РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 630 163**(13) **C1**

(51) МПК
G06F 12/14 (2006.01)
G06F 21/62 (2013.01)
G06F 21/31 (2013.01)
H04L 9/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

На основании пункта 1 статьи 1366 части четвертой Гражданского кодекса Российской Федерации патентообладатель обязуется заключить договор об отчуждении патента на условиях, соответствующих установившейся практике, с любым гражданином Российской Федерации или российским юридическим лицом, кто первым изъявил такое желание и уведомил об этом патентообладателя и федеральный орган исполнительной власти по интеллектуальной собственности.

(21)(22) Заявка: **2016136625, 12.09.2016**

(24) Дата начала отсчета срока действия патента:
12.09.2016

Дата регистрации:
05.09.2017

Приоритет(ы):
(22) Дата подачи заявки: **12.09.2016**

(45) Опубликовано: **05.09.2017** Бюл. № **25**

Адрес для переписки:
170012, г. Тверь, ул. Цветочная, 2, кв. 4, Дроботуну Е.Б.

(72) Автор(ы):
Дроботун Евгений Борисович (RU)

(73) Патентообладатель(и):
Дроботун Евгений Борисович (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2583759 C1, 10.05.2016. RU 2543561 C1, 10.03.2015. RU 2434283 C1, 20.11.2011. RU 2134931 C1, 20.08.1999.**

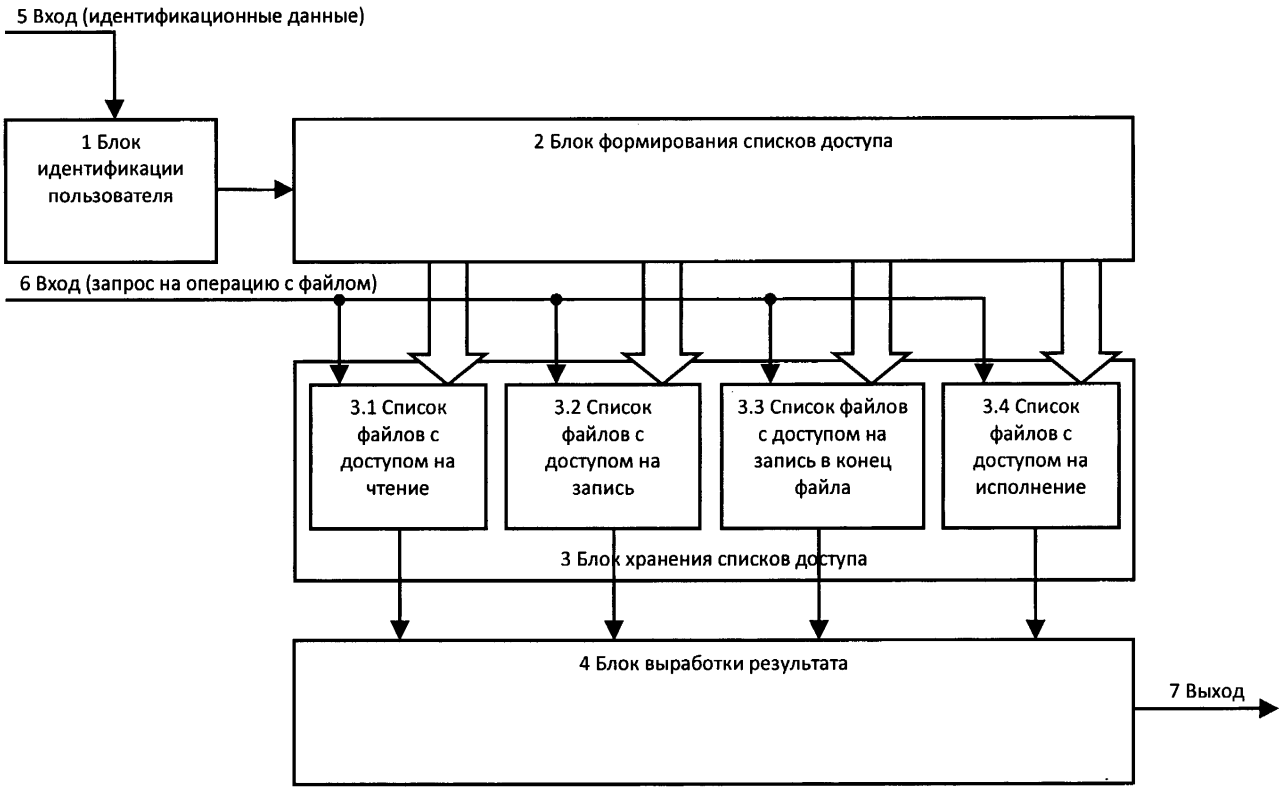
(54) СПОСОБ КОНТРОЛЯ ДОСТУПА К ФАЙЛАМ

(57) Реферат:

Изобретение относится к вычислительной технике, а именно к защите от несанкционированного доступа к информации, обрабатываемой и хранимой в информационно-вычислительных системах различного назначения. Технический результат – снижение времени обращения к файлам при контроле прав доступа к ним и соответственно повышение быстродействия информационно-вычислительной системы в целом. Способ контроля доступа к файлам заключается в предварительном (на этапе получения доступа к операционной системе пользователем, после его идентификации) формировании списков файлов, с которыми пользователю разрешено проводить различные действия. При этом для каждого действия формируются свои списки, которые после входа пользователя помещаются в оперативную память, в область, недоступную для несанкционированного доступа. 1 ил.

RU 2630163 C1

RU 2630163 C1



Фиг. 1

RU 2630163 C1

RU 2630163 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 630 163**(13) **C1**

(51) Int. Cl.
G06F 12/14 (2006.01)
G06F 21/62 (2013.01)
G06F 21/31 (2013.01)
H04L 9/32 (2006.01)

(12) ABSTRACT OF INVENTION

According to Art. 1366, par. 1 of the Part IV of the Civil Code of the Russian Federation, the patent holder shall be committed to conclude a contract on alienation of the patent under the terms, corresponding to common practice, with any citizen of the Russian Federation or Russian legal entity who first declared such a willingness and notified this to the patent holder and the Federal Executive Authority for Intellectual Property.

(21)(22) Application: **2016136625, 12.09.2016**

(24) Effective date for property rights:
12.09.2016

Registration date:
05.09.2017

Priority:
(22) Date of filing: **12.09.2016**

(45) Date of publication: **05.09.2017** Bull. № **25**

Mail address:
170012, g. Tver, ul. Tsvetochnaya, 2, kv. 4, Drobotunu E.B.

(72) Inventor(s):
Drobotun Evgenij Borisovich (RU)

(73) Proprietor(s):
Drobotun Evgenij Borisovich (RU)

(54) METHOD OF CONTROL OF FILES ACCESS

(57) Abstract:

FIELD: information technology.

