РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 595 511** (13) **C2**

(51) МПК
G06F 21/53 (2013.01)
G06F 21/55 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2014148962/08, 05.12.2014**

(24) Дата начала отсчета срока действия патента:
05.12.2014

Приоритет(ы):
(22) Дата подачи заявки: **05.12.2014**

(43) Дата публикации заявки: **27.06.2016** Бюл. № **18**

(45) Опубликовано: **27.08.2016** Бюл. № **24**

(56) Список документов, цитированных в отчете о поиске: **CA 2902110 A1, 28.08.2014;US 2014/0359793 A1, 04.12.2014;WO 2014/084967 A1, 05.06.2014;WO 2005/079467 A2, 01.09.2005;US 7676843 B1, 09.03.2010;WO 2014/063124 A1, 24.04.2014;RU 2397537 C2, 20.08.2010.**

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО Лаборатория Касперского, Управление по интеллектуальной собственности, Надежде Васильевне Кащенко

(72) Автор(ы):
Яблоков Виктор Владимирович (RU),
Филатов Константин Михайлович (RU),
Елисеев Евгений Юрьевич (RU),
Унучек Роман Сергеевич (RU)

(73) Патентообладатель(и):
Закрытое акционерное общество "Лаборатория Касперского" (RU)

(54) СИСТЕМА И СПОСОБ ОГРАНИЧЕНИЯ РАБОТЫ ДОВЕРЕННЫХ ПРИЛОЖЕНИЙ ПРИ НАЛИЧИИ ПОДОЗРИТЕЛЬНЫХ ПРИЛОЖЕНИЙ

(57) Реферат:

Изобретение относится к компьютерной безопасности. Технический результат заключается в повышении безопасности обработки защищаемой информации. Система ограничения работы доверенных приложений при наличии подозрительных приложений содержит средство анализа для сбора данных об установленных приложениях; определения среди установленных приложений доверенного приложения, в результате работы которого формируется защищаемая информация; средство определения для эмуляции работы установленных приложений в искусственной среде, обнаружения по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения; базу данных правил; средство блокирования для ограничения работы доверенного приложения, в результате работы которого формируется защищаемая информация, при обнаружении подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения, выработки перечня действий, которые необходимо выполнить, чтобы снять ограничение с доверенного приложения. 2 н.п. ф-лы, 3 ил., 1 табл.

RU 2595511 C2

RU 2595511 C2

Фиг. 2

RU 2595511 C2

RU 2595511 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 595 511** (13) **C2**

(51) Int. Cl.
G06F 21/53 (2013.01)
G06F 21/55 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2014148962/08, 05.12.2014**

(24) Effective date for property rights:
05.12.2014

Priority:
(22) Date of filing: **05.12.2014**

(43) Application published: **27.06.2016** Bull. № **18**

(45) Date of publication: **27.08.2016** Bull. № **24**

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO Laboratorija Kasperskogo, Upravlenie po intellektualnoj sobstvennosti, Nadezhde Vasilevne Kashchenko

(72) Inventor(s):
YAblokov Viktor Vladimirovich (RU),
Filatov Konstantin Mikhajlovich (RU),
Eliseev Evgenij YUrevich (RU),
Unuchek Roman Sergeevich (RU)

(73) Proprietor(s):
Zakrytoe aktsionernoe obshshestvo "Laboratoriya Kasperskogo" (RU)

(54) SYSTEM AND METHOD OF TRUSTED APPLICATIONS OPERATION IN THE PRESENCE OF SUSPICIOUS APPLICATIONS

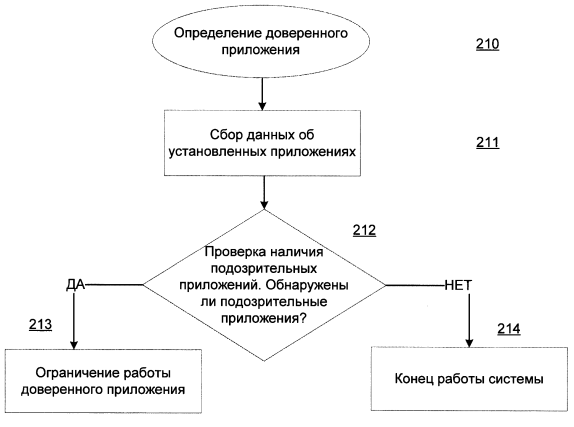
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to computer security. System of limitation of trusted applications operation in presence of suspicious applications includes means of analysis for collection of data on installed applications; determining among installed applications trusted application as result of which protected information is generated; tool for emulating installed applications determination in artificial medium, detecting at least one suspicious application which has possibility of unauthorised processing of protected information, formed as result of trusted application operation; database of rules; locking means for limitation of trusted application operation as result of which protected information is generated, upon detection of suspicious application which has possibility of unauthorised processing of protected information, generated as result trusted application operation, production of list of operations required to execute to remove limitation from trusted application.

