(19) Евразийское патентное ведомство

(11) 044196 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.07.28

(21) Номер заявки
201991351

(22) Дата подачи заявки
2017.12.18

(51) Int. Cl. ***G06F 21/62*** (2013.01)
H04W 12/08 (2009.01)

(54) СПОСОБ КОНТРОЛЯ И ОГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ ЭЛЕКТРОННЫМ УСТРОЙСТВОМ

(31) **102016000127897; 102017000070573**
(32) **2016.12.19; 2017.06.23**
(33) **IT**
(43) **2019.11.29**
(86) **PCT/IB2017/058056**
(87) **WO 2018/116124 2018.06.28**

(71)(73) Заявитель и патентовладелец:
СЭЙНТС ГРУП С.Р.Л. (IT)

(72) Изобретатель:
Пини Джанлука, Джорджетти Джанкарло (IT)

(74) Представитель:
Угрюмов В.М., Гизатуллина Е.М., Строкова О.В., Костюшенкова М.Ю., Гизатуллин Ш.Ф., Парамонова К.В. (RU)

(56) US-B1-8412154
US-B1-8194581
US-A1-2013017806
US-A1-2011185399
US-A1-2008070609
US-A1-2004003279

(57) Предложен способ контроля и ограничения доступа к подключению к данным электронным устройством, которое содержит средство для избирательного разрешения/прекращения подключения к данным, причем указанный способ предусматривает следующие стадии: a) обнаружение начального и конечного моментов времени каждого доступа к подключению к данным в течение предопределенного промежутка времени; b) подсчет с нарастающим итогом общей продолжительности доступов к подключению к данным в течение указанного предопределенного промежутка времени; и c) если общая продолжительность доступов к подключению к данным достигает значения, равного предварительно заданному значению максимальной продолжительности, до конца указанного предопределенного промежутка времени, срабатывание вышеупомянутого средства разрешения/прекращения для прекращения подключения к данным до конца указанного предопределенного промежутка времени. Более того, способ согласно настоящему изобретению может позволять получать подробный отчет и обеспечивать проверку в реальном времени - через удаленный доступ - доступов и их продолжительностей в каждый веб-сайт, времени использования отдельных приложений, инсталлированных на устройстве, списка выполненных, полученных или потерянных вызовов, текстов посланных и полученных сообщений SMS, а также статического изображения (так называемого "скриншота") контролируемых устройств.

044196 B1

044196 B1

Область техники, к которой относится настоящее изобретение

Настоящее изобретение относится к реализуемому посредством электронного процессора способу регулирования доступа к подключению к данным электронным устройством, причем подключение к данным предусматривает подключение к сети Интернет.

Предлагаемый способ может обеспечивать регулирование общей продолжительности доступов в определенном промежутке времени или может обеспечивать доступ к подключению исключительно в течение определенных временных слотов.

Предлагаемый способ может дополнительно обеспечивать дистанционный контроль телефонной книги, перечня входящих и исходящих вызовов, содержания переданных и принятых сообщений, геолокализации и хронологии посещенных вебсайтов путем предоставления подробных данных относительно времени, затраченного на каждый отдельный сайт.

Предшествующий уровень техники настоящего изобретения

В настоящее время использование смартфона и ПК для навигации в режиме онлайн стало компонентом повседневной жизни детей и подростков. Зачастую эти молодые люди фактически имеют доступ к онлайновым приложениям без контроля со стороны родителей в части продолжительности подключения и предлагаемого характера информации. Онлайн-игры и социальные сети находятся среди чаще всего посещаемых веб-страниц, где пользователи помоложе проводят большую часть своего времени.

Сегодня единственный способ, который могут принять родители для контроля и управления использованием Интернета их собственными детьми, - это держать их под постоянным контролем, но этого трудно добиться.

Краткое раскрытие настоящего изобретения

Технической задачей, поставленной и решенной настоящим изобретением, является создание способа, позволяющего устранить вышеупомянутые недостатки известного уровня техники.

Настоящее изобретение относится к программе для процессора и к соответствующему реализуемому им способу регулирования и контроля доступа к сети Интернет электронным устройством, например, настольным компьютером, смартфоном или планшетом.

