться для перезаписи содержимого файла.

[0288] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача запроса доступа может включать в себя операции, признаки, средства или инструкции для передачи запроса доступа, который включает в себя информацию доступа, содержащую географическое местоположение пользовательского устройства, исполняющего клиент доступа, информацию устройства, ассоциированную с пользовательским устройством, информацию сети, ассоциированную с пользовательским устройством, токен аутентификации, ассоциированный с клиентом доступа, или их комбинацию.

[0289] Описан способ для защиты данных в сервере. Способ может включать в себя прием, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, валидацию запроса доступа с использованием информации доступа, генерацию, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа, и передачу, на клиент доступа, пакета доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется для доступа к файлу.

[0290] Описан аппаратный компонент для защиты данных в сервере. Аппаратный компонент может включать в себя процессор, память, связанную с процессором, и инструкции, хранящиеся в памяти. Инструкции могут исполняться процессором, чтобы побуждать аппаратный компонент принимать, от клиента доступа, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, валидировать запрос доступа с использованием информации доступа, генерировать, на основе, по меньшей мере частично, валидации запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа, и передавать, на клиент доступа, пакет доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется для доступа к файлу.

[0291] Описан другой аппаратный компонент для защиты данных в сервере. Аппаратный компонент может включать в себя средство для приема, от клиента доступа, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, средство для валидации запроса доступа с использованием информации доступа, средство для генерации, на основе, по меньшей мере частично, валидации запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа, и средство для передачи, на клиент доступа, пакета доступа, причем пакет доступа компилируется, клиентом доступа,

в исполняемый код, который используется для доступа к файлу.

[0292] Описан долговременный считываемый компьютером носитель, хранящий код для защиты данных в сервере. Код может включать в себя инструкции, исполняемые процессором, чтобы принимать, от клиента доступа, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ, валидировать запрос доступа с использованием информации доступа, генерировать, на основе, по меньшей мере частично, валидации запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа, и передавать, на клиент доступа, пакет доступа, причем пакет доступа компилируется, клиентом доступа, в исполняемый код, который используется для доступа к файлу.

[0293] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием запроса доступа может включать в себя операции, признаки, средства или инструкции для приема, от клиента доступа, запроса шифрования для шифрования файла, причем пакет доступа включает в себя исполняемый код для шифрования файла с использованием одного или более ключей доступа.

[0294] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача пакета доступа может включать в себя операции, признаки, средства или инструкции для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий указание одной или более политик доступа к файлу, ассоциированных с файлом, причем исполняемый код может быть сконфигурирован, чтобы шифровать пакет данных с файлом с использованием одного или более ключей доступа.

[0295] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, одна или более политик доступа к файлу содержат доступ для чтения, доступа для записи, отображения или их комбинацию.

[0296] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача пакета доступа может включать в себя операции, признаки, средства или инструкции для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий исполняемый код, который может быть сконфигурирован, чтобы генерировать лог аудита, ассоциированный с файлом, и шифровать лог аудита с файлом с использованием одного или более ключей доступа.

[0297] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, передача пакета доступа может включать в себя операции, признаки, средства или инструкции для передачи, на клиент доступа, пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем исполняемый код может быть сконфигурирован, чтобы шифровать пакет данных с файлом с использованием

одного или более ключей доступа.

[0298] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием запроса доступа может включать в себя операции, признаки, средства или инструкции для приема, от клиента доступа, указания одной или более политик доступа к файлу, ассоциированных с файлом, и хранения, в ассоциации с идентификатором файла для файла, одной или более политик доступа к файлу.

[0299] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием запроса доступа может включать в себя операции, признаки, средства или инструкции для приема, от клиента доступа, указания одного или более пользователей, которые могут быть авторизованы осуществлять доступ к файлу, и сохранения, в ассоциации с идентификатором файла для файла, указания одного или более пользователей, которые могут быть авторизованы осуществлять доступ к файлу.

[0300] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, прием запроса доступа может включать в себя операции, признаки, средства или инструкции для приема, от клиента доступа, запроса дешифрования для дешифрования файла, причем пакет доступа включает в себя исполняемый код для дешифрования файла с использованием одного или более ключей доступа.

[0301] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для определения, что пакет данных, который содержит одну или более политик доступа к файлу для файла, может быть устаревшим, и передачи, на основе, по меньшей мере частично, определения, что пакет данных может быть устаревшим, обновленного пакета данных, который включает в себя одну или более обновленных политик доступа к файлу для файла.

[0302] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для сравнения, в сервере, информации пользователя, которая может быть включена в информацию доступа, принятую в запросе дешифрования, с записью доступа, ассоциированной с файлом, и определения, что пользователь, ассоциированный с клиентом доступа, может быть авторизован осуществлять доступ к файлу на основе, по меньшей мере частично, результата сравнения, причем пакет доступа может передаваться на клиент доступа на основе, по меньшей мере частично, определения, что пользователь может быть авторизован осуществлять доступ к файлу.

[0303] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для

определения, что клиент доступа может не быть авторизован для дешифрования файла, на основе, по меньшей мере частично, информации доступа, принятой в запросе дешифрования, и запуска, в сервере, действия на основе, по меньшей мере частично, определения, что клиент доступа может не быть авторизован для дешифрования файла.

[0304] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, запуск действия может включать в себя операции, признаки, средства или инструкции для генерации оповещения или сообщения, указывающего, что клиент доступа передал неавторизованный запрос доступа.

[0305] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, запуск действия может включать в себя операции, признаки, средства или инструкции для передачи пакета доступа, который включает в себя исполняемый код для перезаписи содержимого файла.

[0306] Некоторые примеры способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, могут дополнительно включать в себя операции, признаки, средства или инструкции для передачи, на сервис хранения ключей и на основе, по меньшей мере частично, приема запроса доступа, запроса строки ключа и идентификатора файла, ассоциированного с файлом, приема, от сервиса хранения ключей, строки ключа, ассоциированной с идентификатором файла, и генерации одного или более ключей доступа с использованием строки ключа.

[0307] В некоторых примерах способа, аппаратных компонентов и долговременного считываемого компьютером носителя, описанных в настоящем документе, валидация запроса доступа может включать в себя операции, признаки, средства или инструкции для валидации информации доступа, которая включает в себя географическое местоположение пользовательского устройства, исполняющего клиент доступа, информацию устройства, ассоциированную с пользовательским устройством, информацию сети, ассоциированную с пользовательским устройством, токен аутентификации, ассоциированный с клиентом доступа, или их комбинацию.

[0308] Следует отметить, что эти способы описывают примеры реализаций и что операции и этапы могут быть организованы в другом порядке или иным образом модифицированы, так что возможны другие реализации. В некоторых примерах, могут комбинироваться аспекты из двух или более способов. Например, аспекты каждого из способов могут включать в себя этапы или аспекты других способов или другие этапы или методы, описанные в настоящем документе. Таким образом, аспекты раскрытия могут обеспечивать предпочтения потребителя и интерфейс обслуживания.

[0309] Описание, изложенное в настоящем документе, во взаимосвязи с прилагаемыми чертежами, описывает примерные конфигурации и не представляет все примеры, которые могут быть реализованы или которые соответствуют объему формулы изобретения. Термин “примерный”, используемый в настоящем документе, означает

“служащий в качестве примера, экземпляра или иллюстрации”, а не “предпочтительный” или “имеющий преимущество перед другими примерами”. Подробное описание включает в себя конкретные подробности с целью обеспечения понимания описанных методов. Эти методы, однако, могут применяться без этих конкретных подробностей. В некоторых примерах, хорошо известные структуры и устройства показаны в виде блок-схемы во избежание затенения концепций описанных примеров.

[0310] На прилагаемых чертежах, аналогичные компоненты или признаки могут иметь одинаковый ссылочный символ. Дополнительно, разные компоненты одного и того же типа могут различаться дополнением ссылочного символа через тире вторым символом, который проводит различие между аналогичными компонентами. Если только первый ссылочный символ используется в спецификации, описание применимо к любому одному из аналогичных компонентов, имеющих одинаковый первый ссылочный символ, независимо от второго ссылочного символа.

[0311] Информация и сигналы, описанные в настоящем документе, могут быть представлены с использованием любой из большого множества разных технологий и методов. Например, данные, инструкции, команды, информация, сигналы, биты, символы и элементарные посылки, ссылки на которые могут даваться во всем описании выше, могут быть представлены напряжениями, токами, электромагнитными волнами, магнитными полями или частицами, оптическими полями или частицами или любой их комбинацией.

[0312] Различные иллюстративные блоки и модули, описанные в связи с раскрытием в настоящем документе, могут быть реализованы или выполняться универсальным процессором, DSP, ASIC, FPGA или другим программируемым логическим устройством, дискретной вентильной или транзисторной логикой, дискретными аппаратными средствами или любой их комбинацией, предназначенной для выполнения функций, описанных в настоящем документе. Универсальный процессор может представлять собой микропроцессор, но альтернативно, процессор может представлять собой любой традиционный процессор, контроллер, микроконтроллер или конечный автомат. Процессор может также быть реализован как комбинация вычислительных устройств (например, комбинация DSP и микропроцессора, множества микропроцессоров, одного или более микропроцессоров в соединении с ядром DSP или любая другая такая конфигурация).

[0313] Функции, описанные в настоящем документе, могут быть реализованы в аппаратных средствах, программном обеспечении, исполняемом процессором, прошивке или любой их комбинации. При реализации в программном обеспечении, исполняемом процессором, функции могут храниться или передаваться как одна или более инструкций или код на считываемом компьютером носителе. Другие примеры и реализации находятся в объеме раскрытия и прилагаемой формулы изобретения. Например, вследствие природы программного обеспечения, функции, описанные выше, могут быть реализованы с использованием программного обеспечения, исполняемого процессором, аппаратных средств, прошивки, жесткого монтажа или комбинаций любых из них. Признаки, реализующие функции, могут также быть физически расположены в различных

положениях, в том числе распределенных, так что части функций реализуются в разных физических местоположениях. Также, как использовано в настоящем документе, в том числе в формуле изобретения, “или” как используется в списке элементов (например, списке элементов, которому предшествует фраза, такая как “по меньшей мере один из” или “один или более из”) указывает инклюзивный список, так что, например, список из по меньшей мере одного из A, B или C означает A или B или C, или AB или AC или BC, или ABC (т.е. A и B и C). Также, как использовано в настоящем документе, фраза “на основе” не должна пониматься как ссылка на закрытый набор условий. Например, примерный этап, который описан как “на основе условия A”, может быть основан и как на условии A, так и на условии B без отклонения от объема настоящего раскрытия. Иными словами, как использовано в настоящем документе, фраза “на основе” должна пониматься таким же образом, что и фраза “на основе, по меньшей мере частично,”.

[0314] Считываемые компьютером носители включают в себя как долговременные компьютерные запоминающие носители, так и коммуникационные носители, включая любой носитель, который облегчает перенос компьютерной программы из одного места в другое. Долговременный запоминающий носитель может представлять собой любой доступный носитель, доступ к которому может осуществляться универсальным или специализированным компьютером. В качестве примера и не для ограничения, долговременные считываемые компьютером носители могут содержать RAM, ROM, электрически стираемую программируемую постоянную память (EEPROM), ROM на компакт-диске (CD-ROM) или другое хранилище на оптическом диске, хранилище на магнитном диске или другие магнитные запоминающие устройства, или любой другой долговременный носитель, который может использоваться для переноса или хранения желаемого средства программного кода в виде инструкций или структур данных, и доступ к которому может осуществляться универсальным или специализированным компьютером, или универсальным или специализированным процессором. Также, любое соединение может надлежащим образом определяться как считываемый компьютером носитель. Например, если программное обеспечение передается с веб-сайта, сервера или другого удаленного источника с использованием коаксиального кабеля, оптоволоконного кабеля, скрученной пары, цифровой абонентской линии (DSL) или беспроводных технологий, таких как инфракрасная, радио и микроволновая, то коаксиальный кабель, оптоволоконный кабель, скрученная пара, DSL или беспроводные технологии, такие как инфракрасная, радио и микроволновая, включены в определение носителя. Магнитный диск (disk) и оптический диск (disc), как использовано в настоящем документе, включают в себя CD, лазерный диск, оптический диск, цифровой универсальный диск (DVD), флоппи-диск и Blu-ray диск, где магнитные диски (disks) обычно воспроизводят данные магнитным способом, в то время как оптические диски (discs) воспроизводят данные оптическим способом при помощи лазеров. Комбинации описанного выше также включены в объем считываемых компьютером носителей.

[0315] Различные иллюстративные блоки и модули, описанные в соединении с

раскрытием в настоящем документе, могут быть реализованы или выполняться универсальным процессором, цифровым сигнальным процессором (DSP), ASIC, программируемой вентильной матрицей (FPGA) или другим программируемым логическим устройством, дискретной вентильной или транзисторной логикой, дискретными аппаратными компонентами или любой их комбинацией, предназначенной для выполнения функций, описанных в настоящем документе. Универсальный процессор может представлять собой микропроцессор, но альтернативно, процессор может представлять собой любой традиционный процессор, контроллер, микроконтроллер или конечный автомат. Процессор может также быть реализован как комбинация вычислительных устройств (например, комбинация DSP и микропроцессора, множества микропроцессоров, одного или более микропроцессоров в соединении с ядром DSP или любая другая такая конфигурация). Функции каждого блока могут также быть реализованы, полностью или частично, при помощи инструкций, включенных в память, отформатированных для исполнения одним или более универсальными или специализированными процессорами.

[0316] На прилагаемых чертежах, аналогичные компоненты или признаки могут иметь одинаковый ссылочный символ. Дополнительно, разные компоненты одного и того же типа могут различаться дополнением ссылочного символа через тире вторым символом, который проводит различие между аналогичными компонентами. Если только первый ссылочный символ используется в спецификации, описание применимо к любому одному из аналогичных компонентов, имеющих одинаковый первый ссылочный символ, независимо от второго ссылочного символа.

[0317] Описание в настоящем документе обеспечено, чтобы предоставить специалисту в данной области техники возможность осуществить или использовать раскрытие. Различные модификации раскрытия будут очевидны специалистам в данной области техники, и обобщенные принципы, определенные в настоящем документе, могут применяться к другим вариантам без отклонения от объема раскрытия. Таким образом, раскрытие не ограничено примерами и схемами, описанными в настоящем документе, а должно соответствовать наиболее широкому объему, совместимому с принципами и новыми признаками, раскрытыми в настоящем документе.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ для защиты данных в клиенте доступа, содержащий:

передачу, на сервер, запроса доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ;

прием, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакета доступа, который включает в себя исполняемый код и один или более ключей доступа;

исполнение, клиентом доступа, исполняемого кода для осуществления доступа к файлу с использованием одного или более ключей доступа; и

удаление пакета доступа из памяти, ассоциированной с клиентом доступа.

2. Способ по п. 1, причем передача запроса доступа содержит:

передачу, на сервер, запроса шифрования и информации файла.

3. Способ по п. 2, причем прием пакета доступа содержит:

прием пакета доступа, который включает в себя пакет данных, содержащий указание одной или более политик доступа к файлу, ассоциированных с файлом, причем пакет данных зашифрован с файлом с использованием одного или более ключей доступа.

4. Способ по п. 3, причем одна или более политик доступа к файлу включают в себя доступ для чтения, доступ для записи, ограничения на отображение или их комбинацию.

5. Способ по п. 2, причем прием пакета доступа содержит:

прием пакета доступа, который включает в себя пакет данных, содержащий указание информации о владении, ассоциированной с файлом, причем пакет данных зашифрован с файлом с использованием одного или более ключей доступа.