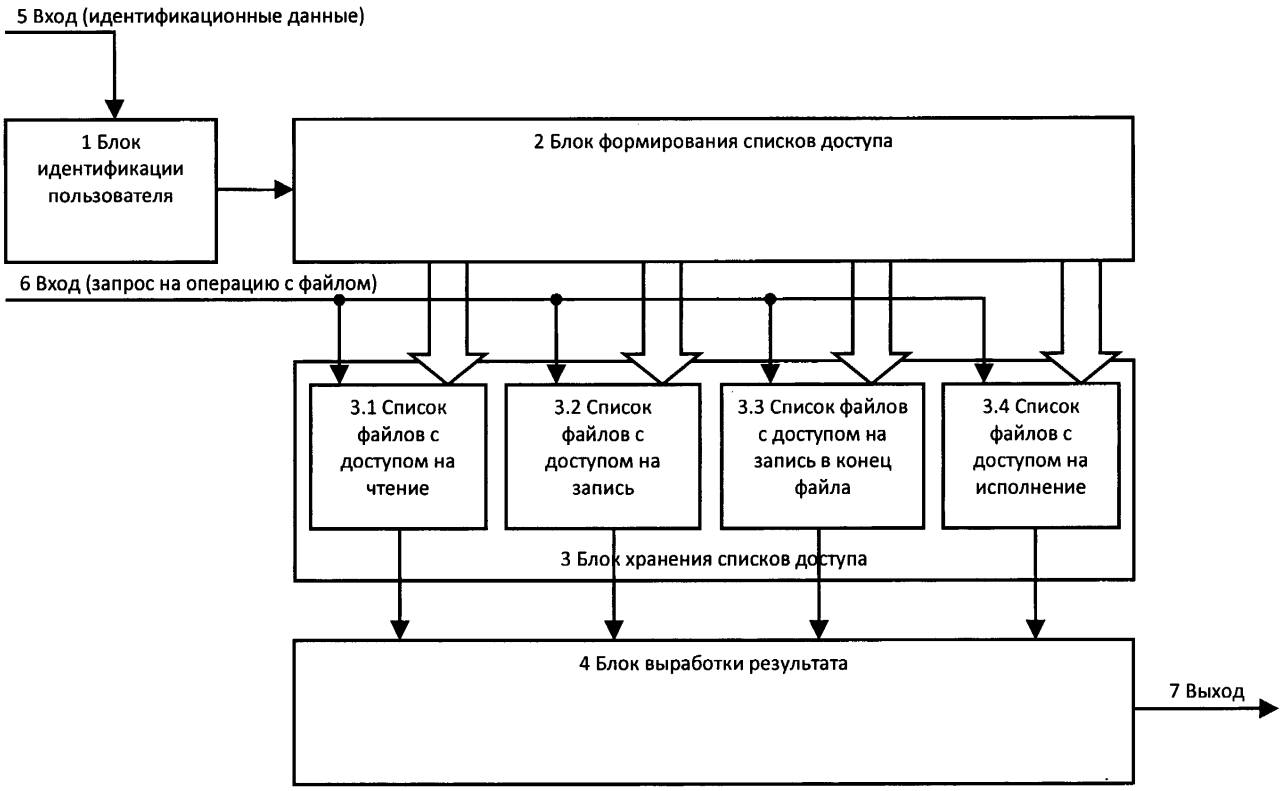
SUBSTANCE: method to control files access is in the preliminary (at the stage of gaining access to the operating system by the user, after his identification) formation of lists of files with which the user is allowed to perform various actions. In this case, for each action, their lists are formed, which, after the user logs on, are placed in the core memory, in an area inaccessible for unauthorized access.

EFFECT: reducing the access time to files when monitoring access rights to them and, accordingly, increasing the speed of the information and calculating system in general.

1 dwg

RU 2630163 C1

RU 2630163 C1



Фиг. 1

RU 2630163 C1

RU 2630163 C1

Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам, и может быть использовано в части защиты от несанкционированного доступа к информации, обрабатываемой и хранимой в информационно-вычислительных системах различного назначения.

Одной из ключевых мер защиты информации, обрабатываемой и хранимой в информационно-вычислительных системах, является реализация контроля доступа (разграничительной политики доступа) к файловым объектам [1].

Известен способ контроля доступа к файлам, реализованный в системе разграничения доступа по расширениям файлов [2]. Данный способ основан на использовании расширения файла в качестве признака, по которому определяется разграничительная политика доступа к файлам.

Недостатками способа является невозможность его реализации в операционных системах, в которых расширения файлов отсутствуют (в частности, в операционных системах семейства Linux) и отсутствие возможности реализаций политик доступа, определенных руководящими документами [1, 3] для информационно-вычислительных систем, обрабатывающих и хранящих критическую и конфиденциальную информацию.

Известен способ контроля доступа к файлам, реализованный в операционных системах семейства Microsoft Windows с файловой системой NTFS, использующий для хранения прав доступа к файлам атрибутов файлов (в частности, атрибут Security Descriptor, который содержит информацию о защите файла, список контроля доступа ACL (Access Control List) и поле аудита, которое определяет, какого рода операции над этим файлом нужно регистрировать) [4].

Недостатком данного способа является реализация только дискреционного контроля доступа, в то время как для некоторых категорий информационно-вычислительных систем (в частности, систем, обрабатывающих и хранящих критическую или конфиденциальную информацию) этого, согласно требованиям по защите информации [3], недостаточно.

Известен способ контроля доступа к файлам, реализованный в системе контроля доступа к файлам на основе их автоматической разметки [5]. Данный способ заключается в автоматическом присвоении прав доступа к файлу в момент его создания и проверки прав доступа к файлу в момент обращения к нему для выполнения различных операций над этим файлом.

Данным способом может быть реализована как дискреционная политика доступа к файловым объектам, так и мандатная политика доступа, что соответствует требованиям руководящих документов. Однако данный способ имеет достаточно высокую ресурсоемкость, поскольку при каждом обращении к любому файловому объекту требуется проведение дополнительных операций по проверке прав доступа к файловому объекту, что увеличивает время выполнения всех операций по работе с файлами.