Вышеупомянутая задача решается способом по независимому п.1 формулы изобретения и программой для процессора по независимому п.11 формулы изобретения.

Предпочтительные признаки настоящего изобретения изложены в зависимых пунктах формулы изобретения.

Способ согласно настоящему изобретению обеспечивает регулирование продолжительности доступа к сети передачи данных (в том числе к сети Интернет) в течение предопределенного промежутка времени, например, на ежедневной, еженедельной или ежемесячной основе.

В соответствии с предпочтительными вариантами осуществления способ согласно настоящему изобретению обеспечивает работу в фоновом режиме в операционной системе ПК, планшета или смартфона, принудительным образом в отношении настроек подключения к данным, независимо от того, передаются ли данные с использованием модуля идентификации абонента (SIM-карты), или используется подключение к внешней сети (ЛВС или Wi-Fi).

Способ согласно настоящему изобретению реализуется посредством программного обеспечения, которое должно быть инсталлировано в электронном устройстве пользователя, который хочет контролировать доступ к сети, или просто выполняется этим устройством.

Конфигурация используемых программным обеспечением настроек для ограничения навигационных данных возможна лишь администратором, осуществляющим регистрацию на стадии инсталляции или первого запуска программного обеспечения. Администратор в любой момент времени может осуществить доступ к сегменту программы, выделенному для регулирования ограничений путем ввода идентификационных данных для проверки подлинности, которые запоминаются на указанной стадии регистрации.

Запрос идентификационных данных для проверки подлинности для изменения операционных параметров программы необходим во избежание самовольного изменения настроек управления, заданных администратором (например, родителем), конечным пользователем (например, несовершеннолетним сыном) этого устройства.

Преимущественно, настоящее изобретение позволяет родителям осуществлять контроль и ограничение навигации по сети Интернет их детьми предопределенным образом, который не может быть изменен последними.

В соответствии с одним предпочтительным аспектом настоящего изобретения указанное ограничение можно осуществлять избирательно для каждой программы/программного приложения (далее просто приложение), инсталлированного на контролируемом устройстве.

Кроме того, могут предусматриваться механизмы поощрения в случае честного поведения, когда предел времени для навигации данных в течение предварительно установленного периода времени не достигнут, и механизмы наказания в случае попыток нарушения настроек программного обеспечения конечным пользователем.

Указанные механизмы побуждают конечных пользователей более тщательно самостоятельно

управлять временем, выделенным им для подключения.

Еще одно важное преимущество, достигаемое благодаря способу согласно настоящему изобретению, заключается в эффективном способствовании решению проблем, связанных с чрезмерным использованием Интернета, в частности, приложений в социальных сетях, несовершеннолетними, а также с контролем доступа к содержанию, не подходящему для их возраста.

Более того, настоящее изобретение может реализовать действенный инструмент противодействия патологическим склонностям к азартным играм или подобным патологическим склонностям помимо предотвращения явления кибербуллинга.

Другие преимущества, признаки и способы использования настоящего изобретения будут очевидными из последующего подробного описания некоторых вариантов осуществления, приведенных в качестве примера, а не в целях ограничения объема настоящего изобретения.

Краткое описание фигур

В приведенном ниже разделе описания приведены ссылки на прилагаемые фигуры, где

на фиг. 1 представлена схема, иллюстрирующая в качестве примера некоторые стадии первого предпочтительного варианта осуществления способа согласно настоящему изобретению; и

на фиг. 2 представлена схема, иллюстрирующая в качестве примера некоторые стадии второго предпочтительного варианта осуществления способа согласно настоящему изобретению.

Вышеупомянутые фигуры приведены исключительно в качестве примера, а не в целях ограничения объема настоящего изобретения.

Подробное раскрытие предпочтительных вариантов осуществления

Предлагаемый способ, реализуемый электронным процессором, предназначен для контроля и ограничения доступа к подключению к данным электронным устройством, оснащенным средствами для избирательного разрешения/прекращения подключения к сети передачи данных в соответствии с описанными ниже режимами.

В настоящем описании выражение "подключение к данным" означает или включает в себя подключение к сети Интернет.

Способ согласно настоящему изобретению предназначен для кодирования в качестве программного обеспечения для инсталляции или просто запуска на электронном устройстве, подлежащем контролю, предпочтительно в виде Приложения.

