РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 332 703** (13) **C2**

(51) МПК
G06F 12/14 (2006.01)
G11C 27/02 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2003126950/09, 03.09.2003**

(24) Дата начала отсчета срока действия патента:
03.09.2003

(30) Конвенционный приоритет:
04.09.2002 US 10/235,587

(43) Дата публикации заявки: **10.03.2005**

(45) Опубликовано: **27.08.2008 Бюл. № 24**

(56) Список документов, цитированных в отчете о поиске: **Eastlake 3rd, D. et al. (Extensible Markup Language) XML-Signature Syntax and Processing, RFC 3275, март 2002 (Найдено в Интернет: http://www.ietf.org/rfc/rfc3275.txt). RU 2154855 C2, 20.08.2000. US 2002/00499908 A1, 25.04.2002. US 2002/0040431 A1, 04.04.2002. US 6041345 A, 21.03.2000.**

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ЭДЕНТ Дэниэль (US),
ВЕСТ Кори (US),
ДУБЛИШ Пратул (US),
СТРОМ Клиффорд П. (US),
КРАЙТС Брайан Д. (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

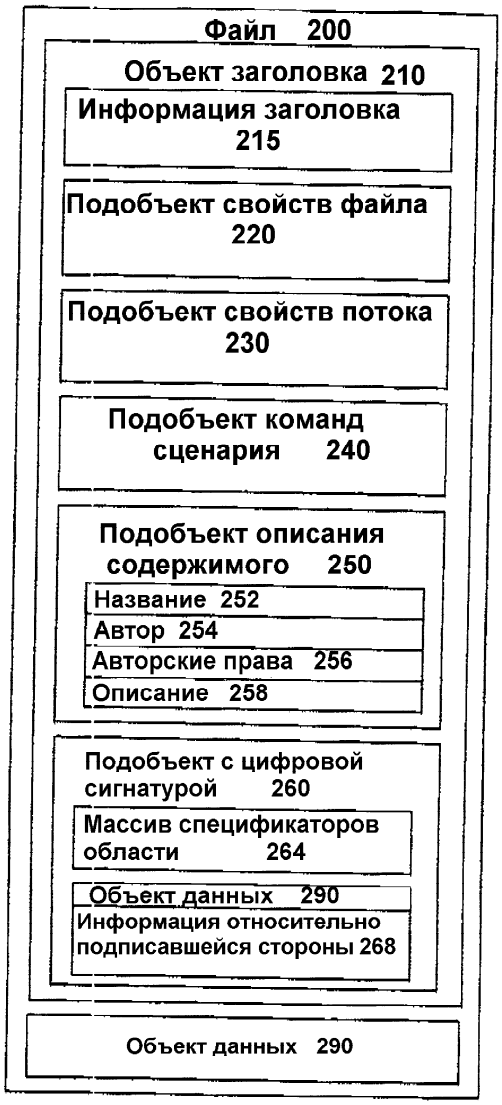
(54) ЗАЩИТА ОБЪЕКТА ЗАГОЛОВКА ПОТОКА ДАННЫХ

(57) Реферат:

Изобретение относится к проверке данных, в частности к объекту заголовка файла данных. Изобретение обеспечивает защиту любого набора подобъектов, не прибегая к какому-либо специальному упорядочиванию подобъектов. В изобретении предложен цифровой объект, содержащий подобъекты, которые содержат информацию, необходимую для проверки надлежащим образом и интерпретации информации, содержащейся в объекте данных. Вводится цифровая сигнатура, которая содержит спецификаторы областей, идентифицирующие области в подобъектах, и информацию достоверности для этих областей. Эта цифровая сигнатура в цифровом объекте позволяет производить модификацию незащищенных областей и переупорядочение подобъектов без нарушения информации проверки достоверности. 9 н. и 45 з.п. ф-лы, 5 ил.

RU 2332703 C2

RU 2332703 C2



ФИГ. 2

RU 2332703 C2

RU 2332703 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 332 703** (13) **C2**

(51) Int. Cl.
G06F 12/14 (2006.01)
G11C 27/02 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2003126950/09, 03.09.2003**

(24) Effective date for property rights: **03.09.2003**

(30) Priority:
04.09.2002 US 10/235,587

(43) Application published: **10.03.2005**

(45) Date of publication: **27.08.2008 Bull. 24**

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
EhDENT Dehniehl' (US),
VEST Kori (US),
DUBLISh Pratul (US),
STROM Klifford P. (US),
KRAJTS Brajan D. (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) PROTECTION OF DATA STREAM HEADER OBJECT

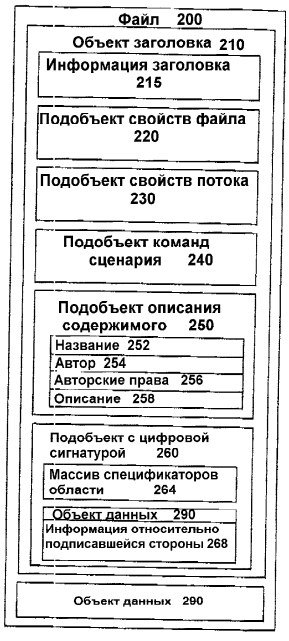
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention provides protection of whatever set of subobjects without using any special arrangement of the objects. There is a digital object proposed in the invention, containing subobjects, witch contain the information required for appropriate checking and interpreting of the information contained in the data object. A digital signature containing fields specificators identifying fields in the subobjects and the validity information for such fields is input.