Известен способ обеспечения безопасности информационных потоков, защищенных информационных системах с мандатным и ролевым управлением доступом [6]. Способ заключается в определении правил назначения прав доступа субъектов доступа к ролям, а также определения для каждой роли уровня целостности.

Данный способ может применяться для осуществления контроля доступа к файлам в информационно-вычислительных системах различного назначения, в том числе и в тех, в которых обрабатывается и хранится критическая или конфиденциальная информация.

Недостатком данного способа является его достаточно высокая ресурсоемкость, обусловленная большим количеством дополнительных проверок при осуществлении

любых операций с файловыми объектами.

Помимо этого известны системы и способы [7-10, 12], реализующие как дискреционный, так и мандатный способ разграничения доступа. Основным недостатком перечисленных систем является их достаточно высокая ресурсоемкость, также обусловленная большим количеством дополнительных проверок при осуществлении любых операций с файловыми объектами и необходимостью в ходе этих проверок обращения к информации, хранящейся на жестком диске информационно-вычислительной системы, время обращения к которому достаточно велико.

Также известен способ обеспечения доступа к объектам в операционной системе МСВС [11]. Данный способ является наиболее близким аналогом заявленного изобретения и выбран в качестве прототипа.

Способ заключается в следующем.

Каждому новому пользователю при его регистрации для допуска к работе с объектами в операционной системе МСВС присваивают и запоминают в памяти, которая выполнена недоступной для несанкционированного обращения, сигнал идентификатора пользователя и сигнал идентификатора образа пользователя, включающий по крайней мере сигнал ранга допуска пользователя (например, «неконфиденциально», «конфиденциально», «строго конфиденциально»), сигнал ранга доверия пользователя (например, «доверенный», «не доверенный») и сигналы идентификаторов действий пользователя, которые в совокупности образуют матрицу доступа. Эта матрица $\{D_i, M_{jk}\}$ состоит из двух частей. Первая часть - матрица D_i допуска к объекту - определяет сигналы идентификаторов действий, разрешенных для выполнения данному пользователю, а также другим пользователям той группы, к которой относится пользователь, например D={read, write, execute} (соответственно «чтение», «запись», «запись в конец файла», «исполнение»). Вторая часть - матрица M_{jk} - определяет сигналы ранга допуска пользователя и сигнал ранга доверия пользователя (принадлежность пользователя к определенной группе).

При обращении к операционной системе пользователь осуществляет свою идентификацию (например, путем ввода своего имени и пароля). При их совпадении с заранее сохраненными в операционной системе имени пользователя и пароля пользователь получает доступ к операционной системе. При этом каждому пользователю соответствует конкретный сигнал идентификатора образа пользователя, содержащий по крайней мере сигнал ранга допуска пользователя, сигнал доверия пользователя и сигналы идентификаторов действий, которые данный пользователь может выполнять над объектами.

Все дальнейшие действия пользователя по отношению к объектам доступа определяются путем использования сигнала идентификатора образа пользователя.

Обратившийся и получивший доступ к операционной системе пользователь осуществляет сигнал запроса для получения доступа к файлу, указывая имя файла, доступ к которому он хотел бы получить, и те действия, которые он хотел бы осуществить с этим файлом.

На основании введенной пользователем информации формируют сигнал запроса на обслуживание, содержащий идентификатор пользователя, имя файла, и сигнал описания запрашиваемых действий.

Каждому файлу соответствует сигнал метки объекта (файла), который содержит структуру данных, описывающую метод доступа к этому объекту, для конкретного пользователя, включающей в себя по крайней мере сигнал имени объекта, сигнал

доступа к объекту, сигналы уровней доверия для действий с объектом и сигналы идентификаторов действий с объектом. Сигнал метки объекта (файла) формируется при создании этого объекта (файла) и хранится на жестком диске вместе с файлом