Программное обеспечение может выпускаться непосредственно в режиме онлайн или поддерживаться аппаратным устройством, таким как USB-накопитель в форме ключа, для подключения к ПК.

В последнем случае способ преимущественно может обеспечить применение механизма для автоматического блокирования ПК, к которому подключен ключ, в случае несанкционированного удаления его. Для того чтобы выполнить безопасное удаление ключа, способ предпочтительно требует ввести идентификационные данные для доступа, подлежащие аутентификации, что будет подробнее объяснено ниже.

На стадии инсталляции/первого запуска программного обеспечения может предусматриваться ввод или получение данных доступа администратора. Данные доступа включают в себя идентификационные данные (такие как имя пользователя и пароль, предпочтительно двойной буквенно-цифровой пароль) и/или биометрические данные (например, отпечаток пальца) администратора. Эти данные доступа хранятся в базе данных или сервере, который может быть удаленным относительно контролируемого устройства.

Администратор является единственным, кто имеет уровень авторизации, необходимый для изменения данных для ограничения доступа к сети передачи данных, которые могут задаваться с помощью предлагаемого способа, таких как временные ограничения, максимальная продолжительность (продолжительности) доступов, контролируемое конкретное Приложение и т.д., а также единственным, кому разрешен доступ к данным, связанным с навигацией, вызовами и сообщениями, хранящимися в вышеупомянутой базе данных.

Предпочтительно, на этой предварительной стадии предусматривается также хранение телематических адресов администратора в случае, если предусмотрена отправка тревожного сообщения этому администратору, если кто-то пытается изменить настройки ограничения, предоставляя данные доступа, отличающиеся от хранящихся данных доступа, то есть, в случае непрохождения аутентификации.

При инсталляции программного обеспечения или его запуска в первый раз необходимо задать опции для блокирования доступа в сеть, что может представлять собой простое включение/выключение подключения, или задать четко сформулированное и индивидуализированное условие продолжительностей доступов для каждой программы/программного Приложения (далее просто именуемого "Приложением"), инсталлированной/ инсталлированного в электронном устройстве.

Способ, реализованным программным обеспечением, по существу реализует ограничение времени доступа к подключению к данным электронным устройством, в котором запущено это программное обеспечение.

Указанное ограничение может применяться в целом ко всему электронному устройству или избирательно и независимо к одному или нескольким Приложениям, инсталлированным в самом устройстве.

В соответствии с одним предпочтительным вариантом осуществления способа ограничение может

реализовываться посредством пороговой системы, так что при достижении максимальной продолжительности подключения, заданной администратором, в предопределенном промежутке времени подключение прерывается. Ограничение задается в предопределенном промежутке времени, которым могут быть один или несколько часов, дней или месяцев. Администратором может задаваться даже продолжительность предопределенного промежутка времени.

Предлагаемый способ по существу обеспечивает обнаружение в предопределенном промежутке времени начального и конечного моментов времени каждого доступа к сети передачи данных. Общая продолжительность доступов к сети в предопределенном промежутке времени подсчитывается с нарастающим итогом. Иными словами, отсчет времени доступа включается в начальный момент времени каждого доступа в сеть передачи данных и отключается в конечный момент времени каждого доступа, чтобы снова начаться при следующем доступе.

Если отсчитанное время доступа достигает значения, равного величине максимальной продолжительности, заданной администратором, до истечения предопределенного промежутка времени, срабатывает средство разрешения/прекращения подключения, чтобы прекратить подключение к данным до конца предопределенного промежутка времени. Таким образом, электронному устройству запрещен доступ в сеть передачи данных до конца предопределенного промежутка времени, когда начнется новый предопределенный промежуток времени (который может быть равным предыдущему или отличным от него), и снова можно будет выполнить подключение к данным в течение заданной максимальной продолжительности времени (которая может быть равной предыдущей или отличной от нее).

В соответствии с одним предпочтительным аспектом предлагаемого способа отсчитывать продолжительность доступов к подключению к данным можно одновременно для одного или нескольких Приложений, инсталлированных в устройстве, в течение одного и того же предопределенного промежутка времени. Альтернативно, можно принять индивидуализированные настройки для каждого приложения как для предопределенного промежутка времени, учитываемого для контроля доступов к подключению к данным, так и для разрешенной максимальной продолжительности подключения, чтобы обеспечить максимальную кастомизацию пределов, накладываемых на использование конкретных Приложений.