6. Способ по п. 2, причем передача запроса шифрования содержит:

передачу, на сервер, указания одной или более политик доступа к файлу, ассоциированных с файлом.

7. Способ по п. 2, причем исполнение исполняемого кода содержит:

шифрование, с использованием исполняемого кода, полезной нагрузки и одного или более пакетов данных с использованием одного или более ключей доступа для генерации зашифрованного файла.

8. Способ по п. 7, причем шифрование одного или более пакетов данных содержит:

шифрование одного или более пакетов данных, которые включают в себя указание одной или более политик доступа к файлу, информацию о владении файлом, лог аудита доступа к файлу или их комбинацию.

9. Способ по п. 1, причем передача запроса доступа содержит:

передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы дешифровать файл.

10. Способ по п. 9, причем прием пакета доступа содержит:

прием пакета доступа, который включает в себя пакет данных, содержащий одну или более обновленных политик доступа к файлу.

11. Способ по п. 9, дополнительно содержащий:

идентификацию, в клиенте доступа, информации валидации, которая включает в себя информацию клиента доступа, информацию компьютера, информацию устройства, информацию географического местоположения, токен аутентификации или их комбинацию, причем запрос дешифрования включает в себя указание информации валидации.

12. Способ по п. 9, дополнительно содержащий:

идентификацию, что файл ассоциирован с клиентом доступа, на основе, по меньшей мере частично, метаданных, ассоциированных с файлом, причем файл включает в себя полезную нагрузку, зашифрованную с использованием первого ключа из одного или более ключей доступа, и один или более зашифрованных пакетов данных, которые зашифрованы с использованием по меньшей мере одного второго ключа из одного или более ключей доступа, причем запрос дешифрования передается на сервер на основе того, по меньшей мере частично, что файл ассоциирован с клиентом доступа.

13. Способ по п. 9, причем исполнение исполняемого кода содержит:

дешифрование файла с использованием одного или более ключей доступа.

14. Способ по п. 13, дополнительно содержащий:

отображение, в клиенте доступа, полезной нагрузки файла в соответствии с одной или более политиками доступа, ассоциированными с файлом.

15. Способ по п. 14, причем одна или более политик доступа включают в себя доступ для чтения, доступ для записи, ограничения на отображение или их комбинацию.

16. Способ по п. 14, причем одна или более политик доступа включены в пакет данных, который был дешифрован с файлом с использованием одного или более ключей доступа.

17. Способ по п. 13, дополнительно содержащий:

обновление лога аудита доступа к файлу, чтобы включать информацию устройства, ассоциированную с клиентом доступа, информацию пользователя, информацию географического местоположения или их комбинацию.

18. Способ по п. 13, дополнительно содержащий:

идентификацию, на основе, по меньшей мере частично, дешифрования файла, полезной нагрузки и одного или более пакетов данных в файле, причем один или более пакетов данных включают в себя указание одной или более политик доступа к файлу, информацию о владении, лог аудита доступа к файлу или их комбинацию.

19. Способ по п. 1, дополнительно содержащий:

создание, в памяти, ассоциированной с клиентом доступа, и на основе, по меньшей мере частично, исполнения исполняемого кода, объекта доступа, который используется, чтобы дешифровать или шифровать файл, причем объект доступа удаляется из памяти, ассоциированной с клиентом доступа, после дешифрования или шифрования файла.

20. Способ по п. 1, дополнительно содержащий:

передачу, на сервер, запроса дешифрования и информации файла, причем исполняемый код включает в себя код, который используется, чтобы перезаписывать

содержимое файла.

21. Способ по п. 1, причем передача запроса доступа содержит:

передачу запроса доступа, который включает в себя информацию доступа, содержащую географическое местоположение пользовательского устройства, исполняющего клиент доступа, информацию устройства, ассоциированную с пользовательским устройством, информацию сети, ассоциированную с пользовательским устройством, токен аутентификации, ассоциированный с клиентом доступа, или их комбинацию.

22. Аппаратный компонент для защиты данных в клиенте доступа, содержащий:

процессор;

память, связанную с процессором; и

инструкции, хранящиеся в памяти и исполняемые процессором, чтобы побуждать аппаратный компонент:

передавать, на сервер, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ;

принимать, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа;

исполнять, клиентом доступа, исполняемый код для осуществления доступа к файлу с использованием одного или более ключей доступа; и

удалять пакет доступа из памяти, ассоциированной с клиентом доступа.

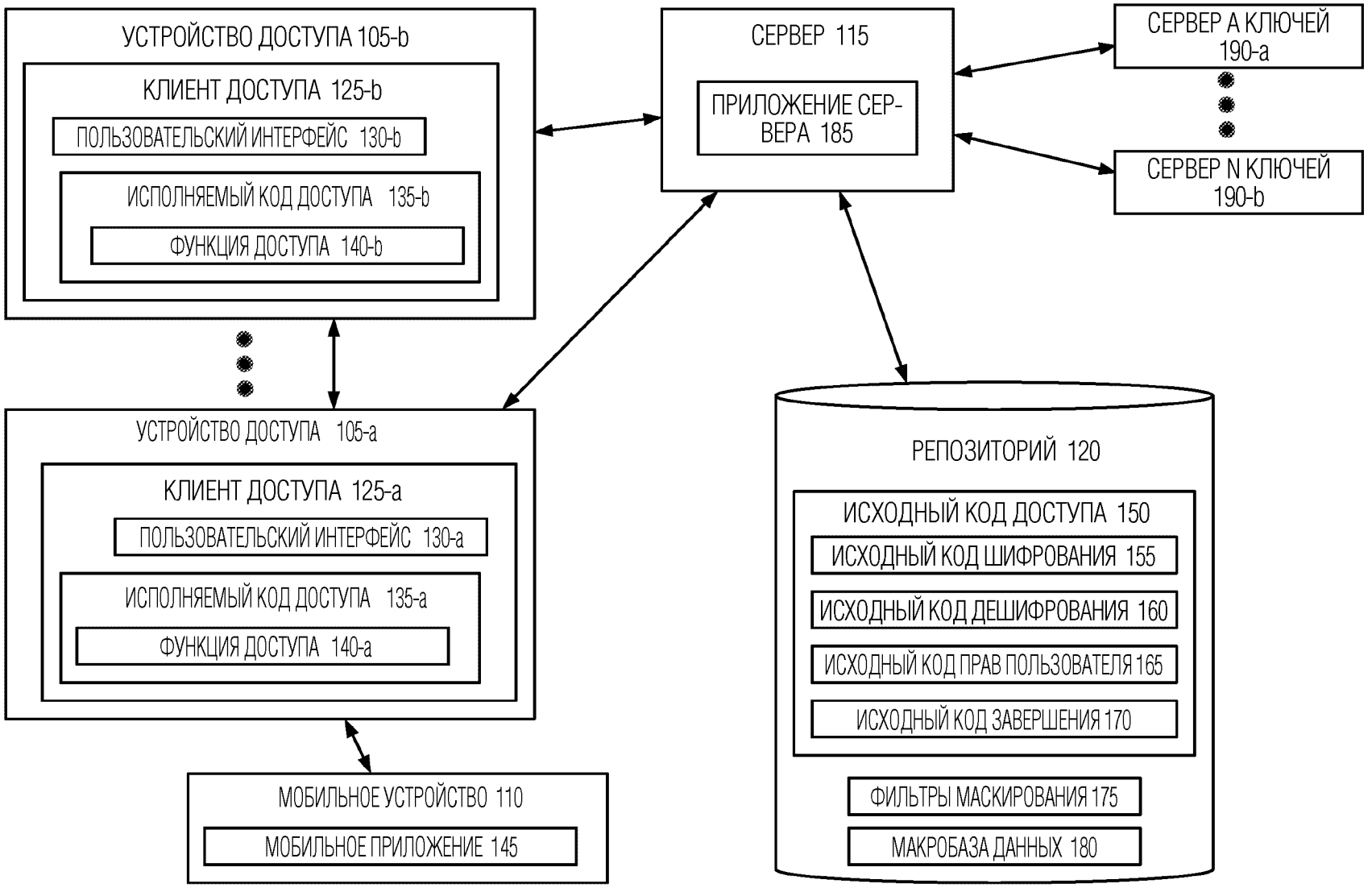
23. Долговременный считываемый компьютером носитель, хранящий код для защиты данных в клиенте доступа, причем код содержит инструкции, исполняемые процессором, чтобы:

передавать, на сервер, запрос доступа, который включает в себя информацию доступа и информацию файла для файла, к которому необходимо осуществить доступ;

принимать, от сервера на основе, по меньшей мере частично, передачи запроса доступа, пакет доступа, который включает в себя исполняемый код и один или более ключей доступа;

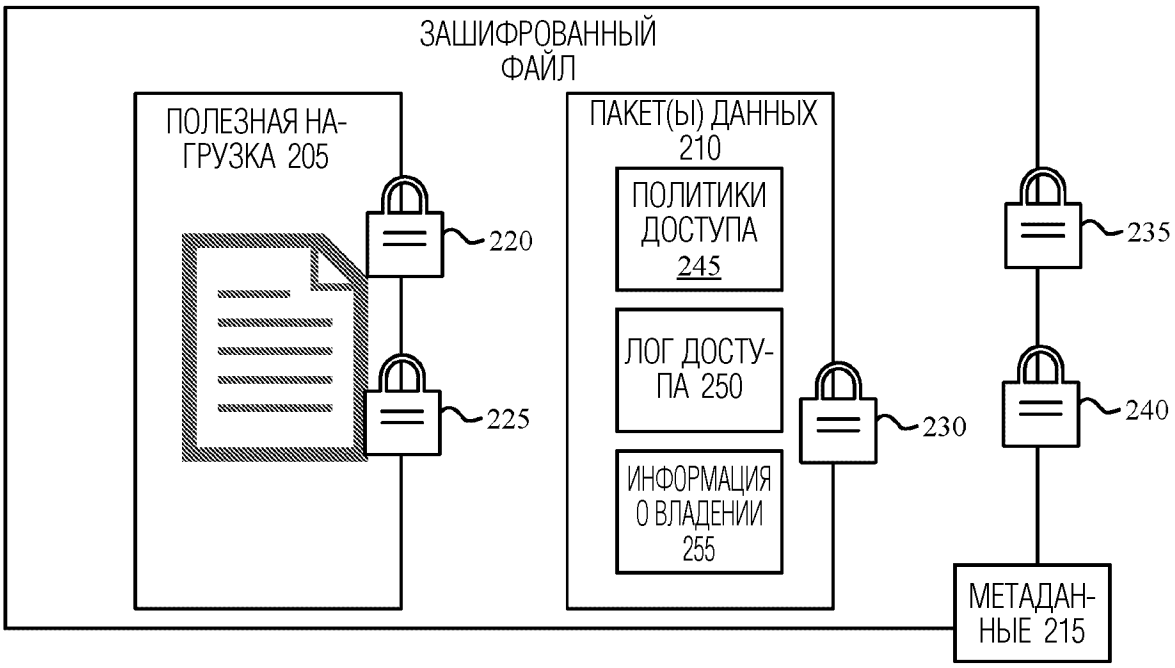
исполнять, клиентом доступа, исполняемый код для осуществления доступа к файлу с использованием одного или более ключей доступа; и

удалять пакет доступа из памяти, ассоциированной с клиентом доступа.

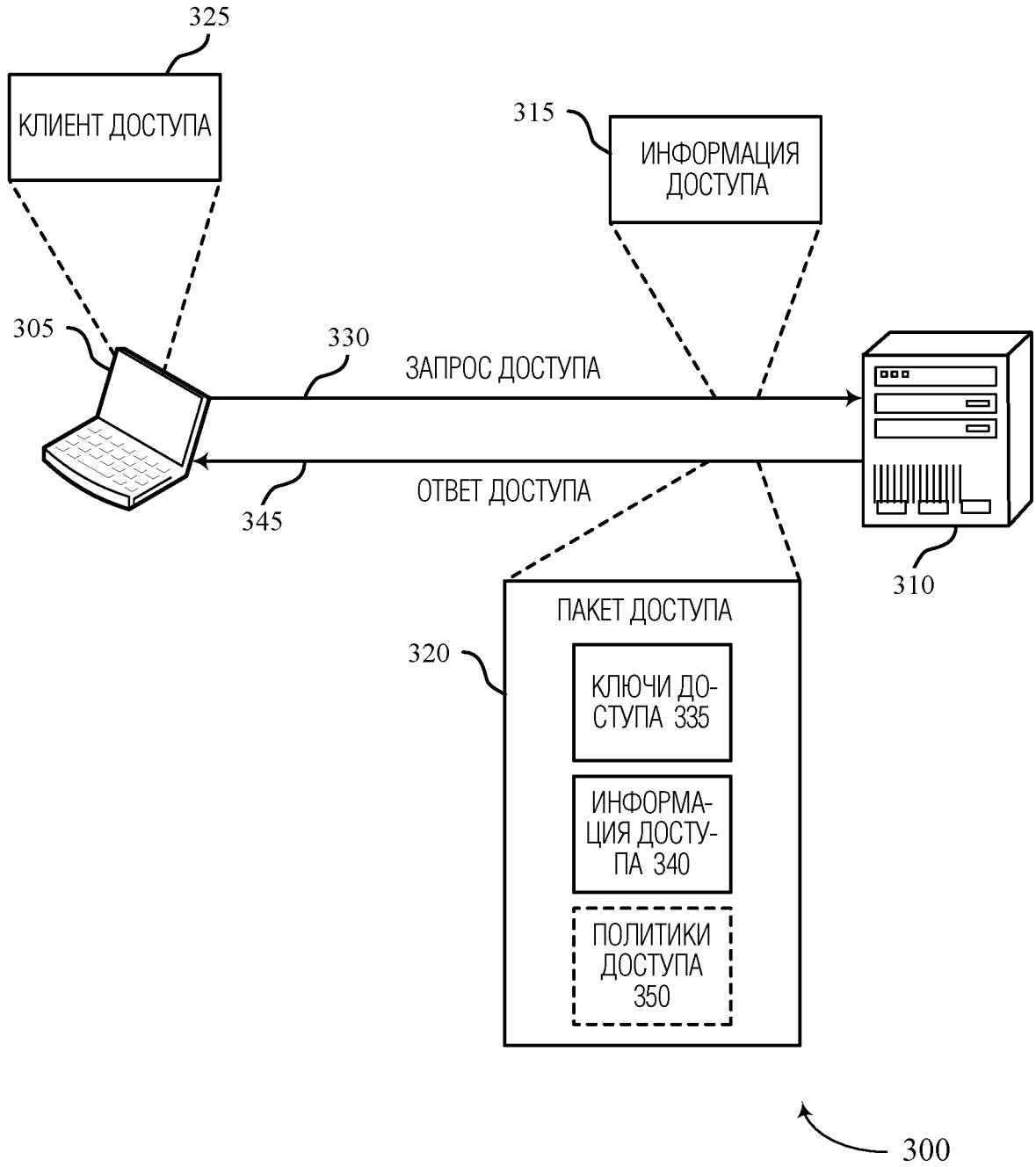

УСТРОЙСТВО ДОСТУПА 105-b
КЛИЕНТ ДОСТУПА 125-b
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС 130-b
ИСПОЛНЯЕМЫЙ КОД ДОСТУПА 135-b
ФУНКЦИЯ ДОСТУПА 140-b
СЕРВЕР 115
ПРИЛОЖЕНИЕ СЕРВЕРА 185
СЕРВЕР А КЛЮЧЕЙ 190-a
СЕРВЕР N КЛЮЧЕЙ 190-b
УСТРОЙСТВО ДОСТУПА 105-a
КЛИЕНТ ДОСТУПА 125-a
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС 130-a
ИСПОЛНЯЕМЫЙ КОД ДОСТУПА 135-a
ФУНКЦИЯ ДОСТУПА 140-a
РЕПОЗИТОРИЙ 120
ИСХОДНЫЙ КОД ДОСТУПА 150
ИСХОДНЫЙ КОД ШИФРОВАНИЯ 155
ИСХОДНЫЙ КОД ДЕШИФРОВАНИЯ 160
ИСХОДНЫЙ КОД ПРАВ ПОЛЬЗОВАТЕЛЯ 165
ИСХОДНЫЙ КОД ЗАВЕРШЕНИЯ 170
ФИЛЬТРЫ МАСКИРОВАНИЯ 175
МАКРОБАЗА ДАННЫХ 180
МОБИЛЬНОЕ УСТРОЙСТВО 110
МОБИЛЬНОЕ ПРИЛОЖЕНИЕ 145
100