Доступ пользователя к конкретному объекту осуществляется только после сравнения сигнала идентификатора образа данного пользователя с сигналом метки файла. При этом сравнивают сигнал ранга допуска пользователя, содержащийся в сигнале образа пользователя, и сигнал уровня доступа к объекту, содержащегося в сигнале метки объекта. Если сигнал ранга допуска пользователя выше сигнала уровня доступа к объекту, операционная система разрешает данному пользователю любые запрошенные действия с данным объектом, в том числе чтение, запись, запись в конец файла, выполнение и т.д. Если сигнал допуска пользователя равен сигналу уровня доступа к объекту, то операционная система сравнивает сигнал ранга доверия пользователя с сигналами уровней доверия для действий и считывает в ядро операционной системы из памяти, которая выполнена недоступной для несанкционированного обращения, сигналы идентификаторов действий, для которых сигнал ранга доверия пользователя выше сигнала уровня доверия к конкретному действию. Далее сравнивают сигналы идентификаторов действий пользователя, содержащихся в сигнале идентификатора образа данного пользователя, и сигналы идентификаторов действий объекта и разрешают данному пользователю выполнение только тех видов действий, сигналы идентификаторов для которых у данного пользователя равны сигналам идентификаторов действий объекта.

Основным недостатком способа, выбранного в качестве прототипа, является его ресурсоемкость. При интенсивном обращении к файлам (что характерно для многих информационно-вычислительных систем различного назначения) за счет большого количества операций запросов к памяти, в которой хранятся сигналы идентификаторов пользователя, сигналы идентификаторы образов пользователя, а также за счет большого количества операций обращений к меткам файлов и большого количества операций сравнения сигналов ранга доступа пользователя, сигналов ранга доверия пользователя, сигналов идентификаторов действий пользователя с соответствующими сигналами из меток объектов (файлов), время каждого обращения к файлам увеличивается, что снижает быстродействие информационно-вычислительной системы в целом. При этом метки файлов хранятся на жестком диске вместе с файлами, а операции считывания этих меток с жесткого диска достаточно ресурсоемкие.

Целью изобретения является снижение времени обращения к файлам при контроле прав доступа к ним, и соответственно повышение быстродействия информационно-вычислительной системы в целом.

Для достижения цели предлагается способ, основанный на предварительном (на этапе получения доступа к операционной системе пользователем, после его идентификации) формировании списков файлов, с которыми пользователю разрешено проводить различные действия. При этом для каждого действия формируются свои списки, которые после входа пользователя помещаются в оперативную память в область, недоступную для несанкционированного доступа.

Определение прав доступа к файлу производится путем поиска файла в соответствующем списке, при этом для увеличения скорости поиска в качестве записей используются числовые значения идентификаторов объектов (файлов), сами списки упорядочены по возрастанию (или убыванию), а в качестве алгоритма поиска применяется какой-либо оптимизированный алгоритм (например, широко известный алгоритм бинарного поиска).

Реализация предлагаемого способа будет пояснена с помощью схемы, представленной на фиг. 1. На схеме изображен один из возможных вариантов системы, реализующий заявленный способ. В ее состав входят: блок идентификации пользователя 1; блок формирования списков доступа 2; блок хранения списков доступа 3, включающий в себя список файлов с доступом на чтение 3.1, список файлов с доступом на запись 3.2, список файлов с доступом на запись в конец файла 3.3, список файлов с доступом на запись 3.4; блок выработки результата 4; вход идентификационных данных 5; вход запроса на операцию с файлом 6; выход 7.

Осуществление способа происходит следующим образом. Идентификационные данные, введенные пользователем через вход 5, передаются в блок идентификации пользователя 1, где производится сравнение введенных идентификационных данных с сохраненными ранее идентификационными данными всех зарегистрированных в системе пользователей. При совпадении введенных данных с какими-либо идентификационными данными зарегистрированных пользователей системы, вырабатывается сигнал формирования списков доступа, который поступает на блок формирования списков доступа 2, после чего происходит формирование списков доступа для данного пользователя.

Указанные списки формируются на основе сравнения сигнала идентификатора образа пользователя с сигналом метки всех файлов, находящихся на данный момент в информационно-вычислительной системе, таким же образом как это реализовано в прототипе.

Если в ходе сравнения выясняется, что пользователь имеет допуск к файлу только на чтение, то числовой идентификатор этого файла заносится в список файлов с доступом на чтение 3.1; если в ходе сравнения выясняется, что пользователь имеет доступ к файлу на запись, то числовой идентификатор этого файла заносится в список файлов с доступом на запись 3.2; если в ходе сравнения выясняется, что пользователь имеет доступ к файлу на запись в конец файла, то числовой идентификатор этого файла заносится в список файлов с доступом на запись в конец файла 3.3; если в ходе сравнения выясняется, что пользователь имеет доступ к файлу на исполнение, то числовой идентификатор этого файла заносится в список файлов с доступом на исполнение 3.4. Файлы, к которым пользователь по результатам сравнения сигналов идентификатора образа пользователя и сигналов меток файлов не имеет допуска, в списки не заносятся.