EFFECT: higher safety of processing of protected information.

2 cl, 3 dwg, 1 tbl



Фиг. 2

RU 2595511 C2

RU 2595511 C2

Область техники

Изобретение относится к области антивирусной безопасности, а именно к системам и способам ограничения работы приложений.

Уровень техники

Возрастающая популярность использования мобильных телефонов в повседневной жизни побуждает разработчиков создавать приложения для обработки информации, в том числе и персональных данных пользователей. Подобные тенденции приводят к тому, что функционал вредоносных приложений часто бывает направлен на хищение персональных данных. Информация о совершенных покупках, личные контакты, SMS-сообщения, фотографии, видеозаписи, документы и т.д. являются персональными данными и могут быть украдены и использованы без ведома их владельца.

Антивирусная программа позволяет анализировать, останавливать и удалять вредоносные приложения. При этом антивирусная программа по ряду причин не может полностью обеспечить защиту и предотвратить хищение персональных данных. Примером может быть ситуация, когда мобильное приложение, которое на настоящий момент проверено антивирусной программой, и не является вредоносным, имеет, например, разрешение на чтение SMS-сообщений (контактов, почты, фотографий, видеозаписей и др.). В этом случае требуется использовать другие более эффективные способы защиты информации.

Чтение SMS-сообщений или контактов приложением не является хищением персональных данных, но обработка и передача информации о контактах могут привести к их хищению. Например, при установке приложений для ОС Android всегда отображается список разрешений, который необходимо принять, чтобы установить приложение. Приложение, например, может требовать разрешения включить себя в список получателей входящих SMS-сообщений. После принятия пользователем списка разрешений и последующей установки приложение будет получать входящие SMS-сообщения. В одном случае приложением может быть видоизмененный и доработанный менеджер сообщений, который позволяет сократить время поиска требуемых пользователю сообщений. В другом случае приложение может среди всех входящих сообщений искать и использовать в своих целях SMS-сообщения, которые содержат одноразовый пароль для совершения финансовой операции (троян Zeus-in-the-mobile).

Таким образом, возникает ситуация, когда есть информация о том, что приложение может быть потенциально опасным, но нет возможности подтвердить или опровергнуть факт хищения персональных данных со стороны приложения.

В настоящее время существует ряд решений, предназначенных для ограничения использования потенциально опасных приложений. В публикации US 20140128047 A1 описан алгоритм, который блокирует работу приложения на основе различных параметров. Среди параметров может быть наличие пользовательских настроек или предпочтений по отношению к каким-либо сервисам и услугам или их комбинации. Проблему потенциально опасных приложений данный подход не решает. В публикации US 20120255021 A1 описан алгоритм определения и блокирования вредоносного приложения на основании его воздействия на агента безопасности операционной системы. Проблему потенциально опасных приложений данных подход не решает.

Указанные решения предлагают лишь ограничить действие потенциально опасных приложений. Настоящее изобретение позволяет более эффективно решить задачу защиты от хищения данных при наличии потенциально опасных приложений.

Раскрытие изобретения

Изобретение относится к системам и способам ограничения работы приложений.

Технический результат настоящего изобретения заключается в повышении безопасности обработки защищаемой информации. Указанный технический результат достигается за счет ограничения работы приложения, в результате работы которого формируется защищаемая информация при обнаружении по крайней мере одного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию.

Система ограничения работы доверенных приложений при наличии подозрительных приложений, которая содержит: средство анализа, предназначенное для определения среди установленных приложений доверенного приложения, в результате работы которого формируется защищаемая информация, сбора данных об установленных приложениях, передачи данных о доверенном приложении и установленных приложениях средству определения; средство определения, предназначенное для обнаружения по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, на основании данных о доверенном приложении и установленных приложениях с применением правил обнаружения подозрительных приложений, передачи результата обнаружения средству ограничения; базу данных правил, предназначенную для хранения правил обнаружения подозрительных приложений; средство блокирования, предназначенное для ограничения работы доверенного приложения, в результате работы которого формируется защищаемая информация, при обнаружении по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию.

В частном случае реализации системы используют базу данных доверенных приложений, предназначенную для хранения информации об известных доверенных приложениях, в результате работы которых формируется защищаемая информация.

В другом частном случае реализации системы средство анализа определяет доверенное приложения, в результате работы которого формируется защищаемая информация, с помощью поиска среди установленных приложений известного доверенного приложения из базы данных доверенных приложений.