ФИГ. 1

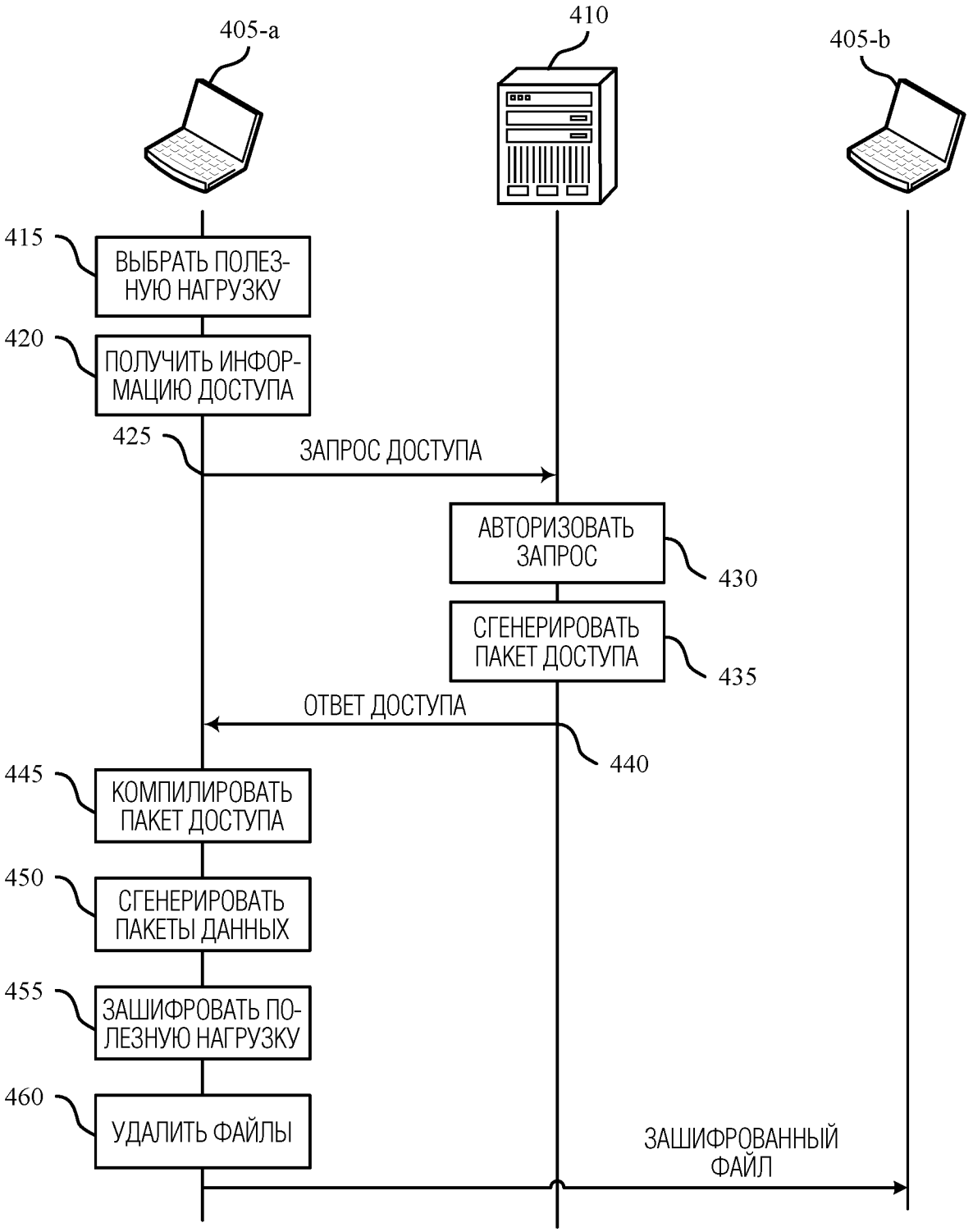
577844


ЗАШИФРОВАННЫЙ ФАЙЛ
ПОЛЕЗНАЯ НАГРУЗКА 205
ПАКЕТ(Ы) ДАННЫХ 210
ПОЛИТИКИ ДОСТУПА 245
ЛОГ ДОСТУПА 250
ИНФОРМАЦИЯ О ВЛАДЕНИИ 255
МЕТАДАННЫЕ 215
220
225
230
235
240
200

ФИГ. 2

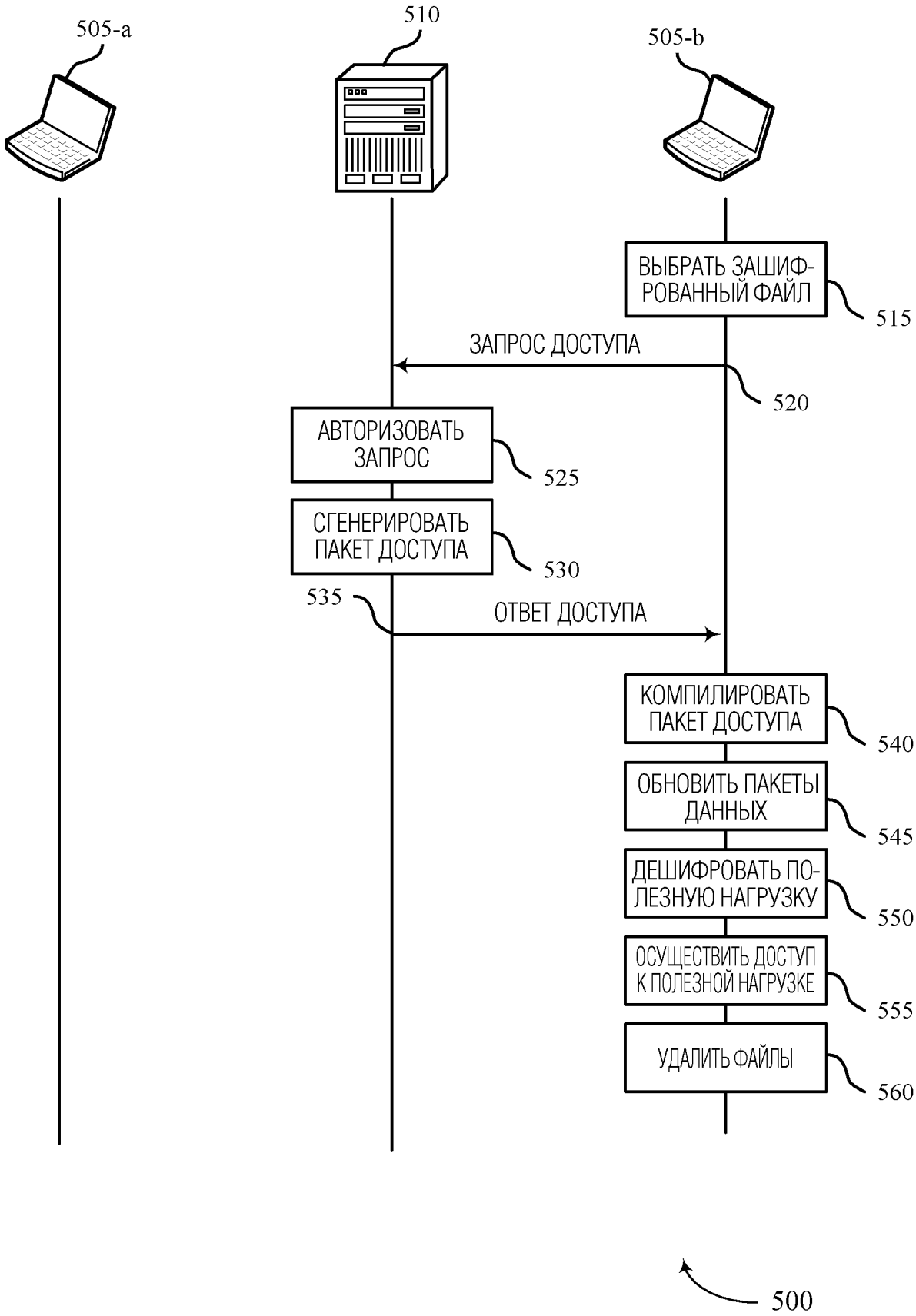

325
КЛИЕНТ ДОСТУПА
315
ИНФОРМАЦИЯ ДОСТУПА
305
330
ЗАПРОС ДОСТУПА
ОТВЕТ ДОСТУПА
345
310
ПАКЕТ ДОСТУПА
320
КЛЮЧИ ДОСТУПА 335
ИНФОРМАЦИЯ ДОСТУПА 340
ПОЛИТИКИ ДОСТУПА 350
300

ФИГ. 3

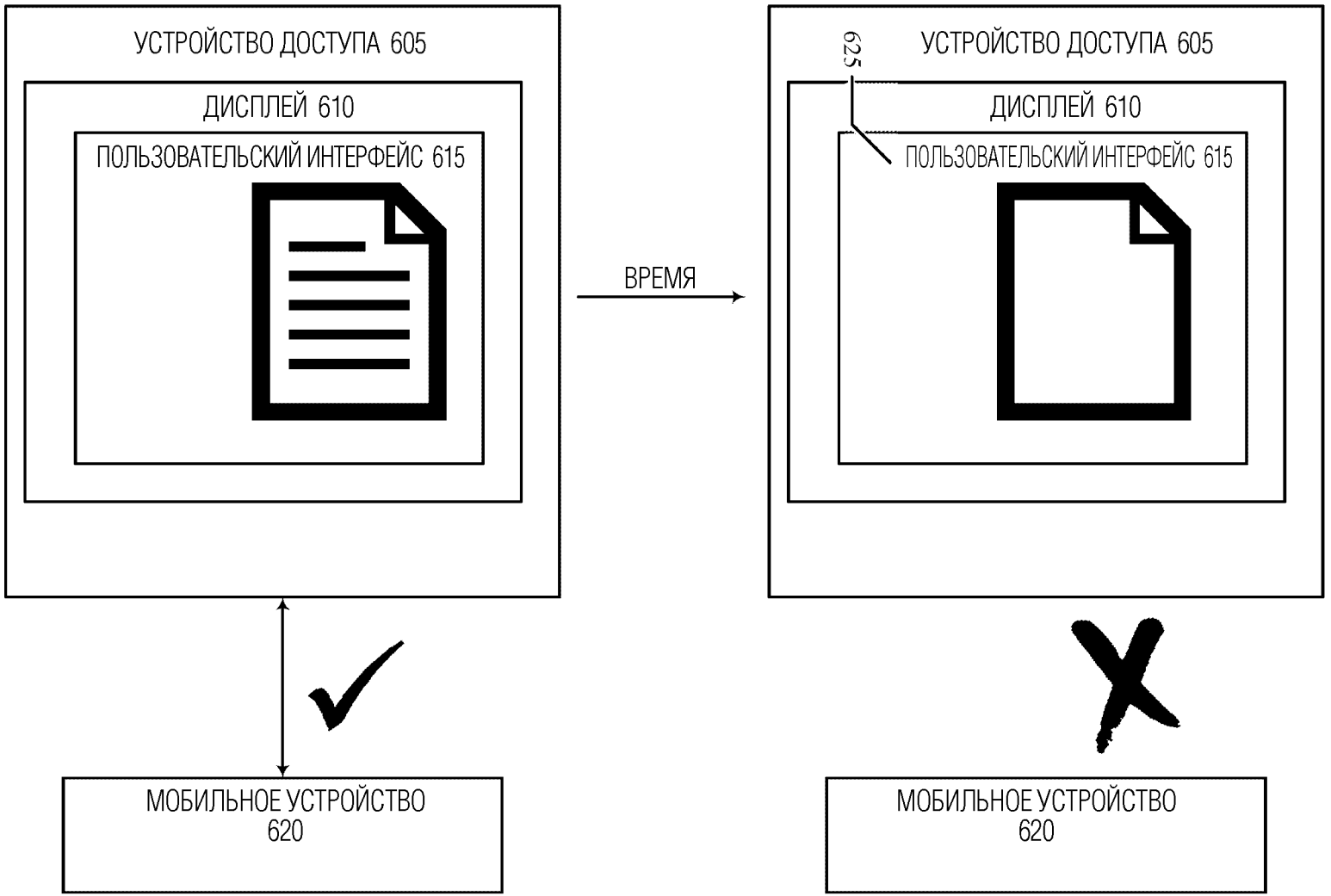

405-a
410
405-b
415
ВЫБРАТЬ ПОЛЕЗНУЮ НАГРУЗКУ
420
ПОЛУЧИТЬ ИНФОРМАЦИЮ ДОСТУПА
425
ЗАПРОС ДОСТУПА
АВТОРИЗОВАТЬ ЗАПРОС
430
СГЕНЕРИРОВАТЬ ПАКЕТ ДОСТУПА
435
ОТВЕТ ДОСТУПА
440
445
КОМПИЛИРОВАТЬ ПАКЕТ ДОСТУПА
450
СГЕНЕРИРОВАТЬ ПАКЕТЫ ДАННЫХ
455
ЗАШИФРОВАТЬ ПОЛЕЗНУЮ НАГРУЗКУ
460
УДАЛИТЬ ФАЙЛЫ
ЗАШИФРОВАННЫЙ ФАЙЛ