По окончании формирования перечисленных списков, все числовые идентификаторы файлов в каждом из сформированных списков упорядочиваются по возрастанию (или убыванию), после чего пользователь получает доступ к операционной системе.

При этом сформированные и упорядоченные списки доступа размещаются в оперативной памяти в области, недоступной для несанкционированного доступа.

При необходимости осуществления пользователем какой-либо операции с файлом, пользователь составляет сигнал запроса, указывая имя файла и операцию, которую необходимо осуществить с файлом. Данный сигнал поступает на вход 6, после чего в зависимости от запрашиваемого действия (чтение, запись, запись в конец файла, исполнение) проверяется наличие числового идентификатора запрашиваемого файла в соответствующем списке (3.1, 3.2, 3.3, 3.4). В случае если в соответствующем списке содержится числовой идентификатор запрашиваемого файла, то блок выработки результата 4 вырабатывает сигнал разрешения на доступ к запрашиваемому файлу. В случае если соответствующий список не содержит числового идентификатора запрашиваемого файла, то блок выработки результата 4 блокирует доступ пользователя к запрашиваемому файлу.

При удалении файла (в случае получения доступа к этому файлу на запись) его числовой идентификатор удаляется из соответствующего списка.

При создании нового файла его числовой идентификатор вносится в список, в соответствии с уровнем доступа, назначенным этому файлу при его создании. При этом данная операция осуществляется таким образом, чтобы не была нарушена упорядоченность значений числовых идентификаторов, содержащихся в списке.

В качестве числового идентификатора файла возможно использование, например, значения системного идентификатора объекта inod (для операционных систем семейства Linux) [13].

Поскольку за счет использования оптимизированного алгоритма поиска числового идентификатора файла в списке, который соответствует запрашиваемой пользователем операции с файлом, и за счет того, что данные списки доступа находятся в оперативной памяти, время обработки запросов к которой существенно ниже времени обработки запросов к жесткому диску, время операции поиска числового идентификатора в соответствующем списке и выдачи разрешения на допуск (или блокировании допуска) будет ниже, чем в случае реализованного в прототипе способа, в котором доступ к файлу определяется путем проведения нескольких операций сравнения сигналов идентификаторов образа пользователя с сигналами меток файла, которые необходимо считывать с жесткого диска.

Таким образом, за счет предварительного формирования списков доступа к файлам при идентификации пользователя и за счет исключения из процедуры проверки прав доступа к запрашиваемому пользователем файлу достаточно ресурсоемкой операции считывания данных с жесткого диска, проведение которой необходимо при считывании сигналов меток файлов для проведения операций сравнения с соответствующими сигналами идентификатора образа пользователя, время обработки запроса на совершение каких-либо операций с файлами уменьшится и соответственно повысится общее быстродействие информационно-вычислительной системы.

Источники информации

1. Методический документ. Меры защиты информации в государственных информационных системах: утв. Директором ФСТЭК 11 февраля 2014 г. // ФСТЭК России. 2014.

2. Пат. 2207619 Российская Федерация, МПК G06F 21/62 (2013.01). Система разграничения доступа по расширениям файлов / Щеглов А.Ю., Щеглов К.А., опубл. 10.01.2016.

3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

4. Руссинович, М. Внутреннее устройство Wicrosoft Windows / М. Руссинович, Д. Соломон. 6-е изд. - СПб.: Питер, 2013. - 800 с.: ил.

5. Пат. 2524566 Российская Федерация, МПК G06F 12/14. Система контроля доступа к файлам на основе их автоматической разметки / Щеглов А.Ю., Щеглов К.А., опубл. 27.07.2014.

6. Пат. 2525481 Российская Федерация, МПК G06F 21/62. Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом / Девянин П. Н., опубл. 20.08.2014.

7. Пат. 2434283 Российская Федерация, МПК G06F 21/20, G06F 21/22. Система защиты

информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну / Бородакий Ю.В., Бельтов А.Г., Добродеев А.Ю., Коротков С.В., Нащекин П.А., Непомнящих А.В., опубл. 20.11.2011.