EFFECT: digital signature in the digital object allows for performing modification of unsecure fields and subobjects rearrangement without corruption of the information with validity check.

54 cl, 5 dwg



ФИГ. 2

RU 2332703 C2

RU 2332703 C2

Область применения изобретения

Настоящее изобретение в целом имеет отношение к проверке данных, а более конкретно к объекту заголовка для файла данных.

Предпосылки к созданию изобретения

Обычно некоторые форматы файлов данных и потоков данных содержат объекты заголовка. Объект заголовка содержит используемую для идентификации информацию "мета-содержимого" и использует эти данные содержимого, которые содержатся в файле данных или в потоке данных.

Например, одним из форматов потока данных является Усовершенствованный Потоковый Формат (ASF), который представляет собой формат расширяемого файла, предназначенный для хранения согласованных мультимедийных данных. Действующая в настоящее время спецификация для этого формата может быть получена по адресу www.microsoft.com. ASF поддерживает передачу данных по самым различным сетям и протоколам, а также позволяет производить локальное считывание.

Каждый ASF файл образован из одного или нескольких медиапотоков. Объект заголовка задает (точно определяет) свойства всего файла, в том числе и специфические свойства потока. В ASF каждый файл должен иметь один объект заголовка. Объект заголовка обеспечивает широко известную байтовую последовательность в начале ASF файлов (GUID - глобально уникальный идентификатор - объекта заголовка) и должен содержать всю информацию, необходимую для надлежащей интерпретации мультимедийных данных. Объект заголовка можно рассматривать в виде контейнера, который содержит информацию относительно объекта заголовка и комбинацию подобъектов заголовка. Информация относительно объекта заголовка включает в себя идентификатор GUID для объекта заголовка ("ASF_Header_Object"), размер объекта заголовка и число подобъектов заголовка, которое содержится в объекте заголовка. Каждый объект заголовка начинается с GUID.

Подобъекты заголовка включают в себя:

Подобъект свойств файла, который определяет глобальные характеристики мультимедийных данных в файле.

Подобъект свойств потока, который определяет специфические свойства и характеристики медиа потока.

Подобъект расширения заголовка, который позволяет добавлять дополнительные функциональные возможности в ASF файл, при одновременном поддержании обратной совместимости, и который представляет собой контейнер, который содержит подобъект расширенного заголовка.

Подобъект списка кодеков (кодеров-декодеров), который содержит дружественную к пользователю информацию относительно кодеков, а также форматы, которые используют для кодирования содержимого в ASF файле.

Подобъект команд сценария, который содержит список пар «тип/параметр» последовательностей Уникода, которые синхронизованы с временной последовательностью ASF файла.

Подобъект маркера, который содержит небольшой специализированный индекс, который используют для создания поименованных точек перехода в файле, для того, чтобы позволить автору содержимого разделить содержимое на логические секции, такие как границы песен на всем CD (компакт-диске) или изменения тем в ходе длительной презентации, и присвоить считываемое человеком имя каждой секции файла, используемой пользователем.

Битовую скорость подобъекта взаимоисключения скорости передачи в битах, который идентифицирует видеопотоки, которые имеют зависимость взаимоисключения друг с другом (другими словами, только один из потоков при такой зависимости может передаваться, при этом все остальные игнорируют).

Подобъект коррекции ошибок, который определяет способ коррекции ошибок и сообщает информацию, необходимую для восстановления при помощи процессора исправления

ошибок.

Подобъект описания содержимого, который позволяет авторам записывать хорошо известные данные, описывающие файл и его содержимое, в том числе название, автор, авторские права, вид и информацию о рейтинге.

Подобъект расширенного описания содержимого, который позволяет авторам записывать данные, описывающие файл и его содержимое, которые выходят за рамки стандартной библиографической информации, такой как название, автор, авторские права, вид и информация о рейтинге.

Подобъект шифрования содержимого, который идентифицирует, является ли содержимое защищенным при помощи системы управления правами на цифровые данные (DRM). Этот подобъект содержит систему DRM приобретения лицензии на URL, DRM на Key ID и другие связанные с DRM метаданные.

Подобъект свойств скорости передачи потока в битах, который определяет среднюю скорость передачи в битах каждого медиапотока в мультимедийных данных.

Подобъект дополнения пробелами, который представляет собой фиктивный подобъект, используемый для обеспечения соответствия размера объекта заголовка.

Компонент (объект), который первым создает файл потока данных, а также любые другие воздействующие на него компоненты, могут добавлять или изменять элементы файла заголовка. Например, создающий содержимое компонент может создавать файл потока данных и включать информацию в объект описания содержимого, касающийся содержимого. Второй компонент может создавать маркеры в данных и добавлять в объект маркера информацию отслеживания. Третий компонент, который распределяет файл потока данных, может добавлять объект команд сценария, содержащий действия или данные для сценария. Например, объект команд сценария может содержать информацию, которая открывает окно веб браузера для заданного URL (унифицированного указателя информационного ресурса).

Так как на ASF файл могут воздействовать различные компоненты, нет возможности определить, какой компонент создал ту или иную часть объекта заголовка. Кроме того, изменение информации хакером не может быть идентифицировано.