ФИГ. 4

400

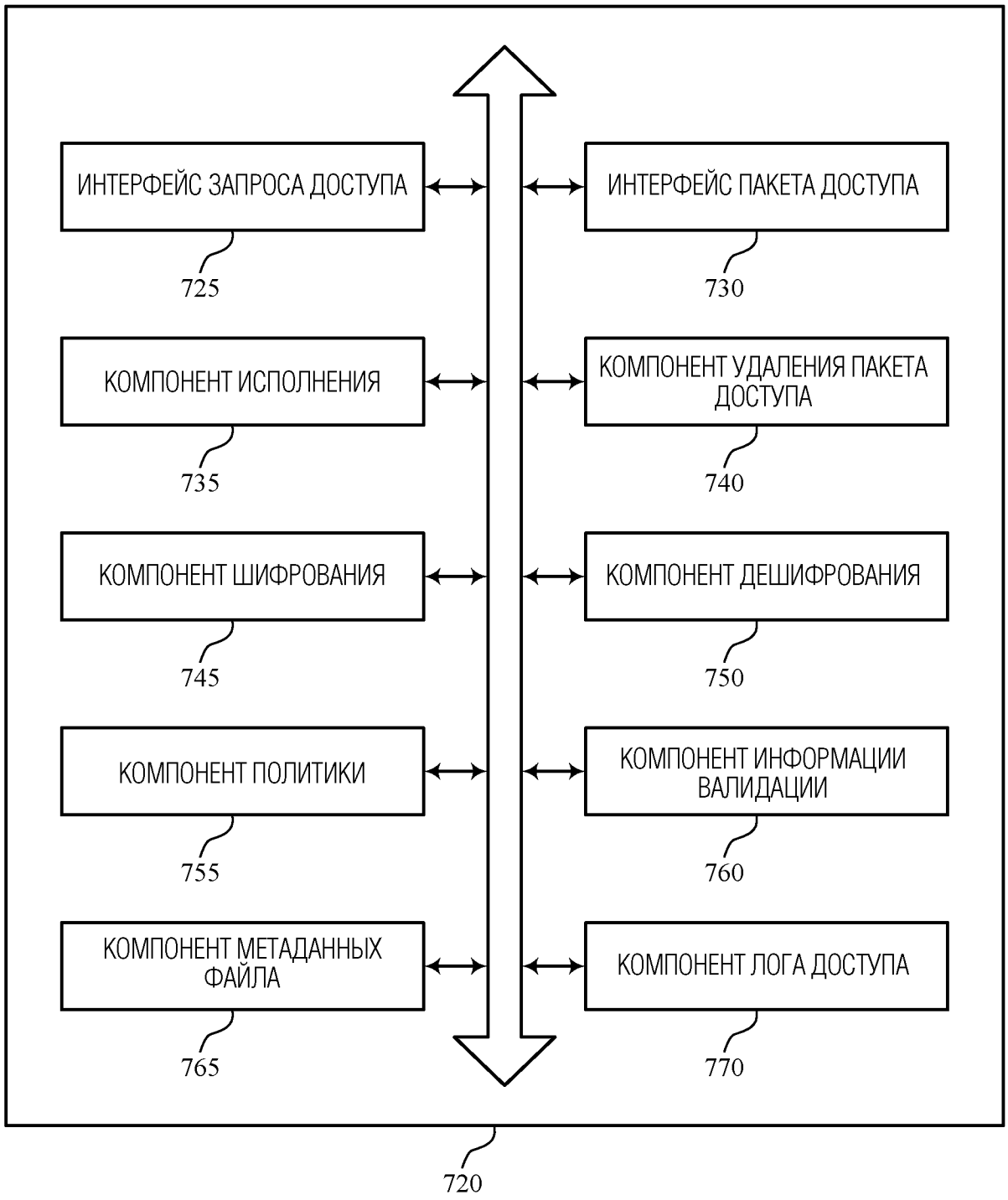

505-a
510
505-b
ВЫБРАТЬ ЗАШИФ-РОВАННЫЙ ФАЙЛ
515
ЗАПРОС ДОСТУПА
520
АВТОРИЗОВАТЬ ЗАПРОС
525
СГЕНЕРИРОВАТЬ ПАКЕТ ДОСТУПА
530
535
ОТВЕТ ДОСТУПА
КОМПИЛИРОВАТЬ ПАКЕТ ДОСТУПА
540
ОБНОВИТЬ ПАКЕТЫ ДАННЫХ
545
ДЕШИФРОВАТЬ ПО-ЛЕЗНУЮ НАГРУЗКУ
550
ОСУЩЕСТВИТЬ ДОСТУП К ПОЛЕЗНОЙ НАГРУЗКЕ
555
УДАЛИТЬ ФАЙЛЫ
560
500

ФИГ. 5

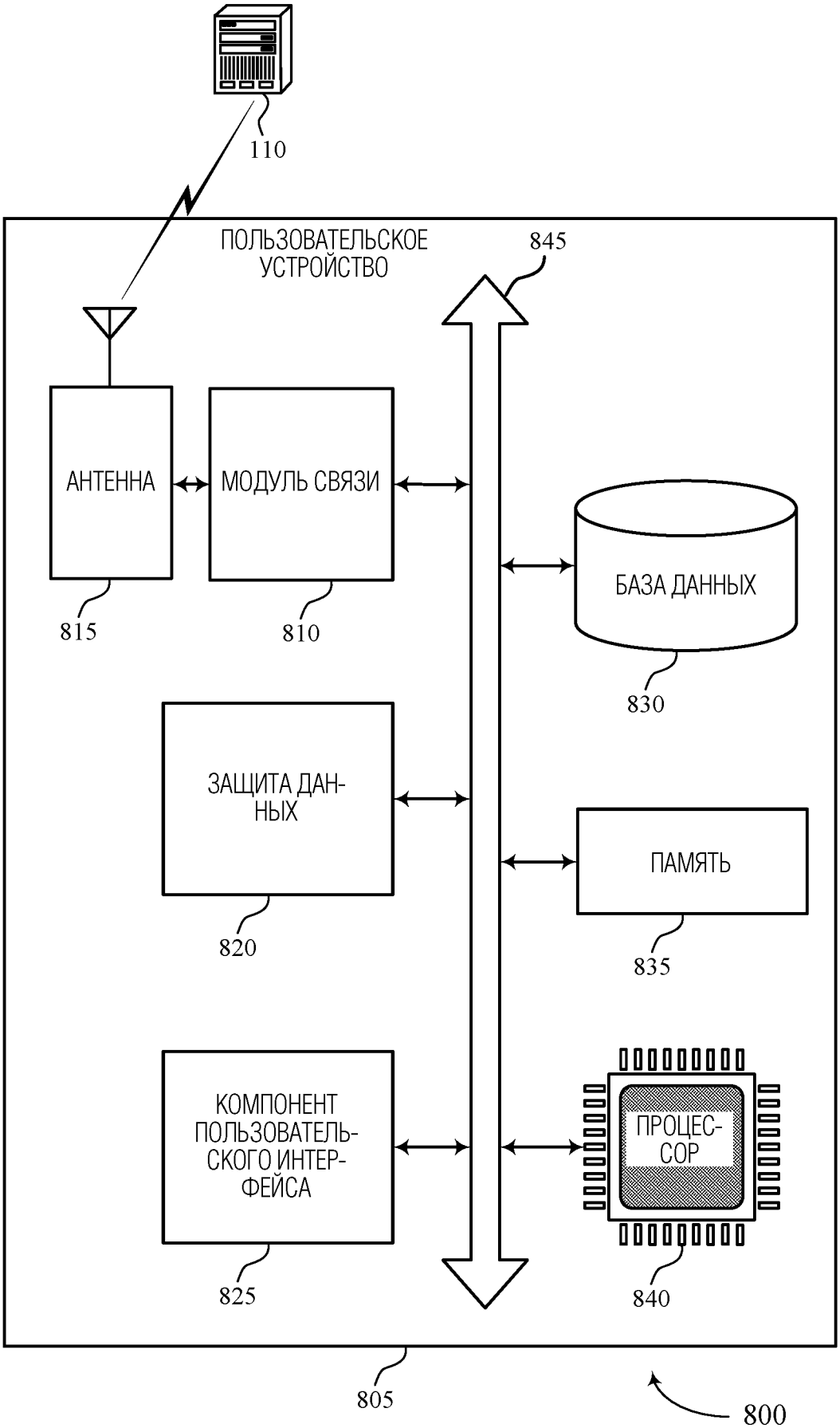

УСТРОЙСТВО ДОСТУПА 605
ДИСПЛЕЙ 610
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС 615
ВРЕМЯ
625
УСТРОЙСТВО ДОСТУПА 605
ДИСПЛЕЙ 610
ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС 615
МОБИЛЬНОЕ УСТРОЙСТВО 620
МОБИЛЬНОЕ УСТРОЙСТВО 620

ФИГ. 6

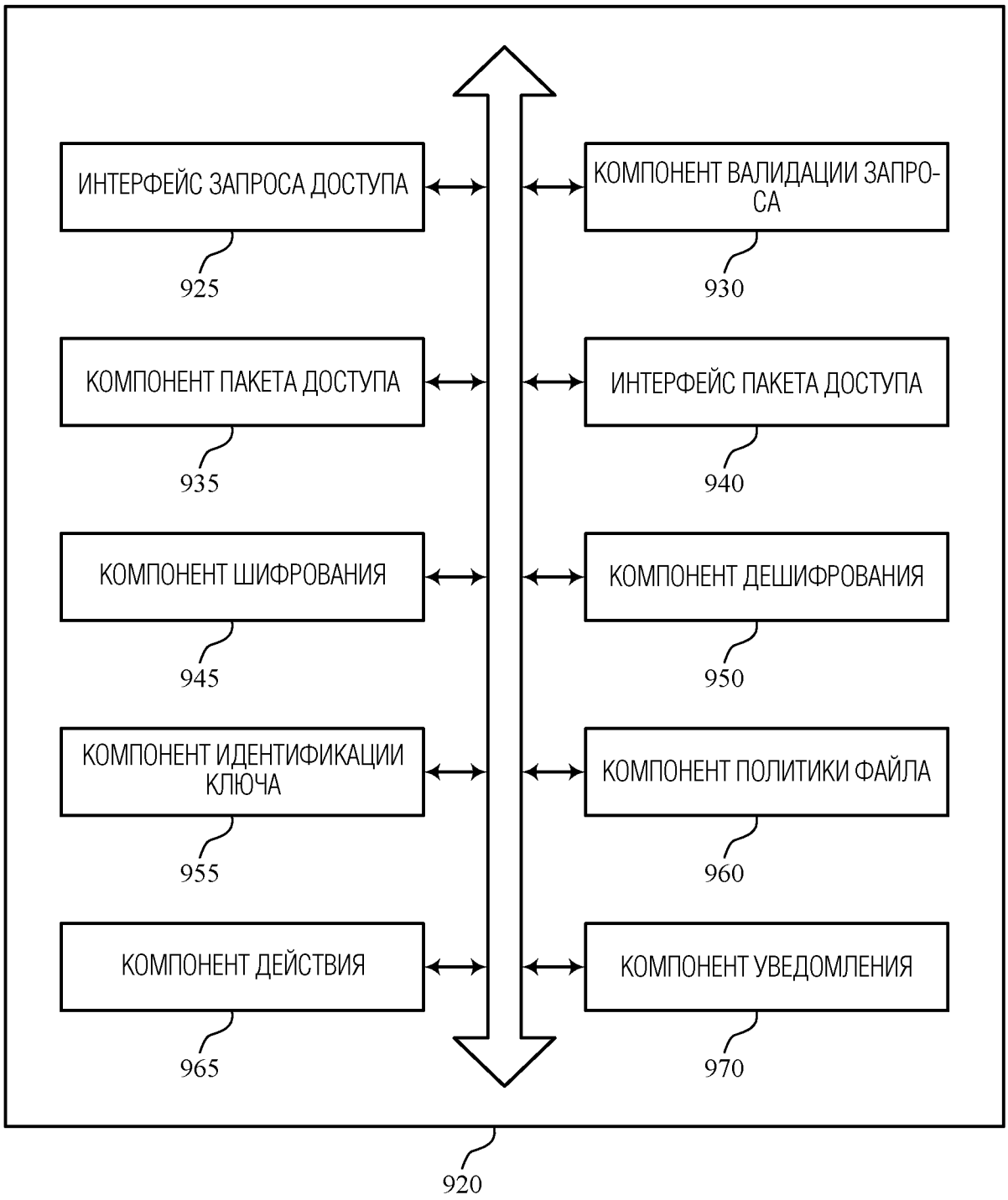
600


ИНТЕРФЕЙС ЗАПРОСА ДОСТУПА
725
ИНТЕРФЕЙС ПАКЕТА ДОСТУПА
730
КОМПОНЕНТ ИСПОЛНЕНИЯ
735
КОМПОНЕНТ УДАЛЕНИЯ ПАКЕТА ДОСТУПА
740
КОМПОНЕНТ ШИФРОВАНИЯ
745
КОМПОНЕНТ ДЕШИФРОВАНИЯ
750
КОМПОНЕНТ ПОЛИТИКИ
755
КОМПОНЕНТ ИНФОРМАЦИИ ВАЛИДАЦИИ
760
КОМПОНЕНТ МЕТАДАННЫХ ФАЙЛА
765
КОМПОНЕНТ ЛОГА ДОСТУПА
770
720
700

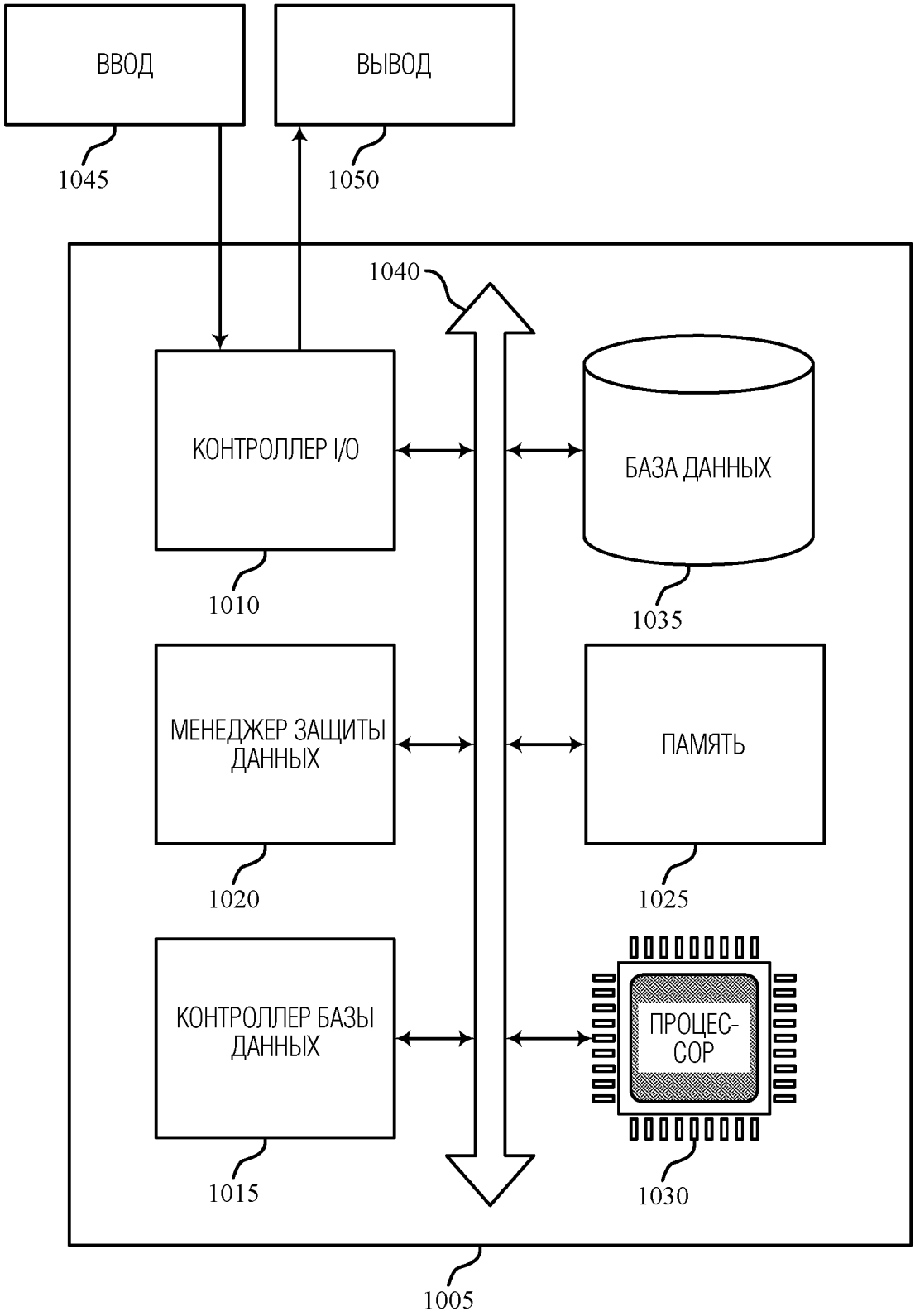
ФИГ. 7


110
ПОЛЬЗОВАТЕЛЬСКОЕ УСТРОЙСТВО
845
АНТЕННА
МОДУЛЬ СВЯЗИ
БАЗА ДАННЫХ
815
810
830
ЗАЩИТА ДАННЫХ
ПАМЯТЬ
820
835
КОМПОНЕНТ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА
ПРОЦЕССОР
825
840
805
800