В этом случае способ предусматривает одновременное обнаружение для каждого Приложения в течение конкретного предопределенного промежутка времени начального и конечного моментов времени каждого доступа к сети передачи данных. Общая продолжительность доступов к сети в течение предопределенного промежутка времени подсчитывается с нарастающим итогом для каждого Приложения согласно вышеупомянутым режимам.

Если время доступа, отсчитанное для некоторого Приложения, до конца предопределенного промежутка времени достигает значения, равного значению максимальной продолжительности, заданному администратором для этого конкретного Приложения, срабатывает средство разрешения/прекращения подключения для прекращения подключения к данным в отношении рассматриваемого Приложения до конца предопределенного промежутка времени.

Таким образом, этому единственному Приложению запрещен доступ к сети передачи данных до конца предопределенного промежутка времени, когда начнется новый предопределенный промежуток времени (который может быть равным предыдущему или отличным от него), и снова можно будет выполнить подключение к данным в течение заданной максимальной продолжительности времени (которая может быть равной предыдущей или отличной от нее).

В одном конкретном случае реализации способа предусматривается, что заданная максимальная продолжительность доступа к подключению к данным равна предопределенному промежутку времени, который, например, может равняться одному часу в день, скажем с 19.00 до 20.00.

Проще говоря, такая конфигурация в действительности реализует назначение временного слота доступа в сеть передачи данных.

Даже в этом случае способ регулирования доступа к сети передачи данных может применяться индивидуально к одному или нескольким Приложениям, инсталлированным в электронном устройстве. Иными словами, для каждого контролируемого Приложения может задаваться разное значение максимальной продолжительности подключения и разный промежуток времени, в течение которого должна подсчитываться продолжительность доступов к подключению, чтобы выполнять контроль и ограничение доступа к сети независимо для каждого из них.

В соответствии с одним преимущественным аспектом способа согласно настоящему изобретению, когда программное обеспечение запускается в электронном устройстве, настройки, относящиеся к дате и времени этого устройства, изменить невозможно, если не ввести заранее данные доступа администратора. Таким образом, исключается возможность обхода конечными пользователями устройства ограничений времени, установленных для доступа к сети передачи данных. Наиболее общим случаем использования настоящего изобретения мог бы быть случай, в котором администратором является родитель, а конечным пользователем является ребенок или, во всяком случае, несовершеннолетний.

В соответствии с одним предпочтительным вариантом осуществления предлагаемого способа может предусматриваться и избирательно активироваться механизм поощрения для автоматического продления времени, предоставляемого для доступа к сети передачи данных, если до конца предопределенно-

го промежутка времени максимальное значение предоставленной продолжительности не достигнуто.

В частности, если до конца указанного предопределенного промежутка времени общая продолжительность доступов в Интернет не достигает значения, равного значению максимальной продолжительности, для следующего предопределенного промежутка времени задается новое значение максимальной продолжительности доступа к сети Интернет, причем это новое значение максимальной продолжительности выше предыдущего. Предпочтительно, новое значение увеличивается пропорционально разнице между отсчитанной общей продолжительностью доступов к сети и заданным значением максимальной продолжительности.

Соответственно, может предусматриваться и автоматически активироваться и механизм санкций для уменьшения максимальной заданной продолжительности, если предпринимаются попытки нарушения данных доступа администратора. Указанный механизм санкций может активироваться автоматически даже в случае обнаружения нескольких успешных аутентификаций (клонирование учетной записи администратора).

В частности, если кто-то пытается зайти в настройки программного обеспечения, и данные доступа не аутентифицированы, максимальная продолжительность доступа к сети Интернет в следующем предопределенном промежутке времени уменьшается. Предпочтительно, новая максимальная продолжительность уменьшается пропорционально числу неудачных аутентификаций.

Реализованный способ может дополнительно применяться для проведения проверки, даже дистанционно, навигационных данных рассматриваемого электронного устройства.

В частности, может предусматриваться получение информации, относящейся к данным, полученным при навигации устройством, таким как адрес посещенных вебстраниц, дата соответствующего посещения и/или время использования каждого Приложения.