8. Пат. 2443017 Российская Федерация, МПК G06F 21/22, G06F 12/14. Система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну / Бородакий Ю.В., Бельтов А.Г., Добродеев А.Ю., Коротков С.В., Нащекин П.А., Непомнящих А.В., Соколов И.А., опубл. 20.02.2012.

9. Пат. 2504935 Российская Федерация, МПК G06F 21/62, G06F 12/14, G06F 21/31. Система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну / Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Нащекин П.А., Чивиков В.Ю., Болдина М.П., опубл. 20.11.2011.

10. Заявка 2009129744 Российская Федерация, МПК G06F 13/00. Система разграничения доступа субъектов к объектам доступа / Минаков В.А., Мирошников В.В., Тупота В.И., опубл. 10.02.2011.

11. Secret Net 7. Руководство администратора. Принципы построения. RU.88338853.501410.015 91 1.

12. Пат. 2134931 Российская Федерация, МПК H04L 9/32, G06F 12/14. Способ обеспечения доступа к объектам в операционной системе МСВС, опубл. 20.08.1999.

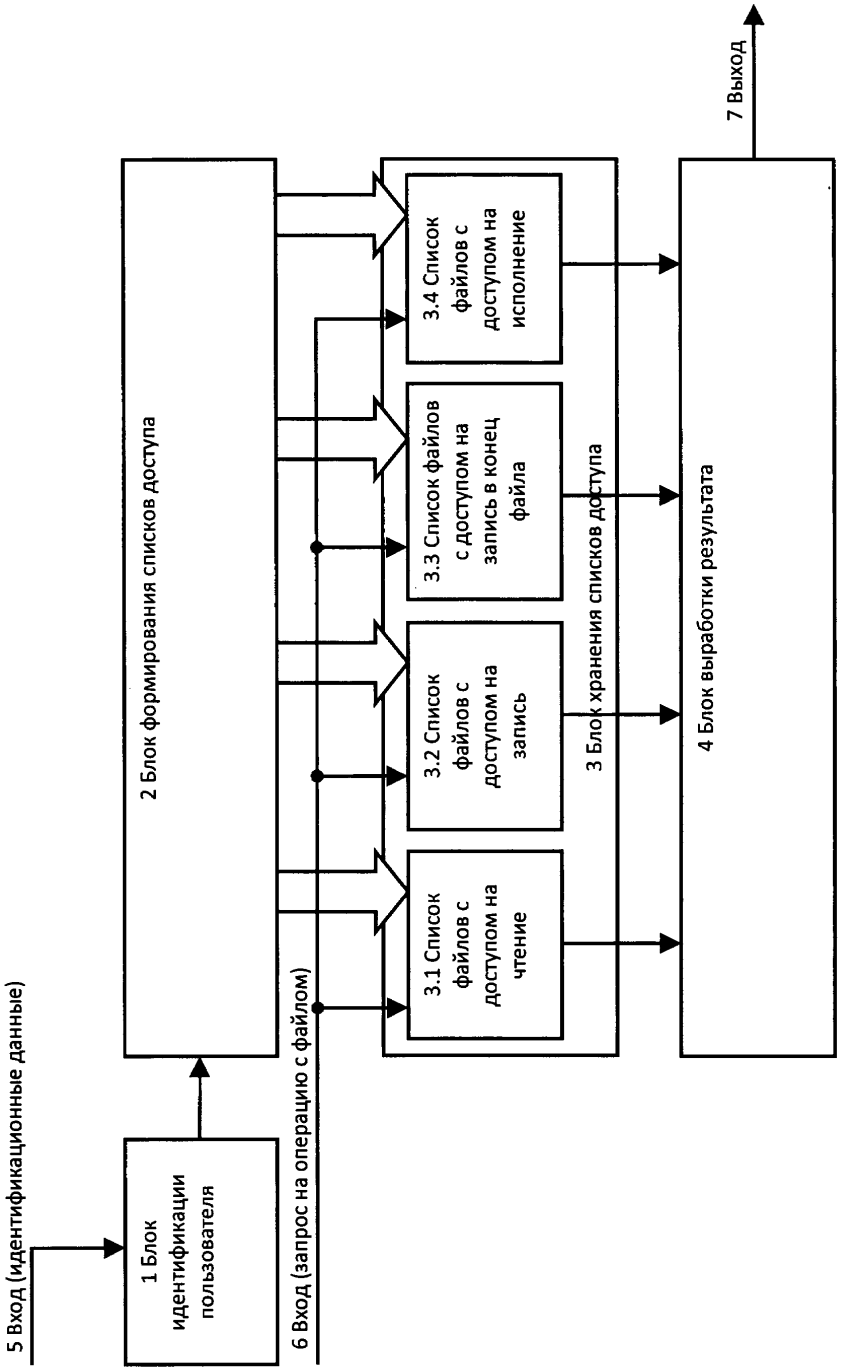
13. Роберт Лав. Linux. Системное программирование. 2-е изд. - СПб.: Питер, 2014. - 448 с.