Еще в одном частном случае реализации системы в базе данных правил дополнительно хранят правила анализа приложений, необходимые для определения доверенного приложения.

В частном случае реализации системы средство анализа определяет доверенное приложение, в результате работы которого формируется защищаемая информация, путем анализа установленных приложений с использованием правил анализа приложений.

Способ ограничения работы доверенных приложений при наличии подозрительных приложений, в котором: при помощи средства анализа определяют среди установленных приложений доверенное приложение, в результате работы которого формируется защищаемая информация; при помощи средства анализа собирают данные об установленных приложениях; при помощи средства определения обнаруживают по крайней мере одно подозрительное приложение, которое имеет возможность несанкционированно обработать защищаемую информацию, на основе данных о доверенном приложении и установленных приложениях с применением правил обнаружения подозрительных приложений; при обнаружении по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, при помощи средства блокирования ограничивают работу доверенного приложения, в результате работы которого формируется защищаемая информация.

В другом частном случае реализации способа хранят информацию об известных доверенных приложениях, в результате работы которых формируется защищаемая информация.

В частном случае реализации способа определяют доверенное приложение, в результате работы которого формируется защищаемая информация, с помощью поиска среди установленных приложений известного доверенного приложения.

В другом частном случае реализации способа дополнительно хранят правила анализа приложений, необходимые для определения доверенного приложения.

Еще в одном частном случае реализации способа определяют доверенное приложение, в результате работы которого формируется защищаемая информация, путем анализа установленных приложений с использованием правил обнаружения подозрительных приложений.

Краткое описание чертежей

Дополнительные цели, признаки и преимущества настоящего изобретения будут очевидными из прочтения последующего описания осуществления изобретения со ссылкой на прилагаемые чертежи, на которых:

Фиг. 1 отображает структурную схему системы ограничения работы доверенных приложений при наличии подозрительных приложений.

Фиг. 2 иллюстрирует алгоритм работы системы ограничения работы доверенных приложений при наличии подозрительных приложений.

Фиг. 3 представляет пример компьютерной системы общего назначения.

Хотя изобретение может иметь различные модификации и альтернативные формы, характерные признаки, показанные в качестве примера на чертежах, будут описаны подробно. Следует понимать, однако, что цель описания заключается не в ограничении изобретения конкретным его воплощением. Наоборот, целью описания является охват всех изменений, модификаций, входящих в рамки данного изобретения, как это определено в приложенной формуле.

Описание вариантов осуществления изобретения

Объекты и признаки настоящего изобретения, способы для достижения этих объектов и признаков станут очевидными посредством отсылки к примерным вариантам осуществления. Однако настоящее изобретение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведенная в описании, является ничем иным, как конкретными деталями, необходимыми для помощи специалисту в области техники в исчерпывающем понимании изобретения, и настоящее изобретение определяется в объеме приложенной формулы.

Современное программное обеспечение (ПО) обрабатывает информацию, которая может являться предметом интереса злоумышленников. Например, мобильные приложения, созданные для выполнения банковских транзакций, используют двухфакторную аутентификацию: в этом случае от пользователя при помощи мобильного приложения, которое установлено на его собственной мобильной компьютерной системе, требуется введение логина и пароля, от банка - пересылка SMS с одноразовым паролем. Если злоумышленник, используя вредоносные приложения, узнает логин и пароль и имеет возможность на устройстве пользователя перехватить SMS-сообщение с одноразовым паролем, то он сможет выполнить онлайн-транзакцию вместо пользователя. Работу вышеупомянутого приложения необходимо ограничивать до устранения всех подозрительных и вредоносных приложений. Для того чтобы успешно защитить пользовательские данные, используют систему ограничения работы

доверенных приложений при наличии подозрительных приложений.

На Фиг. 1 изображена структурная схема системы ограничения работы доверенных приложений при наличии подозрительных приложений. Система ограничения работы доверенных приложений при наличии подозрительных приложений состоит из средства анализа 120, средства определения 130, средства блокирования 140, базы данных правил 150.

Средство анализа 120 предназначено для определения среди установленных на компьютерную систему приложений 110 доверенного приложения, в результате работы которого формируется защищаемая информация.

Доверенным приложением может быть приложение, которое было выпущено легальным производителем 110 для обработки пользовательских данных, в том числе и персональных данных. Доверенное приложение не содержит вредоносного кода.

Защищаемая информация - информация, которая является предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Одним из самых распространенных примеров защищаемой информации являются элементы системы аутентификации. https://ru.wikipedia.org/wiki/%C0%F3%F2%E5%ED%F2%E8%F4%E8%EA%E0%F6%E8%FF

Наличие нескольких элементов системы аутентификации на одном устройстве, например мобильном телефоне, может иметь повышенный интерес у злоумышленников.