ФИГ. 8

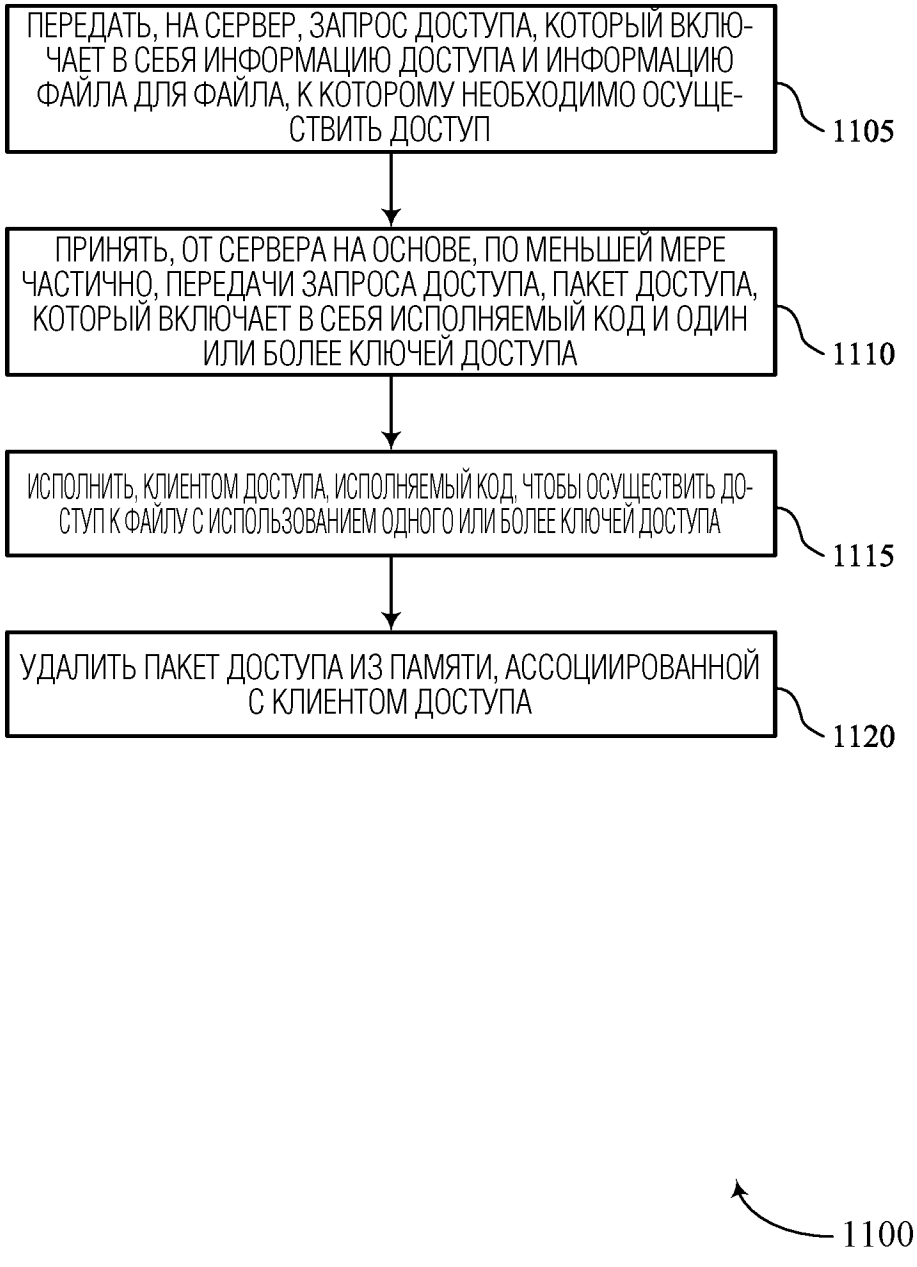

ИНТЕРФЕЙС ЗАПРОСА ДОСТУПА
925
КОМПОНЕНТ ВАЛИДАЦИИ ЗАПРОСА
930
КОМПОНЕНТ ПАКЕТА ДОСТУПА
935
ИНТЕРФЕЙС ПАКЕТА ДОСТУПА
940
КОМПОНЕНТ ШИФРОВАНИЯ
945
КОМПОНЕНТ ДЕШИФРОВАНИЯ
950
КОМПОНЕНТ ИДЕНТИФИКАЦИИ КЛЮЧА
955
КОМПОНЕНТ ПОЛИТИКИ ФАЙЛА
960
КОМПОНЕНТ ДЕЙСТВИЯ
965
КОМПОНЕНТ УВЕДОМЛЕНИЯ
970
920
900

ФИГ. 9

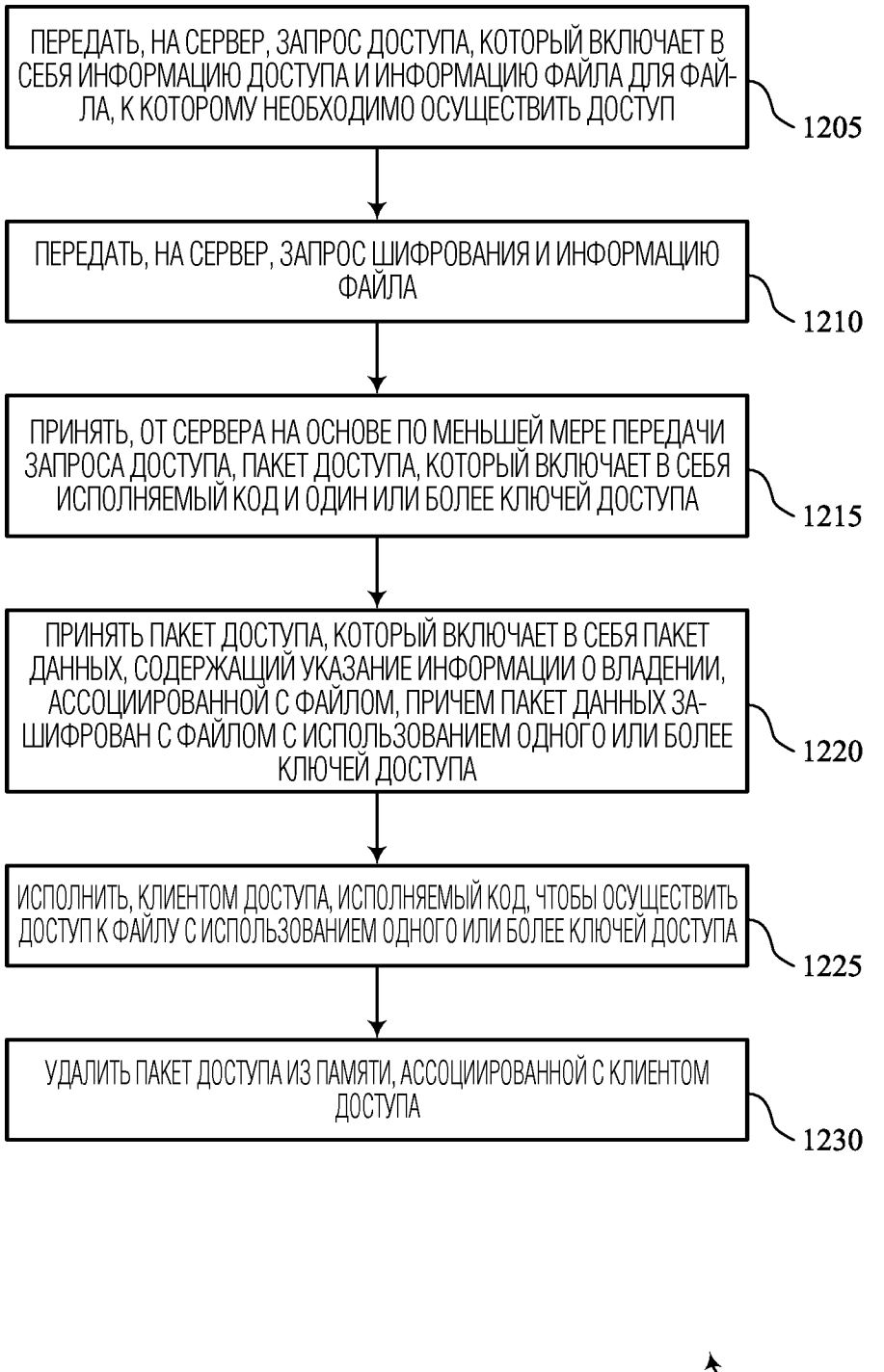

ВВОД
ВЫВОД
1045
1050
1040
КОНТРОЛЛЕР I/O
БАЗА ДАННЫХ
1010
1035
МЕНЕДЖЕР ЗАЩИТЫ ДАННЫХ
ПАМЯТЬ
1020
1025
КОНТРОЛЛЕР БАЗЫ ДАННЫХ
ПРОЦЕС-СОР
1015
1030
1005

ФИГ. 10

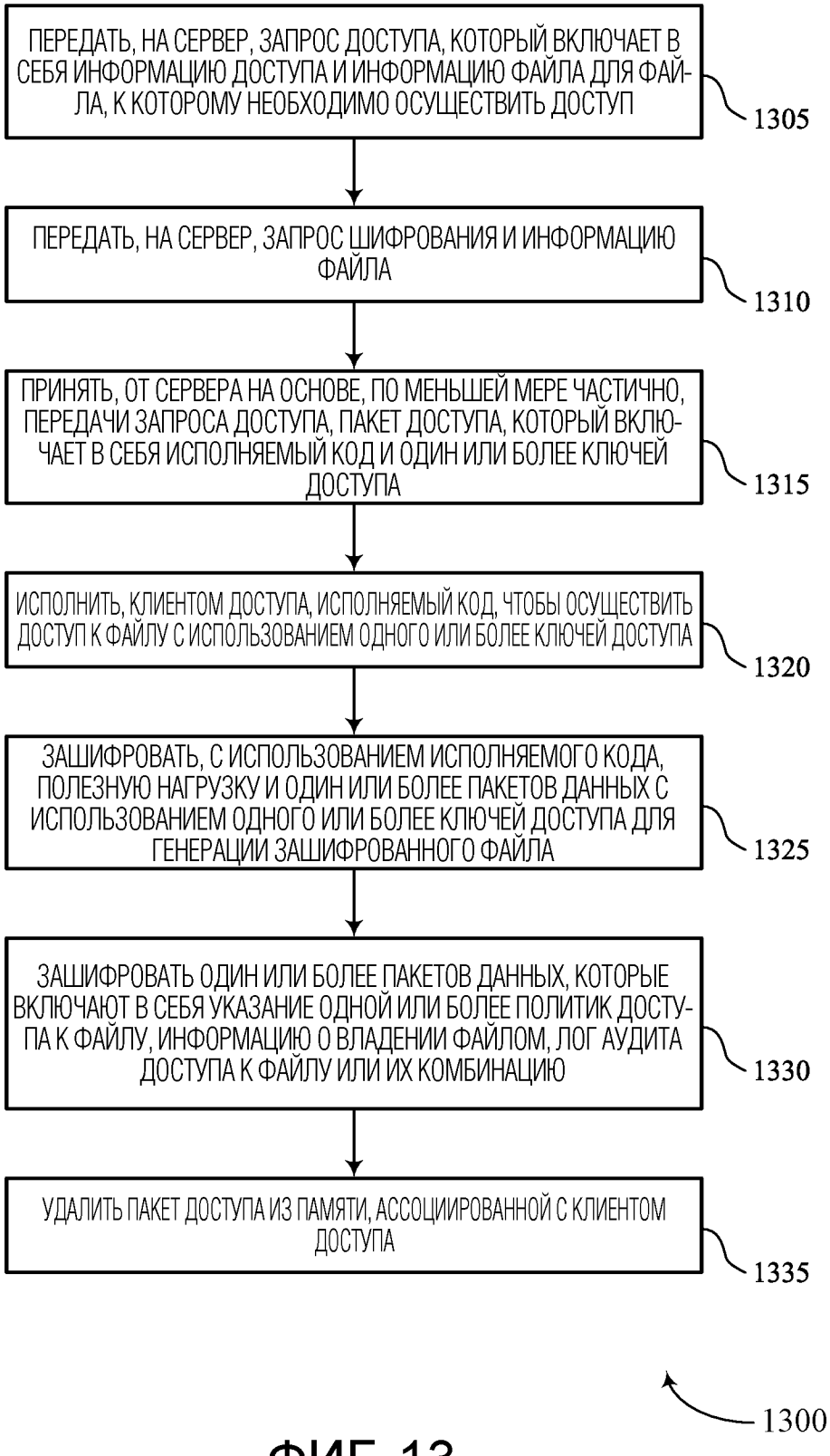
1000


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1105
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1110
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1115
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1120
1100

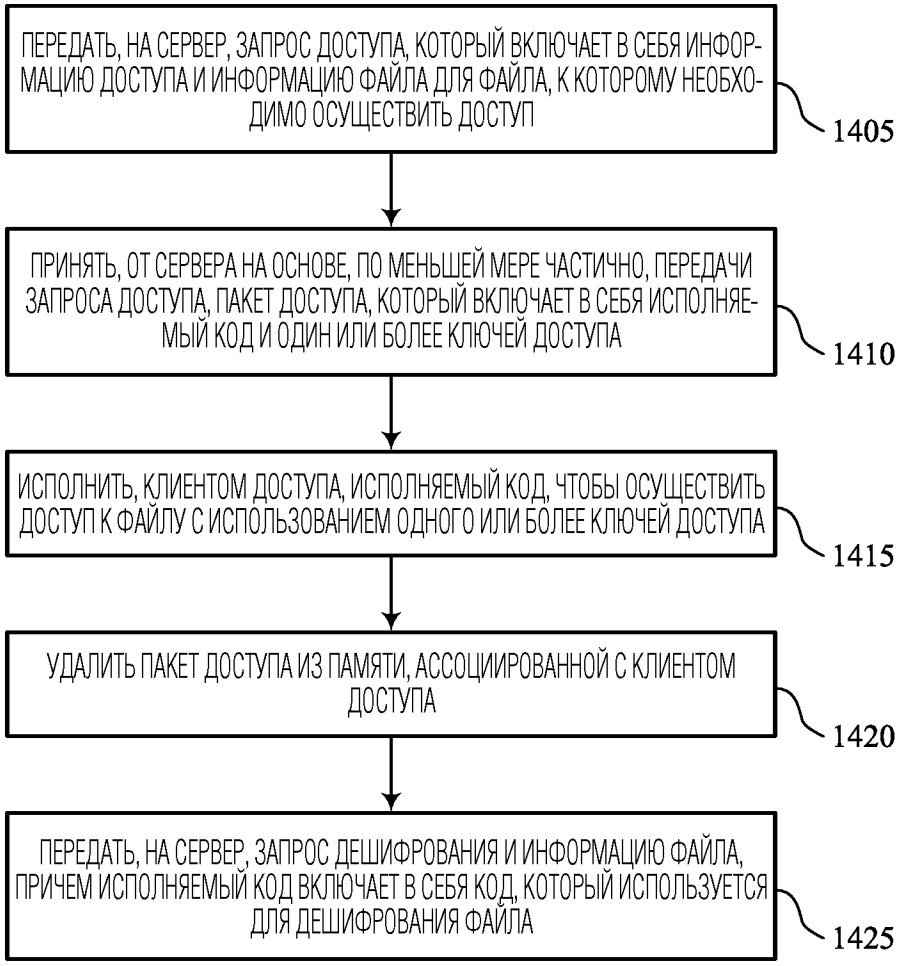
ФИГ. 11


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1205
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА
1210
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ ПО МЕНЬШЕЙ МЕРЕ ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1215
ПРИНЯТЬ ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ПАКЕТ ДАННЫХ, СОДЕРЖАЩИЙ УКАЗАНИЕ ИНФОРМАЦИИ О ВЛАДЕНИИ, АССОЦИИРОВАННОЙ С ФАЙЛОМ, ПРИЧЕМ ПАКЕТ ДАННЫХ ЗАШИФРОВАН С ФАЙЛОМ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1220
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1225
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1230
1200