Краткое изложение изобретения

Настоящее изобретение посвящено созданию системы, способа и структуры данных для проверки подобъектов в объекте заголовка. Настоящее изобретение позволяет производить проверку по одному компоненту одновременно, для одного или нескольких подобъектов в объекте заголовка, в то же время позволяет изменять порядок подобъектов. Новые подобъекты также могут быть последовательно созданы и проверены при помощи другого компонента. Проверка двух или нескольких подобъектов при помощи надежного (доверительного) компонента может быть объединена, так что хакер не может удалить или изменить данные, оставив один подобъект поддающимся проверке, как это записано при помощи надежного компонента, в то время как другой подобъект не является поддающимся проверке.

Дополнительные признаки и преимущества настоящего изобретения изложены в приведенном далее описании.

Краткое описание чертежей

На фиг. 1 показана блок-схема, дающая общее представление о компьютерной системе.

На фиг. 2 показана блок-схема файла в соответствии с настоящим изобретением.

На фиг. 3 показан процесс создания цифровой сигнатуры подобъекта в соответствии с настоящим изобретением.

На фиг. 4 показан процесс проверки подобъект цифровой сигнатуры в соответствии с настоящим изобретением.

На фиг. 5 показан подобъект цифровой сигнатуры в соответствии с настоящим изобретением.

Подробное описание предпочтительных вариантов изобретения

Обзор

Один или несколько подобъектов цифровых сигнатур могут быть созданы и размещены в объекте заголовка файла данных для того, чтобы иметь информацию о сигнатуре для подобъектов и областей подобъектов в объекте заголовка. Если подобъект цифровой сигнатуры присутствует и является достоверным, то может быть обнаружено любое редактирование или любая фальсификация "подписанного" подобъекта. Отметим, что при этом нет необходимости сохранять порядок (упорядоченное расположение) подобъектов.

Подобъект цифровой сигнатуры содержит матрицу (массив) спецификаторов областей. Каждый спецификатор области идентифицирует специфическую область в подобъекте. Спецификатор области может также идентифицировать весь подобъект.

Подобъект цифровой сигнатуры также содержит сигнатуру. Сигнатура представляет собой цифровую сигнатуру областей, перечисленных в массиве спецификаторов областей. Сигнатура может быть использована для проверки отсутствия фальсификации областей, перечисленных в массиве спецификаторов областей.

Примерная вычислительная среда

На фиг. 1 показан пример подходящей вычислительной среды в виде вычислительной системы (компьютера) 100, в которой может быть осуществлено настоящее изобретение. Вычислительная система 100 является только одним из примеров подходящей вычислительной среды, поэтому она не вносит никаких ограничений как в объем, так и в функциональные возможности настоящего изобретения. Кроме того, не следует понимать, что вычислительная среда 100 имеет какую-либо зависимость от одного компонента или комбинации компонентов, показанных в примерной вычислительной среде 100.

Специалисты легко поймут, что компьютер или другие устройства клиента или сервера могут быть использованы как часть вычислительной сети или распределенной вычислительной среды. В этом отношении следует иметь в виду, что настоящее изобретение имеет отношение к любой вычислительной системе, имеющей любое число блоков памяти или запоминающих устройств, и любое число приложений и процессов, имеющихся в любом числе запоминающих устройств или объемов, которые могут быть использованы в связи с настоящим изобретением. Настоящее изобретение может быть применено в среде с компьютерами-серверами и компьютерами клиента, развернутыми в виде сети, или в распределенной вычислительной среде, имеющей удаленные или локальные средства хранения информации. Настоящее изобретение может быть также применено для автономных вычислительных устройств, которые могут быть запрограммированы на языке программирования, а также возможности интерпретации и выполнения, необходимые для создания, приема и передачи информации, связанной с удаленным или локальным обслуживанием.

Настоящее изобретение может быть использовано с рядом других сред или конфигураций вычислительных систем как общего, так и специального применения. В качестве примера хорошо известных вычислительных систем, сред и/или конфигураций, в которых может быть использовано настоящее изобретение, можно указать без ограничения персональные компьютеры, служебные компьютеры (серверы), карманные или портативные компьютеры, мультипроцессорные системы, системы на базе микропроцессоров, телевизионные приставки, программируемые пользователем электронные устройства, сети персональных компьютеров, миникомпьютеры, универсальные компьютеры, а также распределенные вычислительные среды, которые включают в себя любые из указанных выше систем или устройств, и т.п.

Настоящее изобретение может быть описано в общем контексте выполняемых компьютером команд, таких как программные модули. Обычно программные модули содержат стандартные программы (подпрограммы), программы, объекты, компоненты, структуры данных и т.п., которые осуществляют специфические задачи или реализуют особые типы абстрактных данных. Настоящее изобретение может быть также осуществлено в распределенных вычислительных средах, в которых определенные задачи выполняются при помощи удаленных обрабатывающих устройств, которые соединены при помощи сети связи или другого средства передачи данных. В распределенной

вычислительной среде, программные модули и другие данные могут быть размещены как в локальной, так и в удаленной компьютерной памяти, в том числе и в запоминающих устройствах. Распределенные вычислительные возможности совместно используют компьютерные ресурсы и услуги за счет прямого обмена между компьютерными устройствами и системами. Эти ресурсы и услуги включают в себя обмен информацией, кэш-память и память на дисках для файлов. Распределенные вычислительные возможности имеют преимущество по сравнению с сетевым соединением, так как пользователи могут использовать коллективную вычислительную мощность для решения определенной задачи. В этом отношении следует иметь в виду, что различные устройства могут иметь приложения, объекты или ресурсы, в которых могут быть использованы технологии в соответствии с настоящим изобретением.