Доверенные приложения, которые обрабатывают защищаемую информацию, имеют особый интерес для авторов вредоносных программ. Примером доверенных приложений, которые обрабатывают защищаемую информацию, могут быть следующие приложения: банковское приложение (защищаемая информация - логин, пароль, одноразовый пароль, получаемый через SMS), приложения для обработки корпоративной почты (защищаемая информация - логин, пароль, сертификат), приложение для покупок на Ebay (защищаемая информация - логин, пароль, номер банковской карты) и т.д.

Средство анализа 120 может выполнять определение доверенного приложения путем поиска среди установленных приложений 110 доверенных приложений из базы данных доверенных приложений. В этом случае база данных доверенных приложений содержит информацию о доверенных приложениях и о соответствующей защищаемой информации. Пример базы данных доверенных приложений представлен в таблице 1.

Таблица 1.

Название приложения	Разработчик ПО	Защищаемая информация
Сбербанк онлайн	Сбербанк России	Логин, Пароль, одноразовый пароль из SMS.
Aliexpress	Alibaba.com Hong Kong Limited	Имя пользователя, пароль, номер карты.

В другом случае определение доверенного приложения может быть осуществлено путем явного указания пользователем. Пользователь самостоятельно указывает доверенное приложение и выбирает защищаемую информацию.

В ином случае определение доверенного приложения может быть осуществлено путем использования правил анализа приложений. Например, правилом анализа приложения может быть выполнение следующего условия: если приложение

- имеет два и более разрешения на чтение данных пользователя,
- имеет хороший рейтинг от пользователей,
- имеет большое количество скачиваний из магазина приложений (например, Google Play),
- принадлежит определенной категории ПО, например «финансы»,
- подпись содержит сертификат известного легального производителя ПО (http://developer.android.com/tools/publishing/app-signing.html),

то такое приложение можно считать доверенным.

Дополнительным условием к правилам может быть наличие следующего факта: в ходе работы приложения, а именно после обработки совокупности данных пользователя, например логина и пароля, произошло важное событие, которое может быть перехвачено другими приложениями, например получение SMS-сообщения или Data SMS с одноразовым паролем и/или номером сессии, звонка (с сообщением пин-кода) и т.д.

Другой пример правила анализа приложений - если приложение имеет характерную для категории ПО информацию, например логотипа банка (категория «финансы»), других атрибутов банка, например БИК или реквизиты банка, и определен факт того, что с помощью приложения можно совершить платежную операцию, то такое приложение может быть доверенным.

Так же средство анализа 120 предназначено для сбора данных об установленных приложениях 110. К данным об установленных приложениях 110 могут относиться данные о разработчике, разрешениях/правах доступа, категории ПО, рейтинге и количестве скачиваний и комментариев, подписи сертификатом производителя ПО, контрольной сумме и т.д.

Средство анализа 120 передает данные о доверенном приложении и установленных приложениях 110 средству определения 130.

Средство определения 130 предназначено для обнаружения по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обрабатывать защищаемую информацию, на основании данных о доверенном приложении и установленных приложениях 110 с применением правил обнаружения подозрительных приложений.

Подозрительными приложениями могут являться приложения, которые имеют возможность несанкционированно обработать защищаемую информацию.

Под несанкционированной обработкой информации понимают доступ к информации или действия с информацией, осуществляемый с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам. Примером несанкционированной обработки данных может быть обработка подозрительным приложением SMS-сообщения с одноразовым паролем, например, для осуществления транзакции, в результате которой пользователь не получает уведомление о новом сообщении. При этом сообщение может быть прочитано и удалено либо остается прочитанным без дополнительных уведомлений для пользователя.

Характерные признаки подозрительных приложений: автозапуск приложения по определенным событиям, наличие DeviceAdmin (http://developer.android.com/guide/topics/

admin/device-admin.html), получение прав администратора, попытка сокрытия своей работы, загрузка из интернета исполняемого кода и т.д. Упомянутому описанию соответствует вредоносное приложение, классифицированное как lotoor (http://securelist.com/blog/incidents/29836/malware-in-the-android-market-part-2/)

При использовании приложения Battle.net Authenticator при авторизации для запуска игрового приложения на персональном компьютере пользователя требуется введение одноразового пароля. Пользователь при запуске игрового приложения на персональном компьютере вводит логин и пароль. После этого пользователь вводит одноразовый пароль, который автоматически генерируется на сервере после введения основного логина и пароля, и отображается в приложении Battle.Net Authenticator, установленном на мобильном устройстве пользователя. Таким образом перехват основного логина и пароля и контроль мобильного приложения Battle.net Authenticator позволят злоумышленникам выполнять любые действия вместо пользователя. В этом случае приложение Battle.net Authenticator необходимо заблокировать до устранения подозрительных приложений, которые могут обработать входящий трафик либо сделать и обработать снимок текущего состояния экрана.