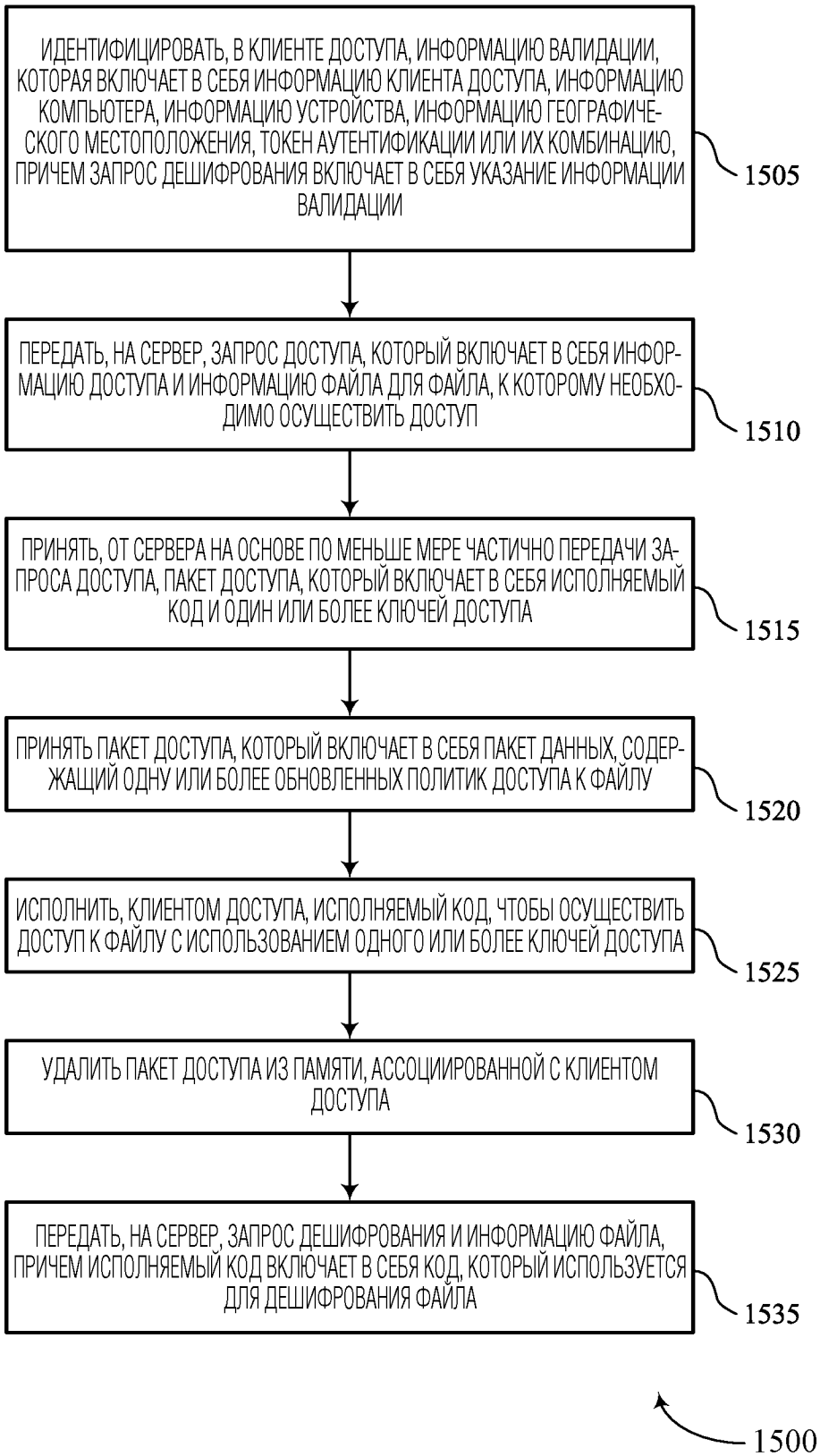
ФИГ. 12


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1305
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА
1310
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1315
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1320
ЗАШИФРОВАТЬ, С ИСПОЛЬЗОВАНИЕМ ИСПОЛНЯЕМОГО КОДА, ПОЛЕЗНУЮ НАГРУЗКУ И ОДИН ИЛИ БОЛЕЕ ПАКЕТОВ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА ДЛЯ ГЕНЕРАЦИИ ЗАШИФРОВАННОГО ФАЙЛА
1325
ЗАШИФРОВАТЬ ОДИН ИЛИ БОЛЕЕ ПАКЕТОВ ДАННЫХ, КОТОРЫЕ ВКЛЮЧАЮТ В СЕБЯ УКАЗАНИЕ ОДНОЙ ИЛИ БОЛЕЕ ПОЛИТИК ДОСТУПА К ФАЙЛУ, ИНФОРМАЦИЮ О ВЛАДЕНИИ ФАЙЛОМ, ЛОГ АУДИТА ДОСТУПА К ФАЙЛУ ИЛИ ИХ КОМБИНАЦИЮ
1330
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1335
1300

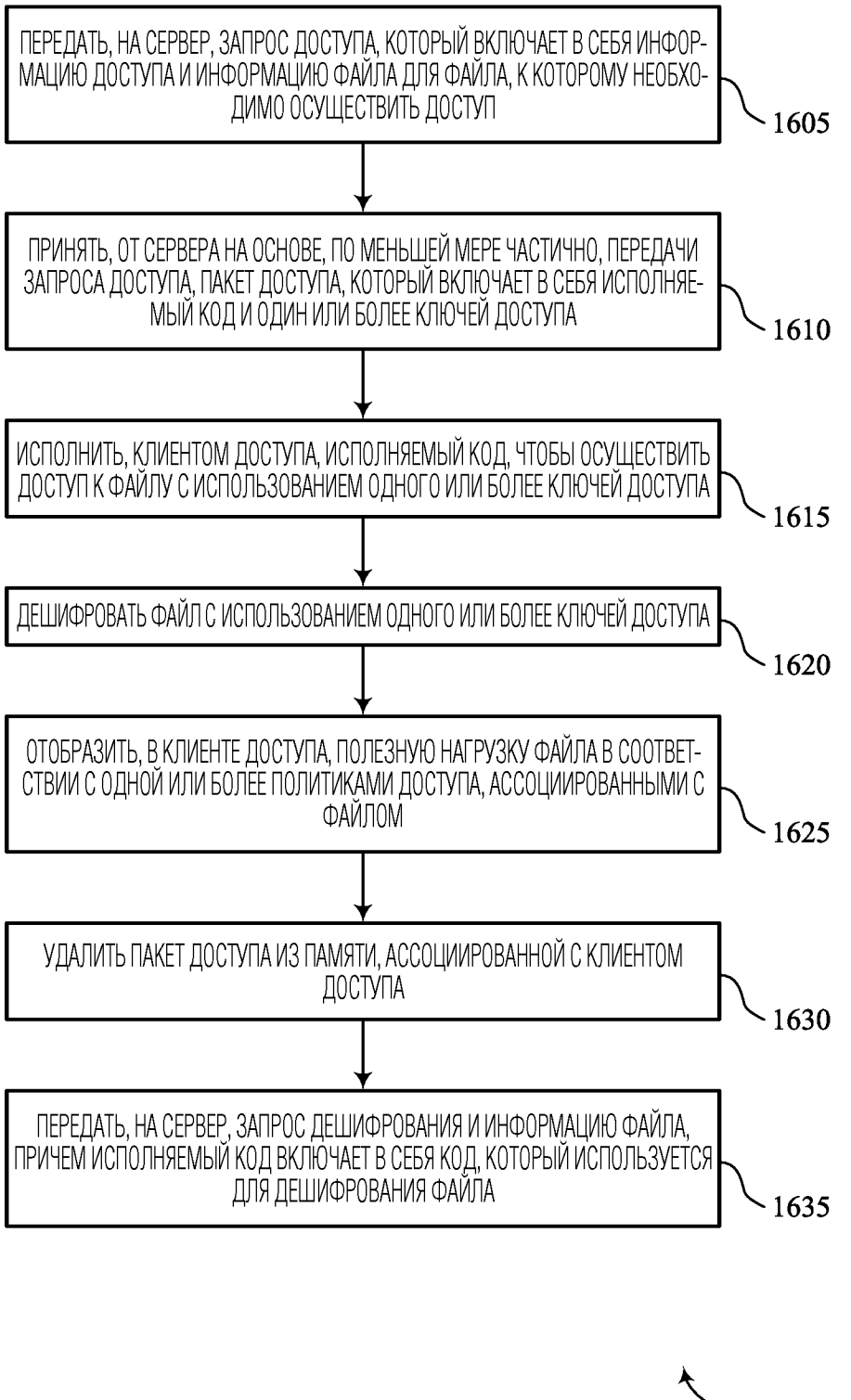
ФИГ. 13


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1405
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1410
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1415
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1420
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДЕШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА, ПРИЧЕМ ИСПОЛНЯЕМЫЙ КОД ВКЛЮЧАЕТ В СЕБЯ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА
1425
1400

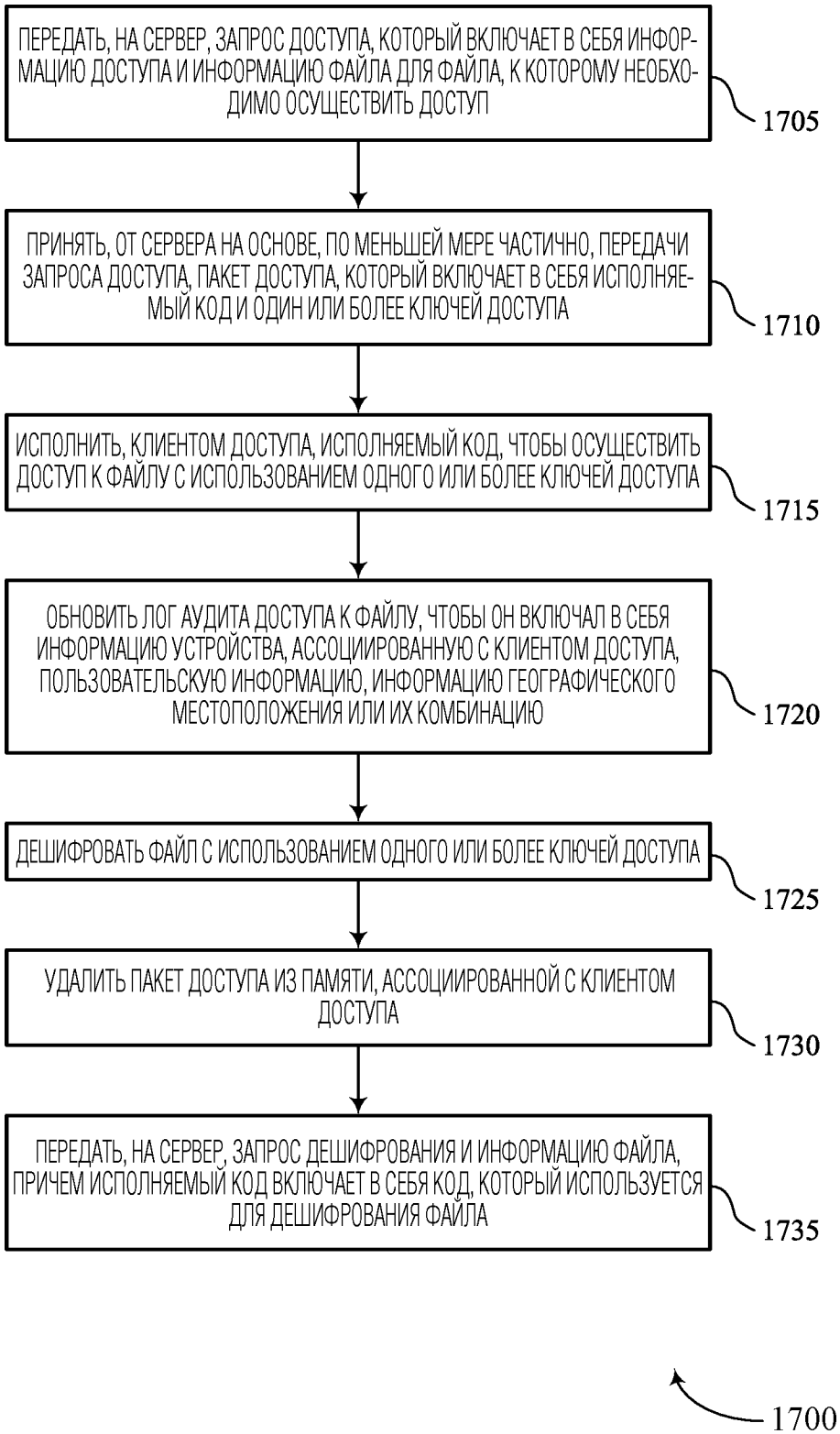
ФИГ. 14


ИДЕНТИФИЦИРОВАТЬ, В КЛИЕНТЕ ДОСТУПА, ИНФОРМАЦИЮ ВАЛИДАЦИИ, КОТОРАЯ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ КЛИЕНТА ДОСТУПА, ИНФОРМАЦИЮ КОМПЬЮТЕРА, ИНФОРМАЦИЮ УСТРОЙСТВА, ИНФОРМАЦИЮ ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ, ТОКЕН АУТЕНТИФИКАЦИИ ИЛИ ИХ КОМБИНАЦИЮ, ПРИЧЕМ ЗАПРОС ДЕШИФРОВАНИЯ ВКЛЮЧАЕТ В СЕБЯ УКАЗАНИЕ ИНФОРМАЦИИ ВАЛИДАЦИИ
1505
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1510
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ ПО МЕНЬШЕ МЕРЕ ЧАСТИЧНО ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1515
ПРИНЯТЬ ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ПАКЕТ ДАННЫХ, СОДЕРЖАЩИЙ ОДНУ ИЛИ БОЛЕЕ ОБНОВЛЕННЫХ ПОЛИТИК ДОСТУПА К ФАЙЛУ
1520
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1525
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1530
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДЕШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА, ПРИЧЕМ ИСПОЛНЯЕМЫЙ КОД ВКЛЮЧАЕТ В СЕБЯ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА
1535
1500