Показанная на фиг. 1 примерная система для реализации настоящего изобретения включает в себя вычислительное устройство общего назначения в виде компьютера 110. Компонентами компьютера 110 могут быть, но без ограничения, процессор 120, системная память 130 и системная шина 121, которая соединяет различные компоненты системы, в том числе и системную память, с процессором 120. В качестве системной шины 121 может быть использован любой из множества типов структур шин, в том числе шина памяти или контроллер памяти, шина периферийных устройств, а также локальная (местная) шина, с использованием любой из множества архитектур шины. В качестве примера, но без ограничения, можно указать, что такими архитектурами шин могут быть шины Industry Standard Architecture (ISA), Micro Channel Architecture (MCA), Enhanced ISA (EISA), локальная шина Video Electronics Standards Association (VESA) и шина Peripheral Component Interconnect (PCI) (также известная как шина Mezzanine).

Компьютер 110 обычно содержит несколько считываемых компьютером сред (носителей). Считываемая компьютером среда может представлять собой любую среду, к которой имеется доступ при помощи компьютера 110, и которая содержит как энергозависимую, так и энергонезависимую память, а также как сменный блок памяти, так и не сменяемый (постоянный) блок памяти. В качестве примера, но без ограничения, можно указать, что считываемая компьютером среда может содержать запоминающую среду компьютера и среду для связи. Запоминающая среда компьютера содержит как энергозависимую, так и энергонезависимую память, а также как сменную, так и не сменяемую память, которые могут быть реализованы при помощи любого способа или технологии хранения информации, например, при помощи считываемых компьютером команд, структур данных, программных модулей или других данных. Запоминающая среда компьютера содержит (но без ограничения) RAM (ЗУ с произвольной выборкой), ROM (постоянное запоминающее устройство, ПЗУ), EEPROM (электрически стираемое программируемое постоянное запоминающее устройство), флэш-память или другие технологии хранения информации, CD ROM (постоянное запоминающее устройство на компакт-диске), цифровые универсальные диски (DVD) или другие оптические диски для хранения информации, магнитные кассеты, накопители на магнитной ленте, накопители на магнитных дисках или другие магнитные накопители, а также любые другие носители, которые могут быть использованы для хранения требуемой информации и к которым имеется доступ при помощи компьютера 110. Среда связи обычно охватывает считываемые компьютером команды, структуры данных, программные модули или другие данные в модулированном сигнале данных, при использовании несущей или другого механизма транспортирования информации, и включают в себя любое средство доставки информации. Термин "модулированный сигнал данных" относится к сигналу, который имеет один или несколько характеристических наборов или изменяется таким образом, чтобы кодировать информацию в сигнале. В качестве примера можно указать без ограничения, что средой связи может быть проводное средство связи, такое как проводная сеть или прямое проводное соединение, а также беспроводное средство связи, такое как акустическое, радиочастотное, инфракрасное и другие беспроводные средства связи. Следует иметь в виду, что комбинации указанных выше средств не выходят за рамки

считываемой компьютером среды.Системная память 130 представляет собой запоминающую среду компьютера в виде энергозависимой и/или энергонезависимой памяти, такой как постоянное запоминающее устройство (ROM) 131 и запоминающее устройство с произвольной выборкой (RAM) 132. Базовая система ввода-вывода 133 (BIOS), которая содержит основные стандартные программы, помогающие при обмене информацией между элементами в компьютере 110, например, при запуске, обычно хранится в ROM 131. RAM 132 обычно содержит модули данных и/или программные модули, которые имеют прямой доступ и/или включаются в работу при помощи процессора 120. В качестве примера (но без ограничения), на фиг. 1 показана операционная система 134, прикладные программы 135, другие программные модули 136 и программные данные 137.

Компьютер 110 может также содержать другие сменные и/или не сменяемые, энергозависимые и/или энергонезависимые компьютерные запоминающие среды. Только в качестве примера на фиг. 1 показан дисковод 140 жесткого диска, который производит считывание/запись не сменяемой энергонезависимой магнитной среды хранения информации, дисковод 151 магнитного диска, который производит считывание/запись сменного энергонезависимого магнитного диска 152, и дисковод 155 оптического диска, который производит считывание/запись сменного энергонезависимого оптического диска 156, такого как CD ROM или другое оптическое устройство. Среди других сменных и/или не сменяемых, энергозависимых и/или энергонезависимых компьютерных запоминающих сред, которые могут быть использованы в примерной операционной среде, можно указать (но без ограничения) кассеты магнитной ленты, платы флэш-памяти, универсальные цифровые диски (DVD), цифровые видеоленты, твердотельные RAM, твердотельные ROM, и т.д. Накопитель 141 на жестком диске обычно соединен с системной шиной 121 через интерфейс не сменяемого запоминающего устройства, такой как интерфейс 140, а дисковод 151 магнитного диска и дисковод 155 оптического диска обычно соединены с системной шиной 121 при помощи интерфейса сменного запоминающего устройства, такого как интерфейс 150.