База данных правил 150 предназначена для хранения правил обнаружения подозрительных приложений и правил анализа. В качестве базы данных правил 150 могут использоваться различные виды баз данных, а именно иерархические (IMS, TDMS, System 2000), сетевые (Cerebrum, Cronospro, DBVist), реляционные (DB2, Informix, Microsoft SQL Server), объектно-ориентированные (Jasmine, Versant, POET), объектно-реляционные (Oracle Database, PostgreSQL, FirstSQL/J, функциональные и т.д.

Правила обнаружения подозрительных приложений, которые хранятся в базе данных правил 150, представляют собой ряд условий, при выполнении которых программа считается подозрительной. Условия в правилах имеют варианты и варьируются в зависимости от известных данных о приложениях.

Примеры правил:

1. Если приложение содержит идентификационные данные банка (номера телефонов, названия, ОГРН. БИК и т.д.) URL, логотип, но не располагается в категории «финансы», то такое приложение считается подозрительным.

2. Если приложение имеет возможность сделать снимки экрана при осуществлении какого-либо события, то такое приложение считается подозрительным.

3. Если приложение имеет возможность чтения, модификации, отправки SMS-сообщений, то такое приложение считается подозрительным.

4. Если приложение имеет возможность перехватывать Data SMS-сообщения, передаваемые по портам доверенных приложений или антивирусных программ, то такое приложение считается подозрительным.

В другом варианте реализации, средство определения 130 может поместить приложение в искусственную среду для эмуляции его работы. Если в результате эмуляции приложения окажется, что осуществляется обращение к доверенному приложению, например, из категории «финансы», или защищаемой информации тем или иным способом, то такое приложение будет считаться подозрительным.

В случае если обнаружено по крайней мере одно подозрительное приложение, средство определения 130 передает результат обнаружения средству блокирования 140.

Средство блокирования 140 предназначено для ограничения работы доверенного приложения при обнаружении по крайней мере одного подозрительного приложения. Ограничение может быть снято после остановки или удаления обнаруженных подозрительных приложений.

В одном из вариантов реализации средство блокирование 140 на основании данных об установленных приложениях 110, доверенном приложении и подозрительных приложениях вырабатывает перечень действий, которые необходимо выполнить, чтобы снять ограничение с доверенного приложения. Примером может служить следующий перечень:

1-е действие - остановка подозрительного приложения А.

2-е действие - удаление подозрительного приложения Б.

Средство блокирования 140 после выполнения требуемого перечня действий снимает ограничение с доверенного приложения.

Фиг. 2 отображает алгоритм системы ограничения работы доверенных приложений при наличии подозрительных приложений. На этапе 210 средство анализа 120 среди установленных приложений 110 выполняет определение доверенного приложения. На этапе 211 средство анализа 120 выполняет сбор данных об установленных приложениях 110 и передает данные о доверенном приложении и об установленных приложениях 110 средству определения 130. На этапе 212 средство определения 130 выполняет проверку наличия подозрительных приложений с применением правил обнаружения подозрительных приложений. Средство определения 130 определяет, было ли обнаружено по крайней мере одно подозрительное приложение, которое может несанкционированно обрабатывать защищаемую информацию, на основании данных о доверенном приложении и установленных приложениях 110. В случае если было обнаружено по крайней мере одно подозрительное приложение, на этапе 213 средство анализа 120 передает данные о по крайней мере одном подозрительном приложении средству блокирования 140. Затем средство блокирования 140 ограничивает работу доверенного приложения. В случае если подозрительных приложений не было обнаружено, на этапе 214, система завершает работу.

Фиг. 3 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая, в свою очередь, память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) 26 содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20, в свою очередь, содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий

диск 27, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации 56, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш-карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.), которые подключены к системной шине 23 через контроллер 55.

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35, а также дополнительные программные приложения 37, другие программные модули 38 и данные программ 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который, в свою очередь, подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например колонками, принтером и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг. 3. В вычислительной сети могут присутствовать также и другие устройства, например маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 50 и глобальную вычислительную сеть (WAN). Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 50 через сетевой адаптер или сетевой интерфейс 51. При использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения техническими средствами связи одного компьютера с другим.