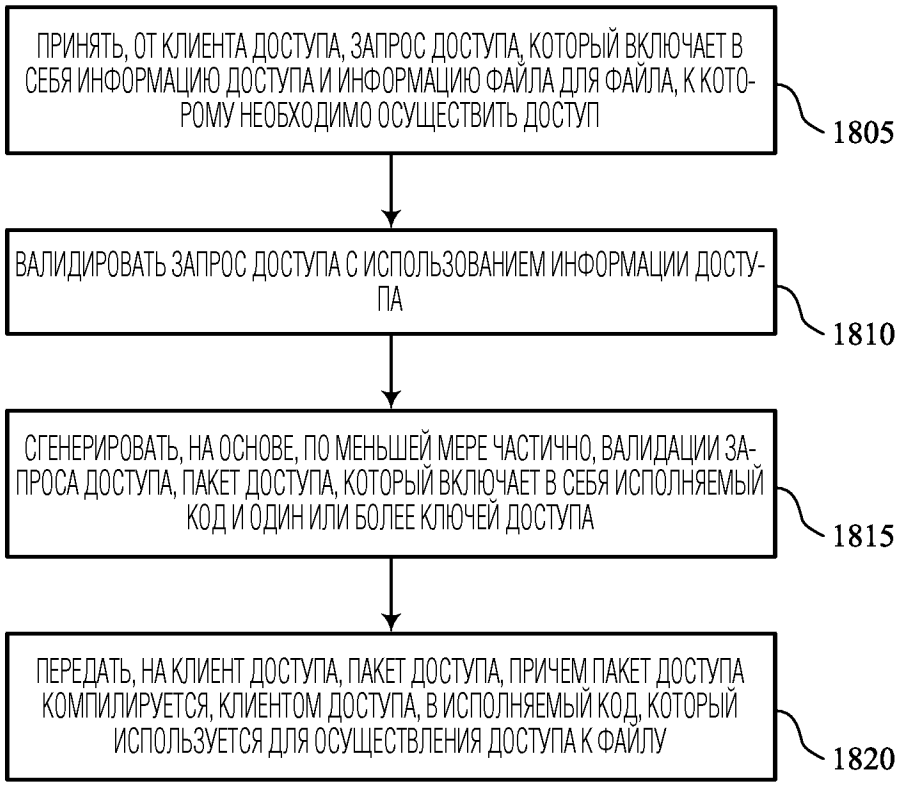
ФИГ. 15


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1605
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1610
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1615
ДЕШИФРОВАТЬ ФАЙЛ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1620
ОТОБРАЗИТЬ, В КЛИЕНТЕ ДОСТУПА, ПОЛЕЗНУЮ НАГРУЗКУ ФАЙЛА В СООТВЕТСТВИИ С ОДНОЙ ИЛИ БОЛЕЕ ПОЛИТИКАМИ ДОСТУПА, АССОЦИИРОВАННЫМИ С ФАЙЛОМ
1625
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1630
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДЕШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА, ПРИЧЕМ ИСПОЛНЯЕМЫЙ КОД ВКЛЮЧАЕТ В СЕБЯ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА
1635
1600

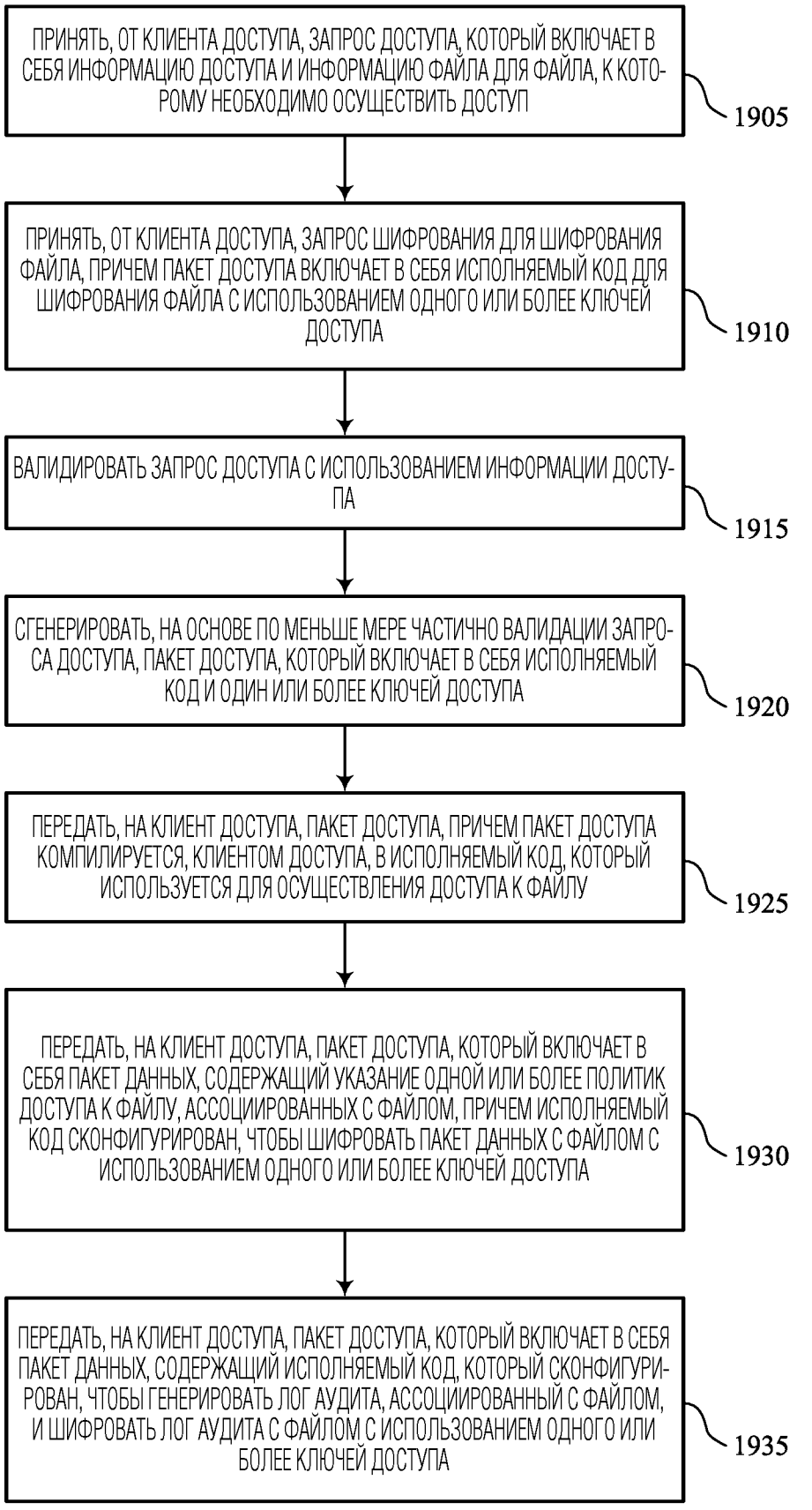
ФИГ. 16


ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1705
ПРИНЯТЬ, ОТ СЕРВЕРА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПЕРЕДАЧИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1710
ИСПОЛНИТЬ, КЛИЕНТОМ ДОСТУПА, ИСПОЛНЯЕМЫЙ КОД, ЧТОБЫ ОСУЩЕСТВИТЬ ДОСТУП К ФАЙЛУ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1715
ОБНОВИТЬ ЛОГ АУДИТА ДОСТУПА К ФАЙЛУ, ЧТОБЫ ОН ВКЛЮЧАЛ В СЕБЯ ИНФОРМАЦИЮ УСТРОЙСТВА, АССОЦИИРОВАННУЮ С КЛИЕНТОМ ДОСТУПА, ПОЛЬЗОВАТЕЛЬСКУЮ ИНФОРМАЦИЮ, ИНФОРМАЦИЮ ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ ИЛИ ИХ КОМБИНАЦИЮ
1720
ДЕШИФРОВАТЬ ФАЙЛ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1725
УДАЛИТЬ ПАКЕТ ДОСТУПА ИЗ ПАМЯТИ, АССОЦИИРОВАННОЙ С КЛИЕНТОМ ДОСТУПА
1730
ПЕРЕДАТЬ, НА СЕРВЕР, ЗАПРОС ДЕШИФРОВАНИЯ И ИНФОРМАЦИЮ ФАЙЛА, ПРИЧЕМ ИСПОЛНЯЕМЫЙ КОД ВКЛЮЧАЕТ В СЕБЯ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА
1735
1700

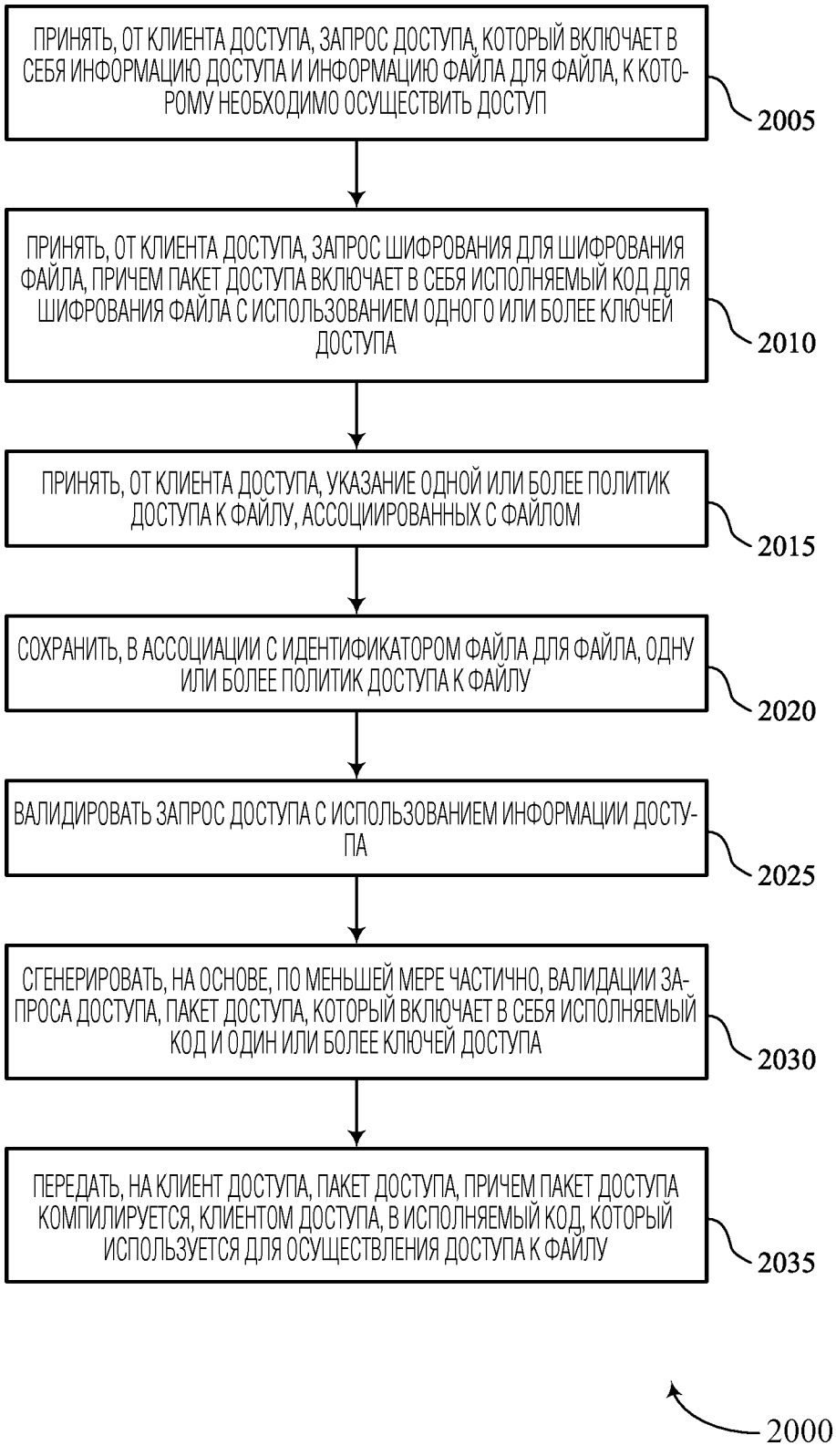
ФИГ. 17


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1805
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
1810
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1815
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
1820
1800

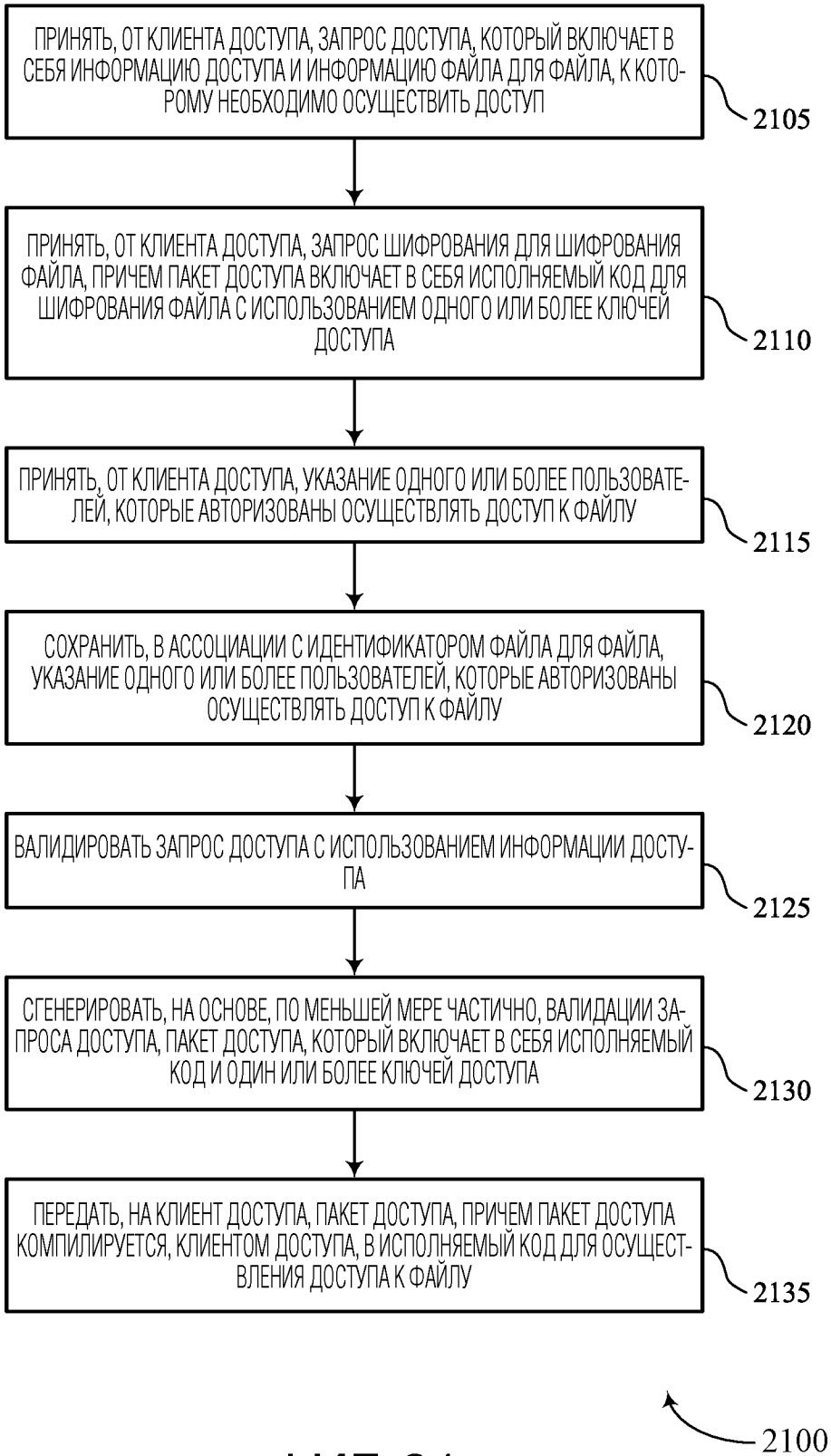
ФИГ. 18


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
1905
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ШИФРОВАНИЯ ДЛЯ ШИФРОВАНИЯ ФАЙЛА, ПРИЧЕМ ПАКЕТ ДОСТУПА ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД ДЛЯ ШИФРОВАНИЯ ФАЙЛА С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1910
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
1915
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ ПО МЕНЬШЕ МЕРЕ ЧАСТИЧНО ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1920
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
1925
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ПАКЕТ ДАННЫХ, СОДЕРЖАЩИЙ УКАЗАНИЕ ОДНОЙ ИЛИ БОЛЕЕ ПОЛИТИК ДОСТУПА К ФАЙЛУ, АССОЦИИРОВАННЫХ С ФАЙЛОМ, ПРИЧЕМ ИСПОЛНЯЕМЫЙ КОД СКОНФИГУРИРОВАН, ЧТОБЫ ШИФРОВАТЬ ПАКЕТ ДАННЫХ С ФАЙЛОМ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1930
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ПАКЕТ ДАННЫХ, СОДЕРЖАЩИЙ ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ СКОНФИГУРИРОВАН, ЧТОБЫ ГЕНЕРИРОВАТЬ ЛОГ АУДИТА, АССОЦИИРОВАННЫЙ С ФАЙЛОМ, И ШИФРОВАТЬ ЛОГ АУДИТА С ФАЙЛОМ С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
1935
1900