Кроме того, может предусматриваться получение информации, относящейся к присутствию конкретных слов и/или содержания в тексте сообщений SMS, посланных посредством рассматриваемого электронного устройства, или в полях поиска посредством браузера рассматриваемого электронного устройства.

Указанные информация и полученные данные хранятся в базе данных, которая может находиться снаружи или внутри рассматриваемого электронного устройства.

Доступ к указанной базе данных может осуществляться посредством любого электронного устройства, в котором выполняется программное обеспечение согласно настоящему изобретению, после аутентификации данных доступа администратора.

В частности, список слов и/или содержание, присутствие которых должно контролироваться, могут храниться в специальной базе данных или "стоп-листе".

Указанный список может кастомизироваться администратором путем добавления новых слов/содержания или удаления слов/содержания, уже существующих в списке.

В соответствии с предпочтительными вариантами осуществления возможно получение ежедневного отчета о действиях, выполненных посредством устройства, в котором инсталлировано программное обеспечение согласно настоящему изобретению, путем выделения слов/содержания, хранящихся в вышеупомянутом стоп-листе.

В соответствии с одним дополнительным аспектом, когда в устройстве, в котором исполняется программное обеспечение, инсталлировано новое Приложение, или повторно инсталлировано ранее удаленное Приложение, доступ этого Приложения к подключению к данным запрещен и может быть разрешен только посредством аутентификации данных доступа администратора.

Кроме того, может предусматриваться система для автоматической посылки уведомления о попытках несанкционированного доступа к настройкам программного обеспечения на телематический адрес администратора, например, посредством SMS/почты/WA/Telegram.

В соответствии с одной дополнительной версией реализованного способа вышеупомянутые ограничения времени можно применять даже в общем к использованию онлайн или оффлайн Приложений игр или социальных сетей.

Программное приложение согласно настоящему изобретению может разрабатываться совместимым с IOS, Android, платформами Windows Phone и операционными системами Windows. Если разработано с использованием аппаратной поддержки, оно может включаться в немодифицируемый USB-накопитель в форме ключа, который может извлекаться из ПК только после аутентификации администратора. Предпочтительно, если он извлекается из ПК несанкционированно, полностью блокируется его использование.

В соответствии с дополнительными предпочтительными вариантами осуществления способа согласно настоящему изобретению может предусматриваться, что данные, относящиеся к доступам в сеть передачи данных одного или нескольких устройств, хранятся в реальном времени в базе данных, доступной администратору посредством дополнительного дистанционного устройства, в котором прогоняется исполняется программное обеспечение.

В зависимости от конкретной конфигурации программного обеспечения, настраиваемого на стадии первого запуска или инсталляции, возможна реализация следующих режимов способа: режим "обнару-

жение" или режим "отображение".

Использование в режиме "обнаружение" происходит, главным образом, в фоновом режиме путем автоматического получения и сохранения в базе данных информации о подключении к данным конкретного электронного устройства.

Использование в режиме "отображение" обеспечивает доступ к информации (и принятие ее во внимание) о подключениях к данным одного или нескольких связанных электронных устройств, в которых исполняется программное обеспечение согласно настоящему изобретению, а также изменение настроек для ограничения продолжительности подключений для любого связанного устройства, и это прерогатива владельца уровня авторизации администратора.

При первом запуске программного обеспечения в электронном устройстве необходимо выбрать режим использования "обнаружение" или "отображение", который впоследствии может быть изменен администратором.

Предпочтительные реализации для выбора и настройки режимов "обнаружение" или "отображение" для запуска программного обеспечения согласно настоящему изобретению проиллюстрированы на прилагаемых фиг. 1 и 2 соответственно.

В случае выбора режима "обнаружения" запрашивается ввод PIN-кода, требуемого для выполнения дополнительных последующих процедур для гарантии его защиты. Благодаря этому коду впоследствии можно изменить выбранный режим, изменить сам PIN (персональный идентификационный номер) или увязать устройство, в котором исполняется программное обеспечение, для осуществления его контроля даже дистанционно.