Формула изобретения

1. Система ограничения работы доверенных приложений при наличии подозрительных приложений, которая содержит:

а) средство анализа, предназначенное для:

сбора данных об установленных приложениях, где данными об установленных приложениях является по крайней мере одно из:

- данные о разработчике приложения,

- разрешения доступа приложения,
- категория приложения,
- рейтинг приложения,
- количество скачиваний и комментариев приложения,
- наличие подписи сертификата производителя программного обеспечения,
- контрольная сумма файлов приложения;

определения среди установленных приложений доверенного приложения, в результате работы которого формируется защищаемая информация, на основании собранных данных об установленных приложениях и при помощи правил анализа приложений;

передачи данных о доверенном приложении и собранных данных об установленных приложениях средству определения;

б) средство определения, предназначенное для:

размещения установленных приложений в искусственную среду;

эмуляции работы установленных приложений, размещенных в искусственной среде;

среди установленных приложений, эмуляция которых выполнена, обнаружения по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения, на основании данных о доверенном приложении и собранных данных об установленных приложениях с применением правил обнаружения подозрительных приложений;

передачи собранных данных об установленных приложениях, данных о доверенном приложении и данных о подозрительном приложении средству блокирования;

в) базу данных правил, предназначенную для хранения правил анализа приложений и правил обнаружения подозрительных приложений;

г) средство блокирования, предназначенное для:

ограничения работы доверенного приложения, в результате работы которого формируется защищаемая информация, при обнаружении по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения;

на основании данных о доверенном приложении и данных о подозрительном приложении выработки перечня действий, которые необходимо выполнить, чтобы снять ограничение с доверенного приложения.

2. Способ ограничения работы доверенных приложений при наличии подозрительных приложений, в котором:

а) при помощи средства анализа собирают данные об установленных приложениях, где данными об установленных приложениях является по крайней мере одно из:

- данные о разработчике приложения,
- разрешения доступа приложения,
- категория приложения,
- рейтинг приложения,
- количество скачиваний и комментариев приложения,
- наличие подписи сертификата производителя программного обеспечения,
- контрольная сумма файлов приложения;

б) при помощи средства анализа определяют среди установленных приложений доверенное приложение, в результате работы которого формируется защищаемая информация, на основании собранных данных об установленных приложениях и при помощи правил анализа приложений;

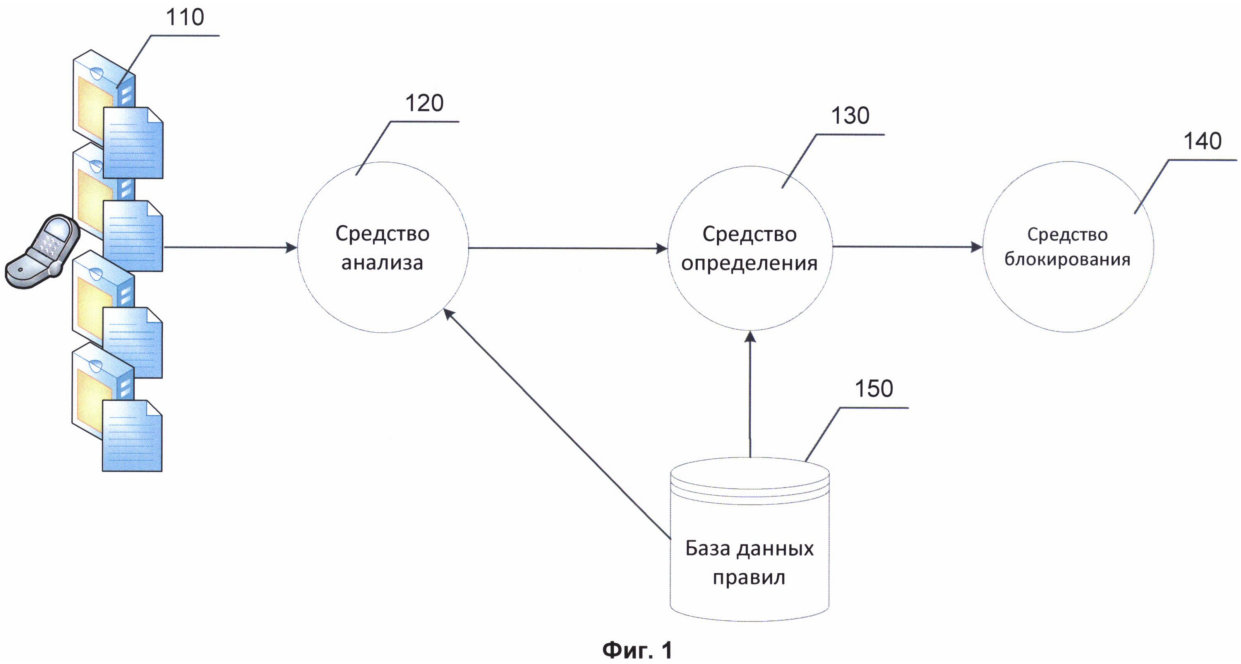
в) при помощи средства определения размещают установленные приложения в искусственную среду;