Описанные выше и показанные на фиг. 1 дисководы и объединенные с ними компьютерные запоминающие среды (образующие накопители на дисках) обеспечивают хранение в компьютере считываемых команд, структур данных, программных модулей и других данных для компьютера 110. На фиг. 1 показан, например, дисковод 141 жесткого диска, который хранит операционную систему 144, прикладные программы 145, другие программные модули 146 и программные данные 147. Следует иметь в виду, что эти компоненты могут быть теми же самыми (или другими), что и операционная система 134, прикладные программы 135, другие программные модули 136 и программные данные 137. Операционная система 144, прикладные программы 145, другие программные модули 146 и программные данные 147 имеют здесь другие позиционные обозначения для того, чтобы показать, что они, как минимум, являются другими копиями. Пользователь может вводить команды и информацию в компьютер 20 при помощи входных устройств, таких как клавиатура 162 и координатно-указательное устройство 161, обычно называемое мышью, шаровым указателем (трекболом) или сенсорной панелью. Среди других входных устройств (не показаны) можно назвать микрофон, джойстик, игровую клавиатуру, спутниковую тарелку, сканер и т.п. Эти и другие входные устройства часто подсоединяют к процессору 120 при помощи входного интерфейса 160 пользователя, который подключен к системной шине, но могут быть соединены также при помощи другого интерфейса и шинных структур, таких как параллельный порт, игровой порт или универсальная последовательная шина (USB). Монитор 191 или дисплей другого типа также подключают к системной шине 121 при помощи интерфейса, такого как видеоинтерфейс 190. Кроме монитора, компьютеры могут также иметь и другие периферийные выходные устройства, такие как динамики 197 и принтер 196, которые могут быть подключены через интерфейс 190 периферийных устройств вывода.

Компьютер 110 может работать в образующей сеть среде с использованием логических

связей с одним или несколькими удаленными компьютерами, такими как удаленный компьютер 180. Удаленным компьютером 180 может быть персональный компьютер (PC), сервер, маршрутизатор, сеть PC, одноранговое устройство или другой общий узел сети, причем такой компьютер 180 обычно содержит многие или все элементы, описанные выше для компьютера 110, несмотря на то, что на фиг. 1 показано только его запоминающее устройство 181. Логические соединения, показанные на фиг. 1, включают в себя локальную вычислительную сеть (LAN) 171 и глобальную вычислительную сеть (WAN) 173, однако они могут также содержать и другие сети. Такие объединенные в сеть среды широко используют в офисах, в корпоративных сетях, в других внутренних сетях и в Интернете.

В случае использования в среде, объединенной в сеть LAN, компьютер 110 подключают к сети LAN 171 через интерфейс сети или адаптер 170. В случае использования в среде, объединенной в сеть WAN, компьютер 110 обычно содержит модем 172 или другое средство обмена информацией с сетью WAN 173, такой как Интернет. Модем 172, который может быть внутренним или внешним, может быть подключен системой к шине 121 через входной интерфейс 160 пользователя или через другое подходящее устройство. В объединенной в сеть среде, программные модули, описанные в связи с компьютером 110, или их части, могут храниться в удаленном запоминающем устройстве. В качестве примера, но без ограничения, на фиг. 1 показаны удаленные прикладные программы 185, которые постоянно хранятся в запоминающем устройстве 181. Однако следует иметь в виду, что показанные сетевые соединения даны только в качестве примера, причем могут быть использованы и другие средства создания канала связи между компьютерами.

Подобъекты с цифровой сигнатурой

В том случае, когда объект заголовка содержит подобъекты и области подобъектов, которые должны быть защищены, то в соответствии с настоящим изобретением подобъект с цифровой сигнатурой может быть добавлен в заголовок для того, чтобы обеспечить возможность проверки отсутствия вмешательства (фальсификации) в подписанные подобъекты и области подобъектов. Этот подобъект с цифровой сигнатурой может быть основан на любом алгоритме цифровой подписи, на вход которого подают некоторые данные и который создает сигнатуру (подпись), которая позднее может быть проверена. В соответствии с одним из вариантов использованным алгоритмом является RSA алгоритм (криптосистема, предложенная R.L.Rivest, A.Shamir и L.M.Adleman). В соответствии с другим вариантом используют алгоритм эллиптической кривой. В других вариантах используют другие алгоритмы сигнатуры.

Обратимся теперь к рассмотрению фиг. 2, на которой показан файл 200, который содержит объект 210 заголовка. В дополнение к информации 215 заголовка объект 210 заголовка содержит подобъект 220 свойств файла, подобъект 230 свойств потока, подобъект 240 команд сценария и подобъект 250 описания содержимого. Подобъект 250 описания содержимого включает в себя информацию относительно названия 252, автора 254 и авторских прав 256, а также собственно описание 258 содержимого. Подобъект 240 команд сценария содержит унифицированный указатель информационного ресурса (URL) 245. Файл 200 также содержит объект 290 данных. Следует иметь в виду, что данный чертеж является примерным, причем в объекте заголовка могут существовать комбинации подобъектов, отличающиеся от показанных.