Что касается режима "отображение", для своей активации он требует аутентификации. Администратор может регистрироваться в соответствии с тем, что было сказано ранее, например, путем ввода адреса электронной почты и пароля, и доступ разрешается только после подтверждения правильности введенных данных посредством ссылки подтверждения.

После логина можно увязать одно или несколько подлежащих контролю устройств и отображать данные, относящиеся к действиям, выполняемым ими. Предпочтительно можно также обеспечить показ удаленного рабочего стола экрана связанных устройств.

В частности, для каждого связанного устройства, в котором исполняется программное обеспечение согласно настоящему изобретению, можно извлекать, отображать и/или верифицировать одно или более из следующего:

данные о продолжительности (например, всего, еженедельно, ежедневно) и дата/время доступа к сети передачи данных каждого Приложения, инсталлированного в связанном устройстве;

снимок экрана (скриншот) или показ удаленного рабочего стола экрана;

список адресов сайтов, к которым обращался браузер, и связанная дата обращения даже в случае навигации в скрытом режиме;

список (выполненных, потерянных, полученных) вызовов и (посланных, полученных) сообщений SMS;

блокирование данных навигации; и

настройка времени использования.

В частности, можно получать временные скриншоты экрана устройства, на котором инсталлировано предлагаемое программное обеспечение, чтобы в данный момент времени (например, в определенное время, когда устройство использовалось не контролируемым несовершеннолетним) знать содержание экрана устройства.

Кроме того, может обеспечиваться возможность доступа к мультимедийным каналам рассматриваемого устройства, в частности, к базе данных фотографий/видео (галерея изображений) и/или к камерам для проверки содержания хранимых в них фотографий и/или видео.

В частности, способ согласно настоящему изобретению может позволять получать подробный отчет и обеспечивать проверку в реальном времени - через удаленный доступ - доступов и их продолжительностей в каждый веб-сайт, времени использования отдельных приложений, инсталлированных в устройстве, списка выполненных, полученных или потерянных вызовов, текстов посланных и полученных сообщений SMS, а также статического изображения (так называемого "скриншота") контролируемых устройств.

Настоящее изобретение описано со ссылками на предпочтительные варианты осуществления. Следует понимать, что могут существовать и другие варианты осуществления в пределах сущности и объема настоящего изобретения, определенных объемом правовой защиты прилагаемой формулы изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ контроля и ограничения доступа к данным электронным устройством, при этом указанное электронное устройство содержит процессор, память и модули для избирательного разрешения/прекращения доступа к данным, причем указанный способ предусматривает следующие стадии:

а) предоставление данных доступа администратора, причем указанные данные доступа содержат идентификационные данные и/или биометрические данные; и

b) хранение указанных данных доступа в базе данных;

c) обнаружение начального и конечного моментов времени каждого доступа к данным в течение предопределенного промежутка времени;

d) подсчет с нарастающим итогом общей продолжительности доступов к данным в течение указанного предопределенного промежутка времени согласно следующему режиму:

i) подсчет активируют в начальный момент времени каждого доступа к данным, и

ii) подсчет прекращают в конечный момент времени каждого доступа к данным;

e) если общая продолжительность доступов к данным достигает значения, равного предварительно заданному значению продолжительности, до конца указанного предопределенного промежутка времени, срабатывание вышеупомянутых модулей разрешения/прекращения для прекращения доступа к данным до конца указанного предопределенного промежутка времени, если общая продолжительность доступов к данным не достигает значения, равного указанному значению продолжительности, до конца указанного предопределенного промежутка времени, на следующий предопределенный промежуток времени задают новое значение продолжительности доступа к данным, причем указанное новое значение продолжительности выше предыдущего значения пропорционально разнице между отсчитанной общей продолжительностью доступов к данным и предварительно заданным значением продолжительности, причем

указанное предварительно заданное значение продолжительности может быть задано и/или изменено после аутентификации указанных данных доступа, причем если указанные данные доступа не аутентифицируются, продолжительность доступа к данным в следующем предопределенном промежутке времени уменьшают пропорционально числу неудачных аутентификаций.

2. Способ по п.1, предусматривающий следующие дополнительные стадии:

f) получение информации, касающейся данных, полученных при подключении к сети передачи данных устройством, которая содержит: адрес посещенных веб-страниц, дату/время соответствующих посещений и/или время использования каждого Приложения, инсталлированного на выбранном электронном устройстве; и

g) сохранение указанной информации в базе данных.