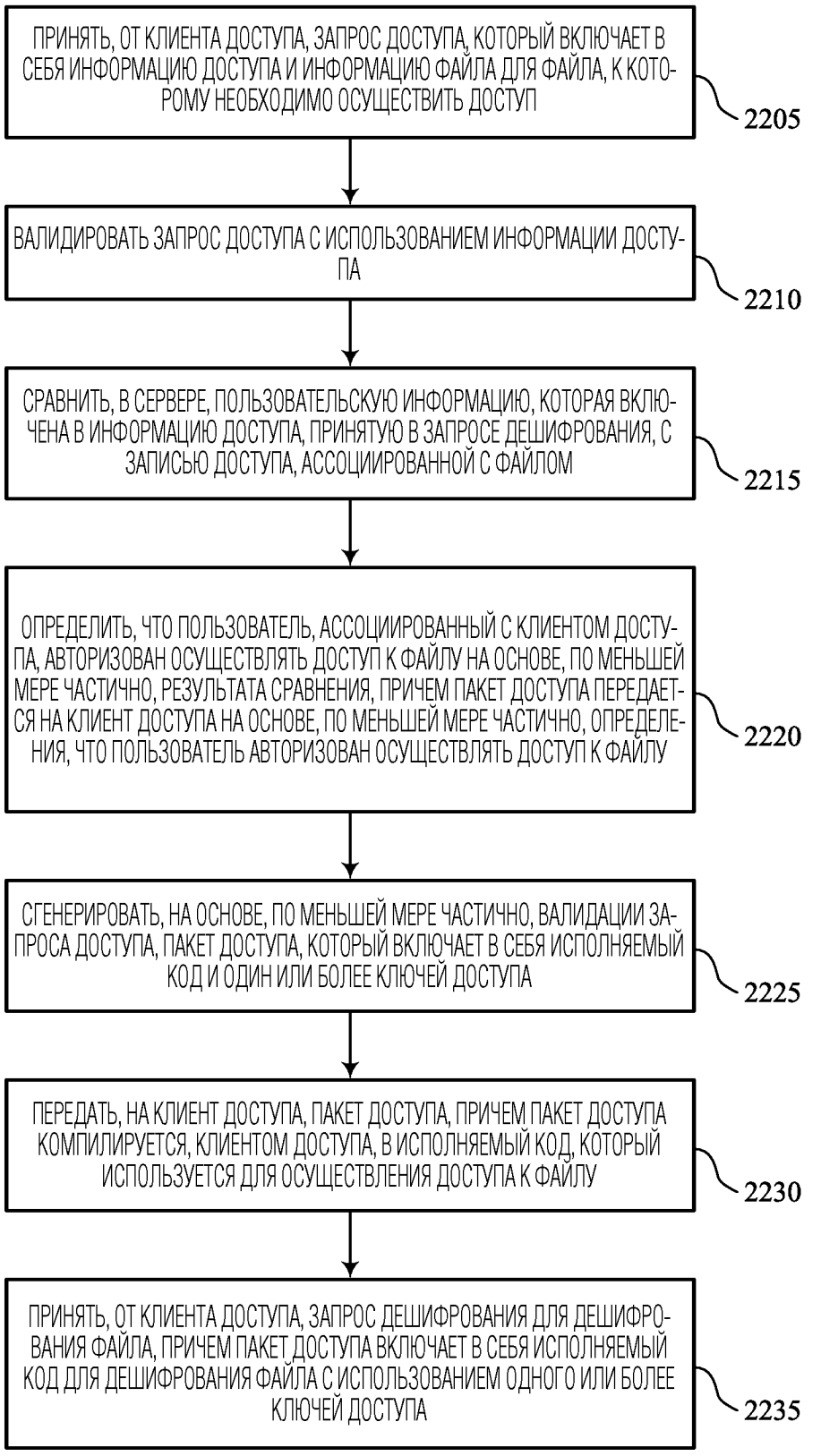
ФИГ. 19


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
2005
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ШИФРОВАНИЯ ДЛЯ ШИФРОВАНИЯ ФАЙЛА, ПРИЧЕМ ПАКЕТ ДОСТУПА ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД ДЛЯ ШИФРОВАНИЯ ФАЙЛА С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2010
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, УКАЗАНИЕ ОДНОЙ ИЛИ БОЛЕЕ ПОЛИТИК ДОСТУПА К ФАЙЛУ, АССОЦИИРОВАННЫХ С ФАЙЛОМ
2015
СОХРАНИТЬ, В АССОЦИАЦИИ С ИДЕНТИФИКАТОРОМ ФАЙЛА ДЛЯ ФАЙЛА, ОДНУ ИЛИ БОЛЕЕ ПОЛИТИК ДОСТУПА К ФАЙЛУ
2020
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
2025
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2030
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
2035
2000

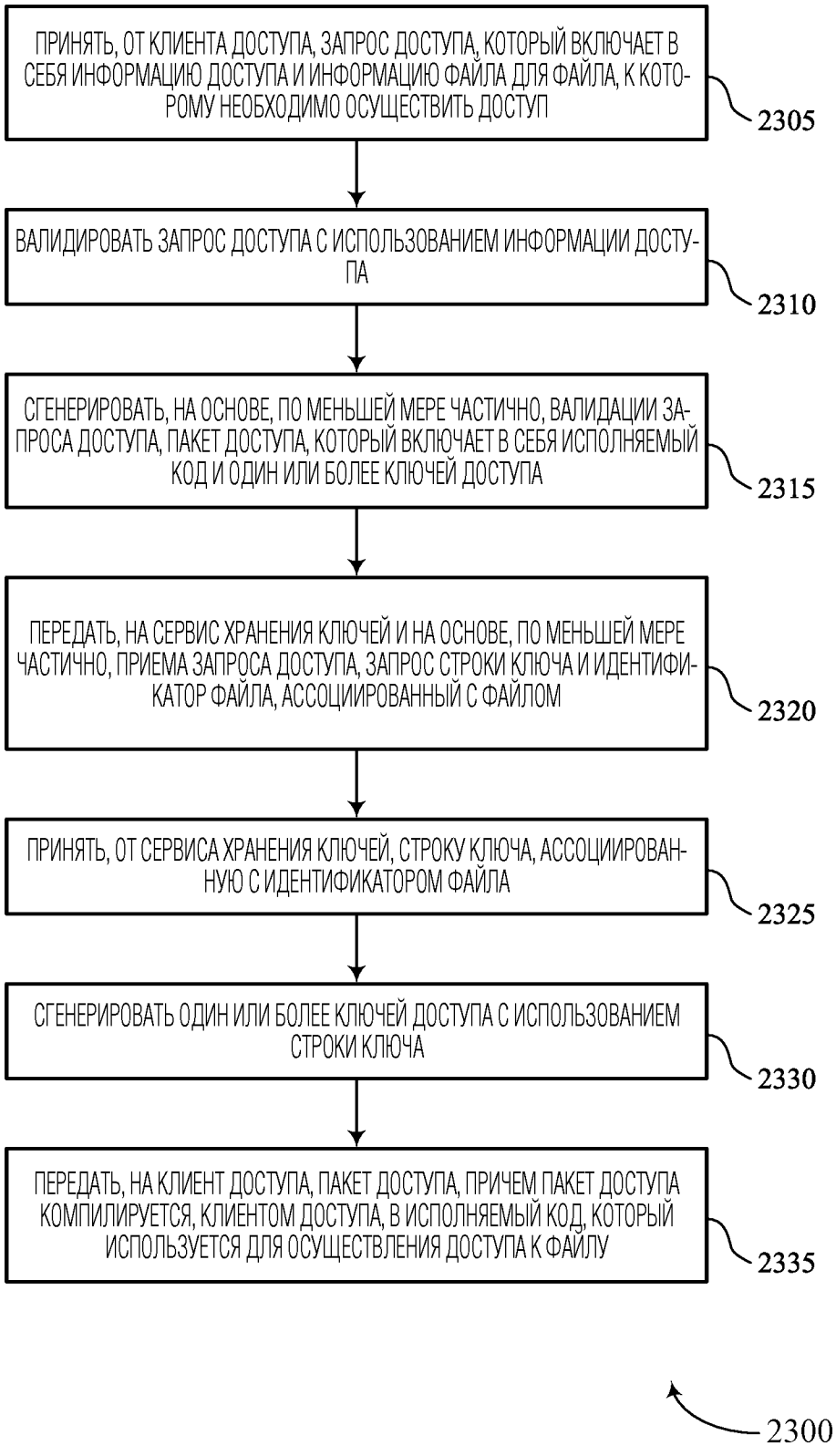
ФИГ. 20


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
2105
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ШИФРОВАНИЯ ДЛЯ ШИФРОВАНИЯ ФАЙЛА, ПРИЧЕМ ПАКЕТ ДОСТУПА ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД ДЛЯ ШИФРОВАНИЯ ФАЙЛА С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2110
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, УКАЗАНИЕ ОДНОГО ИЛИ БОЛЕЕ ПОЛЬЗОВАТЕЛЕЙ, КОТОРЫЕ АВТОРИЗОВАНЫ ОСУЩЕСТВЛЯТЬ ДОСТУП К ФАЙЛУ
2115
СОХРАНИТЬ, В АССОЦИАЦИИ С ИДЕНТИФИКАТОРОМ ФАЙЛА ДЛЯ ФАЙЛА, УКАЗАНИЕ ОДНОГО ИЛИ БОЛЕЕ ПОЛЬЗОВАТЕЛЕЙ, КОТОРЫЕ АВТОРИЗОВАНЫ ОСУЩЕСТВЛЯТЬ ДОСТУП К ФАЙЛУ
2120
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
2125
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2130
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
2135
2100

ФИГ. 21


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
2205
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
2210
СРАВНИТЬ, В СЕРВЕРЕ, ПОЛЬЗОВАТЕЛЬСКУЮ ИНФОРМАЦИЮ, КОТОРАЯ ВКЛЮЧЕНА В ИНФОРМАЦИЮ ДОСТУПА, ПРИНЯТУЮ В ЗАПРОСЕ ДЕШИФРОВАНИЯ, С ЗАПИСЬЮ ДОСТУПА, АССОЦИИРОВАННОЙ С ФАЙЛОМ
2215
ОПРЕДЕЛИТЬ, ЧТО ПОЛЬЗОВАТЕЛЬ, АССОЦИИРОВАННЫЙ С КЛИЕНТОМ ДОСТУПА, АВТОРИЗОВАН ОСУЩЕСТВЛЯТЬ ДОСТУП К ФАЙЛУ НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, РЕЗУЛЬТАТА СРАВНЕНИЯ, ПРИЧЕМ ПАКЕТ ДОСТУПА ПЕРЕДАЕТСЯ НА КЛИЕНТ ДОСТУПА НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ОПРЕДЕЛЕНИЯ, ЧТО ПОЛЬЗОВАТЕЛЬ АВТОРИЗОВАН ОСУЩЕСТВЛЯТЬ ДОСТУП К ФАЙЛУ
2220
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2225
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
2230
ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДЕШИФРОВАНИЯ ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА, ПРИЧЕМ ПАКЕТ ДОСТУПА ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД ДЛЯ ДЕШИФРОВАНИЯ ФАЙЛА С ИСПОЛЬЗОВАНИЕМ ОДНОГО ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2235
2200

ФИГ. 22


ПРИНЯТЬ, ОТ КЛИЕНТА ДОСТУПА, ЗАПРОС ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИНФОРМАЦИЮ ДОСТУПА И ИНФОРМАЦИЮ ФАЙЛА ДЛЯ ФАЙЛА, К КОТОРОМУ НЕОБХОДИМО ОСУЩЕСТВИТЬ ДОСТУП
2305
ВАЛИДИРОВАТЬ ЗАПРОС ДОСТУПА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ ДОСТУПА
2310
СГЕНЕРИРОВАТЬ, НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ВАЛИДАЦИИ ЗАПРОСА ДОСТУПА, ПАКЕТ ДОСТУПА, КОТОРЫЙ ВКЛЮЧАЕТ В СЕБЯ ИСПОЛНЯЕМЫЙ КОД И ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА
2315
ПЕРЕДАТЬ, НА СЕРВИС ХРАНЕНИЯ КЛЮЧЕЙ И НА ОСНОВЕ, ПО МЕНЬШЕЙ МЕРЕ ЧАСТИЧНО, ПРИЕМА ЗАПРОСА ДОСТУПА, ЗАПРОС СТРОКИ КЛЮЧА И ИДЕНТИФИКАТОР ФАЙЛА, АССОЦИИРОВАННЫЙ С ФАЙЛОМ
2320
ПРИНЯТЬ, ОТ СЕРВИСА ХРАНЕНИЯ КЛЮЧЕЙ, СТРОКУ КЛЮЧА, АССОЦИИРОВАННУЮ С ИДЕНТИФИКАТОРОМ ФАЙЛА
2325
СГЕНЕРИРОВАТЬ ОДИН ИЛИ БОЛЕЕ КЛЮЧЕЙ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ СТРОКИ КЛЮЧА
2330
ПЕРЕДАТЬ, НА КЛИЕНТ ДОСТУПА, ПАКЕТ ДОСТУПА, ПРИЧЕМ ПАКЕТ ДОСТУПА КОМПИЛИРУЕТСЯ, КЛИЕНТОМ ДОСТУПА, В ИСПОЛНЯЕМЫЙ КОД, КОТОРЫЙ ИСПОЛЬЗУЕТСЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДОСТУПА К ФАЙЛУ
2335
2300

ФИГ. 23