Можно предотвратить фальсификацию частей объекта 210 заголовка за счет добавления подобъекта 260 с цифровой сигнатурой. Подобъект 260 с цифровой сигнатурой содержит массив 264 спецификатора области и сигнатуру 266. В соответствии с одним из вариантов подобъект 260 с цифровой сигнатурой также содержит информацию 268 о подписавшейся стороне. В соответствии с одним из вариантов информация 268 о подписавшейся стороне содержит один или несколько сертификатов, которые могут быть использованы для надежной проверки сигнатуры 266.

Процесс создания подобъекта 260 с цифровой сигнатурой показан на фиг. 3. На этапе 310 принимают решение о том, какие одну или несколько областей подобъектов заголовка

следует подписать, и определяют спецификаторы областей для этих областей. Например, со ссылкой на фиг. 2, подписываемыми областями могут быть подобъект 230 команд сценария, а также секции названия, автора и авторского права подобъекта 250 описания содержимого. Вновь обратимся к рассмотрению фиг. 3, где на этапе 320 создают массив 264 спецификатора областей (фиг. 2). На этапе 330 области, указанные в массиве 264 спецификатора областей, конкатенируют (в том порядке, в котором они заданы в массиве 264 спецификатора областей) с массивом 264 спецификатора областей. Затем эту область подписывают на этапе 340 для получения сигнатуры 266 (фиг. 2).

В том случае, когда изменяют файл, который содержит объект заголовка, имеющий подобъект с цифровой сигнатурой, порядок подобъектов может быть изменен, и могут быть введены дополнительные подобъекты. Если необходимо проверять дополнительные области или подобъекты, то может быть добавлен новый подобъект с цифровой сигнатурой.

Со ссылкой на фиг. 2, для проверки объекта 210 заголовка, используют подобъект 260 с цифровой сигнатурой и области, заданные при помощи массива 264 спецификатора областей. Как показано на фиг. 4, на этапе 410 идентифицируют области подобъекта заголовка, заданные в массиве 264 спецификатора областей (фиг. 2). На этапе 420 эти области конкатенируют (в том порядке, в котором они заданы в массиве 264 спецификатора областей) вместе с массивом 264 спецификатора областей. На этапе 430 проверяют сигнатуру 266 (фиг. 2) для того, чтобы определить ее правомерность для конкатенации.

В соответствии с одним из вариантов осуществления настоящего изобретения могут быть подписаны как области подобъектов, так и подобъекты целиком с использованием подобъекта цифровой сигнатуры. В соответствии с другим вариантом могут быть подписаны только полные подобъекты. В соответствии с одним из вариантов осуществления настоящего изобретения более одной областей единственного подобъекта могут быть подписаны при помощи одного подобъекта цифровой сигнатуры. В соответствии с одним из вариантов осуществления настоящего изобретения подписываемые области одного и того же подобъекта могут перекрываться.

В соответствии с одним из вариантов осуществления настоящего изобретения каждый объект заголовка может содержать по меньшей мере один подобъект с цифровой сигнатурой. Если объект заголовка не содержит ожидаемого подобъекта с цифровой сигнатурой, то тогда можно предположить, что была произведена фальсификация объекта заголовка. Если объект заголовка содержит подобъект с цифровой сигнатурой, который не дает правильного результата при проверке или поступил из не достоверного источника, то лицо, получившее файл с таким объектом заголовка, может действовать по своему усмотрению, например, не использовать этот файл. В соответствии с этим вариантом проверку проводят для того, чтобы убедиться в том, существует ли какой-либо подобъект с цифровой сигнатурой. Если его нет, то проверка дает отрицательный результат. Если подобъекты с цифровой сигнатурой имеются, то каждый их них проверяют на достоверность.

В соответствии с одним из вариантов любой файл F, который является набором объектов O_1, O_2, O_n, может быть подписан в соответствии с настоящим изобретением. В этом случае создают новый объект O_{DS}, который содержит массив спецификатора областей, задающий подписанные объекты или области объектов, и сигнатуру для этих объектов и массива.

Реализация примерного ASF

В соответствии с одним из вариантов файлом является ASFфайл. Компоненты подобъекта с цифровой сигнатурой для ASFфайла в соответствии с одним из вариантов показаны на фиг. 5. Подобъект 500 с цифровой сигнатурой содержит GUID (глобально уникальный идентификатор) 510. Каждый объект и подобъект в ASFфайле начинается с GUID. Идентификаторы GUID используют для того, чтобы единственным образом идентифицировать все типы объектов в ASFфайлах. Каждый тип объекта в ASFфайле

имеет собственный уникальный идентификатор GUID. Однако, вообще говоря, идентификаторы GUID не могут быть использованы для идентификации единственным образом подобъектов в объекте заголовка ASF, так как многие подобъекты в объекте заголовка ASF могут иметь одинаковый тип объекта и, следовательно, иметь одинаковый GUID.

Следующим элементом в примерном подобъекте 500 с цифровой сигнатурой в ASF является размер подобъекта 520. И в этом случае все ASFобъекты и подобъекты обычно содержат размер объекта и подобъекта. Массиву 540 спецификатора областей, который описан выше, предшествует число подписанных областей, которые содержатся в массиве 540 спецификатора. Идентификатор 550 алгоритма вычисления контрольной суммы и идентификатор 560 алгоритма вычисления сигнатуры, идентифицирующие алгоритмы вычисления контрольной суммы и цифровой сигнатуры используют в цифровой сигнатуре подобъекта. Сигнатуре 580 областей и массиву спецификатора областей предшествует длина сигнатуры 570. Информация 590 о подписавшейся стороне содержит информацию, которая необходима для проверки или получения информации относительно подписавшейся стороны. Информация 590 о подписавшейся стороне может содержать информацию относительно идентичности подписавшейся стороны. В соответствии с одним из вариантов информация 590 о подписавшейся стороне содержит цепочку сертификата, которая может быть использована для проверки того, что открытый ключ подписавшейся стороны происходит из надежного источника.