3. Способ по любому из предшествующих пунктов, в котором указанный предопределенный промежуток времени характеризуется продолжительностью один или несколько часов, дней, недель или месяцев.

4. Способ по любому из предшествующих пунктов, в котором на указанной стадии f) дополнительно предусматривают предоставление телематических адресов указанного администратора,

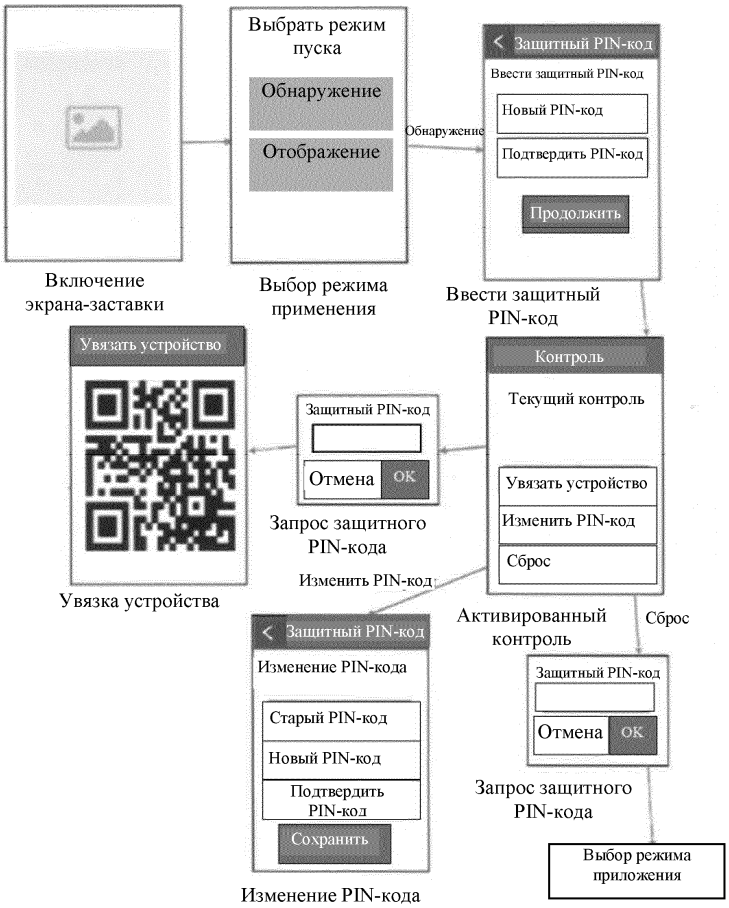
причем, если указанные данные доступа не аутентифицируются, предусматривают отправку тревожного сообщения на телематические адреса указанного администратора.

5. Способ по любому из предшествующих пунктов, который выполняют одновременно для одного или нескольких Приложений, инсталлированных на электронном устройстве, причем для каждого из указанных Приложений предварительно задают соответствующий предопределенный промежуток времени и соответствующее значение продолжительности доступа к данным.