г) при помощи средства определения эмулируют работу установленных приложений, размещенных в искусственной среде;

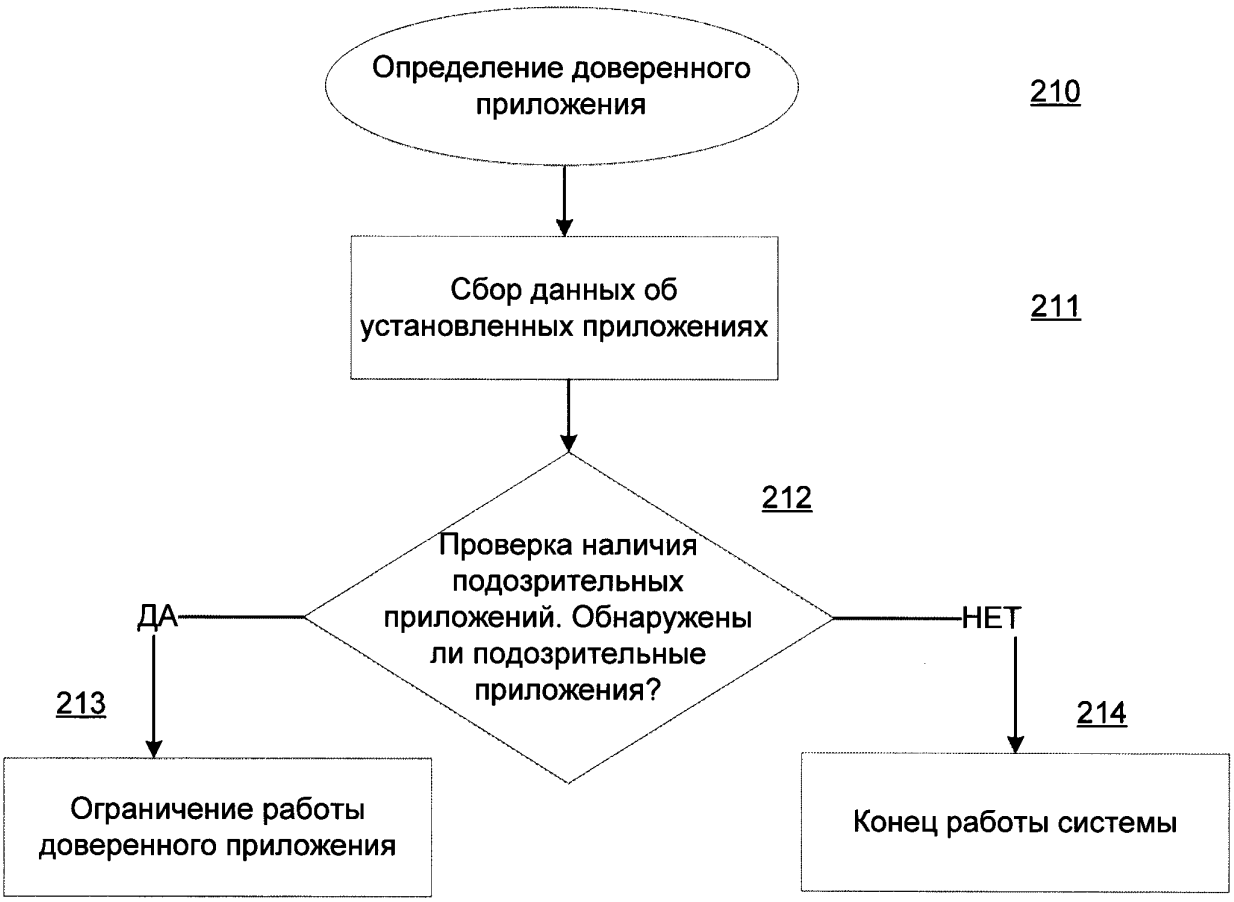
д) при помощи средства определения среди установленных приложений, эмуляция которых выполнена, обнаруживают по крайней мере одно подозрительное приложение, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения, на основании данных о доверенном приложении и собранных данных об установленных приложениях с применением правил обнаружения подозрительных приложений;

е) при помощи средства ограничения ограничивают работу доверенного приложения, в результате работы которого формируется защищаемая информация, при обнаружении по крайней мере одного подозрительного приложения, которое имеет возможность несанкционированно обработать защищаемую информацию, сформированную в результате работы доверенного приложения;