В примерной реализации ASF, каждый спецификатор области содержит смещение области подобъекта, размер области подобъекта, длину контрольной суммы и контрольную сумму объекта. Смещение области идентифицирует, где начинается область в подобъекте, а размер области идентифицирует размер области. Контрольная сумма объекта соответствует контрольной сумме заданной области. Алгоритмом контрольной суммы в соответствии с предпочтительным вариантом является алгоритм Secure Hash Algorithm (SHA-1). Этот алгоритм содержится в публикации Federal Information Processing Standards Publication 180-1, которая доступна в Интернете по адресу http: //www.itl.nist.gov/fipspubs/fip 180-1htm. В альтернативных вариантах может быть использован любой хэширующий алгоритм с низкой вероятностью конфликтов. В альтернативном варианте контрольная сумма объекта соответствует контрольной сумме подобъекта, содержащего заданные области.

Когда производят проверку сигнатуры, то для того, чтобы определить в каком подобъекте локализована область (на этапе 410 фиг. 4), исследуют подобъекты заголовка. Для каждого исследованного подобъекта вычисляют контрольную сумму в соответствии с алгоритмом, заданным идентификатором 550 алгоритма вычисления контрольной суммы. В том варианте, в котором вычисляют контрольную сумму для области, вычисление контрольной суммы проводят для данных, которые содержатся в том подобъекте, который начинается при заданном смещении области подобъекта и продолжается до заданного размера области подобъекта. В том варианте, в котором контрольную сумму вычисляют для всего подобъекта, вычисление контрольной суммы проводят для указанного подобъекта. Когда вычисленная контрольная сумма совпадает с контрольной суммой в спецификаторе области, считают, что идентифицирован правильный подобъект для спецификатора области. После идентификации подобъектов, соответствующих каждой области спецификатора, можно проводить проверку сигнатуры.

В соответствии с данным вариантом осуществления настоящего изобретения, для того, чтобы указать необходимость подписи всего подобъекта, смещение в спецификаторе области должно быть равно нулю, а размер области должен быть равен длине подобъекта. В соответствии с другим вариантом, контрольную сумму вычисляют для всего подобъекта, а не для заданной области.

В соответствии с этим вариантом несколько подобъектов с цифровой сигнатурой могут быть включены в объект, для того, чтобы обеспечить гибкость при совместной проверке подобъектов с различными областями, а также обеспечить проверку подобъектов

различными системами.

В соответствии с другими вариантами для идентификации областей могут быть использованы другие способы. В соответствии с одним из вариантов данные, которые единственным образом могут идентифицировать подобъект, содержатся в спецификаторе области, вместе со смещением области и данными о размере области.

В соответствии с другими вариантами только весь подобъект может быть подписан. В соответствии с одним из вариантов спецификатор области содержит контрольную сумму для всего подобъекта. В соответствии с другим вариантом используют также и длину контрольной суммы. В соответствии с еще одним вариантом в спецификаторе области используют и другие данные, которые могут идентифицировать подобъект.

Заключение

В соответствии с настоящим изобретением предлагается система и способ для защиты объекта заголовка потока данных. Как уже было упомянуто выше, несмотря на то, что были описаны примерные варианты настоящего изобретения с указанием различных вычислительных устройств и архитектур сети, лежащие в основе этих вариантов концепции, могут быть применены к любому вычислительному устройству или системе, в которых требуется обеспечить защиту объекта заголовка потока данных. Таким образом, технологии обеспечения защиты объекта заголовка потока данных в соответствии с настоящим изобретением могут быть использованы в различных устройствах и приложениях. Например, способы в соответствии с настоящим изобретением могут быть использованы в операционной системе вычислительного устройства, в виде отдельного объекта к устройству, части другого объекта, в качестве загружаемого с сервера объекта, в виде "посредника" между устройством или объектом и сетью, а также в виде распределенного объекта, и т.п. Несмотря на то что выбранные здесь примерные названия и примеры являются представительными во многих случаях, эти названия и примеры не носят ограничительного характера.

Различные описанные способы могут быть реализованы при помощи аппаратных или программных средств, а также, при необходимости, за счет их комбинации. Таким образом, способы и устройства в соответствии с настоящим изобретением, или их определенные аспекты и части, могут иметь вид программного кода (то есть команд), реализованного на материальных средствах, таких как гибкие диски, компакт-диски CD-ROM, накопители на жестких дисках или любые другие машиночитаемые запоминающие среды, причем после загрузки программы в машину (такую как компьютер) и ее выполнения, машина становится устройством для осуществления настоящего изобретения. В случае выполнения программного кода на программируемых компьютерах, вычислительное устройство обычно включает в себя процессор, запоминающую среду, считываемую процессором (причем такая среда включает в себя энергозависимую и энергонезависимую память и/или запоминающие элементы), по меньшей мере одно устройство ввода и по меньшей мере одно выходное устройство. Одна или несколько программ могут быть использованы в соответствии с настоящим изобретением, например, за счет использования обработки данных при помощи API (программного интерфейса приложения) или другого аналогичного средства, причем эти программы для обмена информацией с системой компьютера преимущественно используют процедурный язык программирования высокого уровня или объектно-ориентированный язык программирования. Однако указанные программы по желанию могут быть реализованы также на ассемблере или в машинном языке. В любом случае, языком может быть компилированный или интерпретированный язык, объединенный с реализациями аппаратных средств.