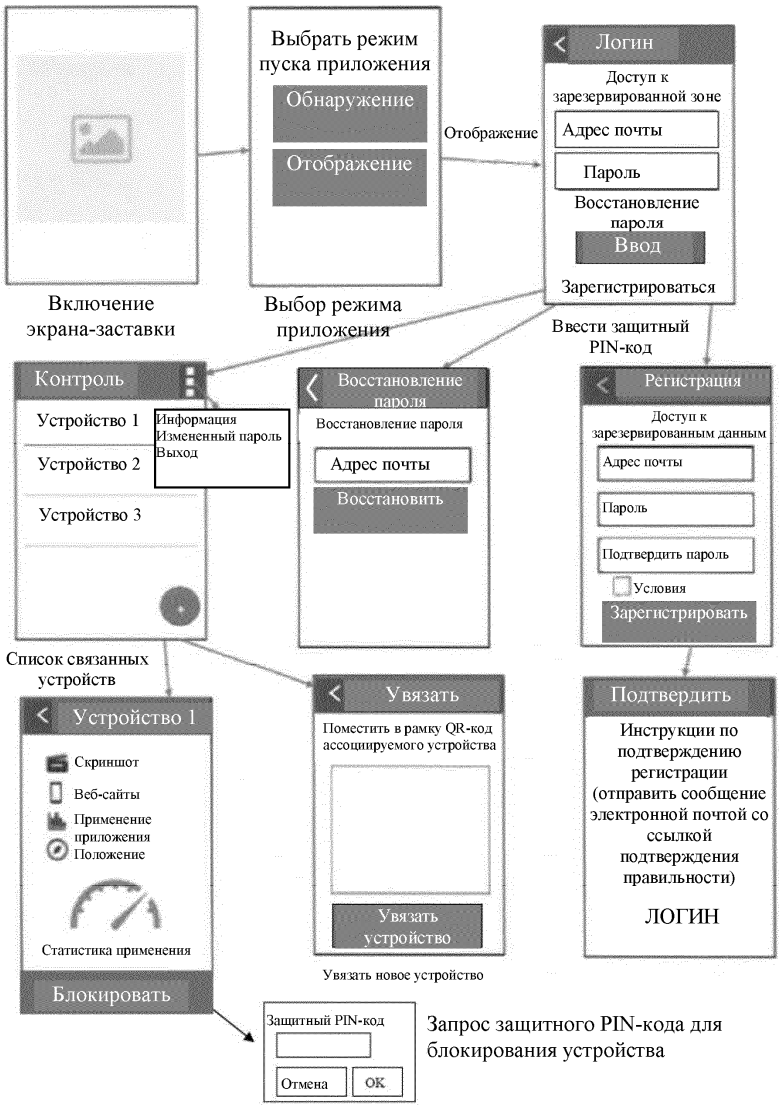
6. Способ по любому из предшествующих пунктов, в котором Приложение инсталлировано на устройстве, при этом доступ указанного Приложения к данным запрещен и может быть разрешен только посредством модуля аутентификации данных доступа администратора.

7. Способ любому из предшествующих пунктов, в котором предусмотрена стадия дистанционного отображения скриншота экрана электронного устройства администратором после аутентификации указанных данных доступа.

8. Машиночитаемый носитель данных, содержащий программу для процессора электронного устройства, обеспечивающую реализацию операций способа по п.1, при ее выполнении процессором электронного устройства.


Включение экрана-заставки
Выбрать режим пуска
Обнаружение
Отображение
Выбор режима применения
Обнаружение
Защитный PIN-код
Ввести защитный PIN-код
Новый PIN-код
Подтвердить PIN-код
Продолжить
Ввести защитный PIN-код
Увязать устройство
Увязка устройства
Защитный PIN-код
Отмена
OK
Запрос защитного PIN-кода
Контроль
Текущий контроль
Увязать устройство
Изменить PIN-код
Сброс
Активированный контроль
Изменить PIN-код
Сброс
Защитный PIN-код
Изменение PIN-кода
Старый PIN-код
Новый PIN-код
Подтвердить PIN-код
Сохранить
Изменение PIN-кода
Защитный PIN-код
Отмена
OK
Запрос защитного PIN-кода
Выбор режима приложения

Фиг. 1


Выбрать режим пуска приложения
Обнаружение
Отображение
Отображение
Логин
Доступ к зарезервированной зоне
Адрес почты
Пароль
Восстановление пароля
Ввод
Зарегистрироваться
Включение экрана-заставки
Выбор режима приложения
Ввести защитный PIN-код
Контроль
Устройство 1
Устройство 2
Устройство 3
Информация
Измененный пароль
Выход
Восстановление пароля
Восстановление пароля
Адрес почты
Восстановить
Регистрация
Доступ к зарезервированным данным
Адрес почты
Пароль
Подтвердить пароль
Условия
Зарегистрировать
Список связанных устройств
Устройство 1
Скриншот
Веб-сайты
Применение приложения
Положение
Статистика применения
Блокировать
Увязать
Поместить в рамку QR-код ассоциируемого устройства
Увязать устройство
Увязать новое устройство
Подтвердить
Инструкции по подтверждению регистрации (отправить сообщение электронной почтой со ссылкой подтверждения правильности)
ЛОГИН
Защитный PIN-код
Отмена
OK
Запрос защитного PIN-кода для блокирования устройства

Фиг. 2