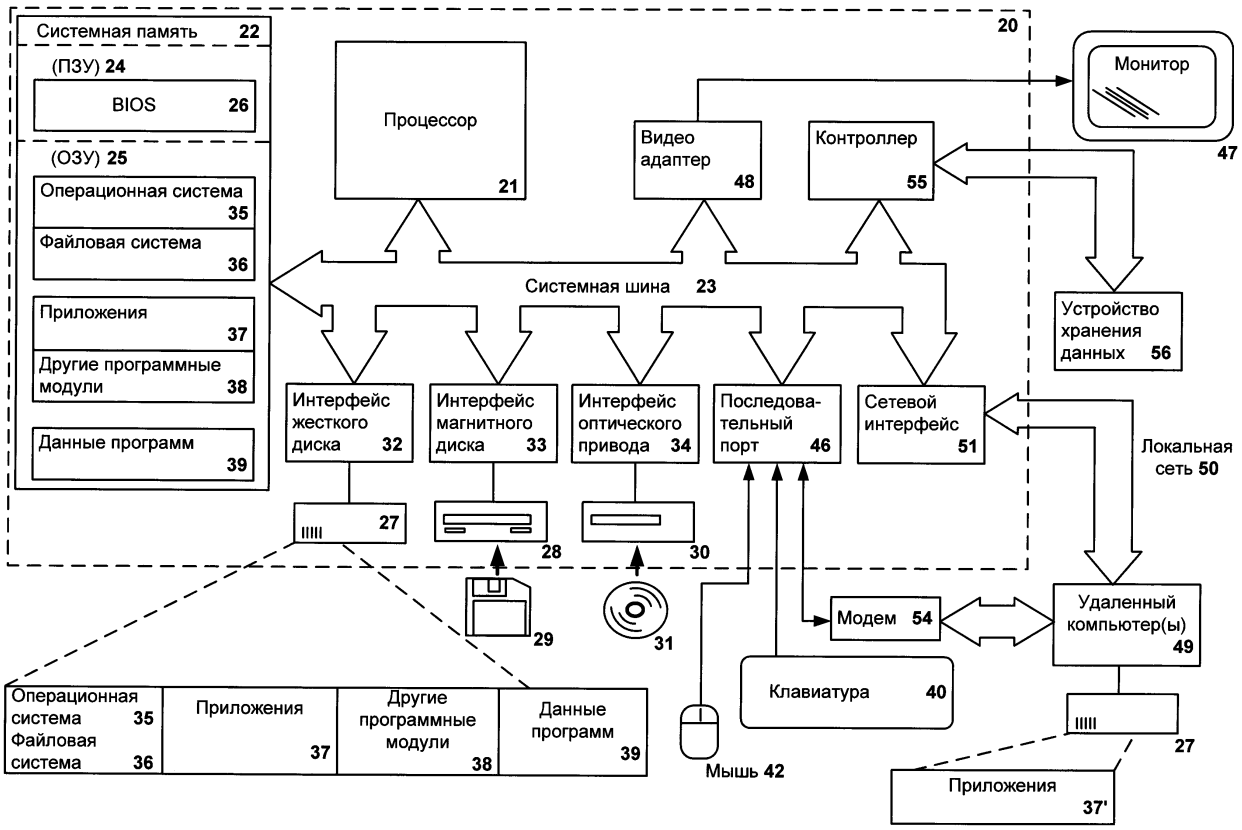
ж) при помощи средства ограничения на основании данных о доверенном приложении и данных о подозрительном приложении вырабатывают перечень действий, которые необходимо выполнить, чтобы снять ограничение с доверенного приложения.


110
120
130
140
Средство анализа
Средство определения
Средство блокирования
150
База данных правил

Фиг. 1


Определение доверенного приложения
210
Сбор данных об установленных приложениях
211
212
Проверка наличия подозрительных приложений. Обнаружены ли подозрительные приложения?
ДА
НЕТ
213
214
Ограничение работы доверенного приложения
Конец работы системы

Фиг. 2


20
Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39
Процессор 21
Видео адаптер 48
Контроллер 55
Монитор
47
Системная шина 23
Устройство хранения данных 56
Интерфейс жесткого диска 32
Интерфейс магнитного диска 33
Интерфейс оптического привода 34
Последова-тельный порт 46
Сетевой интерфейс 51
Локальная сеть 50
27
28
30
29
31
Модем 54
Удаленный компьютер(ы) 49
Клавиатура 40
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39
Мышь 42
27
Приложения 37'

Фиг. 3