(57) Формула изобретения

Способ контроля доступа к файлам, заключающийся в том, что каждому пользователю заранее присваивают и затем запоминают в памяти сигнал идентификатора пользователя и сигнал идентификатора образа пользователя, включающий по крайней мере сигнал ранга допуска пользователя, сигнал ранга доверия пользователя и сигналы идентификаторов действий пользователя для каждого файла, содержащегося в информационно-вычислительной системе, заранее формируют и затем записывают на жесткий диск сигналы меток файлов, включающих в себя по крайней мере сигнал имени файла, сигнал уровня доступа к файлу, сигналы уровней доверия для действий над файлом и сигналы идентификаторов действий над файлом; пользователь вводит сигнал идентификатора пользователя, по которому осуществляют его идентификацию и аутентификацию и при идентификации принимают решение о доступе пользователя к операционной системе, отличающийся тем, что после идентификации пользователя на основании сравнения сигналов ранга доступа пользователя, ранга доверия пользователя и сигналов идентификаторов действий пользователя, входящих в состав идентификатора образа пользователя, с соответствующими сигналами метки файла, которую считывают с жесткого диска, формируют список доступа к файлам на чтение, список доступа к файлам на запись, список доступа к файлам на запись в конец файла и список доступа к файлам на исполнение, при этом если в ходе сравнения упомянутых сигналов выясняется, что к данному файлу пользователь имеет доступ на чтение, то числовой идентификатор этого файла записывают в список доступа к файлам на чтение, если в ходе сравнения упомянутых сигналов выясняется, что к данному файлу пользователь имеет доступ на запись, то числовой идентификатор этого файла записывают в список доступа к файлам на запись, если в ходе сравнения упомянутых сигналов выясняется, что к данному файлу пользователь имеет доступ на запись в конец файлов, то числовой идентификатор этого

файла записывают в список доступа к файлам на запись в конец файлов, если в ходе сравнения упомянутых сигналов выясняется, что к данному файлу пользователь имеет доступ на исполнение, то числовой идентификатор этого файла записывают в список доступа к файлам на исполнение, при этом после формирования все списки доступа к файлам упорядочивают по возрастанию или убыванию; при необходимости обращения к файлу формируют запрос, включающий в себя сигнал имени объекта и сигнал описания запрашиваемых действий над файлом, передают сформированный сигнал в ядро операционной системы, в зависимости от сигнала описания запрашиваемых действий над файлом, с помощью алгоритма бинарного поиска проверяют наличие числового идентификатора файла, к которому осуществлено обращение, в соответствующем списке и, при наличии числового идентификатора файла, к которому осуществлено обращение в соответствующем списке, вырабатывают сигнал разрешения совершения запрашиваемых действий над файлом, при отсутствии числового идентификатора файла, к которому осуществлено обращение в соответствующем списке, запрашиваемые действия блокируются; при удалении файла его числовой идентификатор также удаляется из всех списков; при создании нового файла его числовой идентификатор вносят в списки доступа к файлам в соответствии с уровнем доступа, назначенному файлу при его создании, при этом данную операцию осуществляют таким образом, чтобы не была нарушена упорядоченность значений числовых идентификаторов, содержащихся в списке.

1


5 Вход (идентификационные данные)
1 Блок идентификации пользователя
6 Вход (запрос на операцию с файлом)
2 Блок формирования списков доступа
3.1 Список файлов с доступом на чтение
3.2 Список файлов с доступом на запись
3.3 Список файлов с доступом на запись в конец файла
3.4 Список файлов с доступом на исполнение
3 Блок хранения списков доступа
4 Блок выработки результата
7 Выход

Фиг. 1