Способы и устройства в соответствии с настоящим изобретением могут быть также осуществлены за счет обмена информацией, материализованного в виде программного кода, который передают в некоторой среде передачи информации, такой как электрические провода или кабели, волоконная оптика или другом средстве связи, причем после приема и загрузки программного кода и его выполнения машиной, такой как EPROM, вентильная

матрица, программируемое логическое устройство (PLD), компьютер пользователя, видеомагнитофон и т.п., или приемная машина, имеющая возможности обработки сигнала, например, в соответствии с описанными здесь выше примерными вариантами эта машина становится устройством для осуществления настоящего изобретения. В случае реализации на процессоре общего назначения программный код совместно с процессором образует уникальное устройство, которое обладает функциональными возможностями в соответствии с настоящим изобретением. Кроме того, следует иметь в виду, что в соответствии с настоящим изобретением вообще может быть использована любая технология хранения информации, которая является комбинацией аппаратных и программных средств.

Несмотря на то, что были описаны предпочтительные варианты осуществления изобретения со ссылкой на чертежи, совершенно ясно, что могут быть использованы и другие аналогичные варианты, причем в них специалистами в данной области могут быть внесены изменения и дополнения, которые не выходят однако за рамки приведенной ниже формулы изобретения. Например, в то время как примерные сетевые среды в соответствии с настоящим изобретением описаны в виде связанных в общую сеть среды, такой как среда связанных сетью одноранговых пользователей следует иметь в виду, что настоящее изобретение не ограничивается только этим вариантом, причем описанные в настоящем изобретении способы могут быть применены к любому вычислительному устройству или к любой вычислительной среде, например, к игровой стойке, карманному компьютеру, портативному компьютеру и т.п., с проводным или беспроводным соединением, при этом указанные способы могут быть применены к любому числу таких вычислительных устройств, соединенных при помощи сети связи и взаимодействующих в этой сети. Более того, следует подчеркнуть, что могут быть использованы различные компьютерные платформы, в том числе операционные системы портативных устройств и специфические операционные системы другого применения, особенно при возрастании числа объединенных в сеть беспроводных устройств. Более того, настоящее изобретение может быть осуществлено в виде множества вычислительных микросхем или устройств, причем хранение информации может быть осуществлено во множестве различных устройств. Таким образом, настоящее изобретение не ограничено случаем какого-либо единственного варианта, а скорее должно рассматриваться в объеме приложенной формулы изобретения.

Формула изобретения

1. Способ создания цифровой сигнатуры в цифровом объекте для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутый способ обеспечивает цифровую сигнатуру для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем упомянутые подобъекты могут быть переупорядочены внутри объекта без нарушения достоверности цифровой сигнатуры, при этом способ предусматривает:

создание массива, содержащего для каждой из упомянутых по меньшей мере одной области спецификатор области, идентифицирующий область;

формирование цифровой сигнатуры на основании данных, которые содержат каждую область и упомянутый массив; и

добавление в цифровой объект подобъект с сигнатурой, содержащий упомянутый массив и упомянутую цифровую сигнатуру.

2. Способ по п.1, в котором каждая из упомянутых по меньшей мере одной областей содержит подобъект из упомянутых по меньшей мере одного подобъектов.

3. Способ по п.1, в котором каждый из упомянутых спецификаторов областей содержит контрольную сумму, вычисленную в соответствии с алгоритмом вычисления контрольной суммы.

4. Способ по п.3, в котором упомянутую контрольную сумму подсчитывают для области.

5. Способ по п.3, в котором упомянутую контрольную сумму подсчитывают для подобъекта, содержащего эту область.

6. Способ по п.3, в котором упомянутый подобъект с сигнатурой содержит идентификатор алгоритма вычисления контрольной суммы, причем идентификатор идентифицирует используемый алгоритм вычисления контрольной суммы.

7. Способ по п.3, в котором каждый из упомянутых спецификаторов областей содержит длину контрольной суммы.

8. Способ по п.1, в котором упомянутый подобъект с сигнатурой содержит идентификатор алгоритма сигнатуры, причем идентификатор идентифицирует алгоритм сигнатуры, используемый для создания цифровой сигнатуры.

9. Способ по п.1, в котором упомянутый подобъект с сигнатурой содержит идентификатор подписавшейся стороны, идентифицирующий подписавшуюся сторону для верификации указанной цифровой сигнатуры.

10. Способ по п.9, в котором упомянутый идентификатор подписавшейся стороны содержит цифровые сертификаты, необходимые для надежной идентификации и верификации открытого ключа упомянутой подписавшейся стороны.

11. Способ по п.1, в котором каждый из упомянутых спецификаторов областей содержит значение смещения области, идентифицирующее начальное местоположение соответствующей области в подобъекте.

12. Способ по п.1, в котором каждый из упомянутых спецификаторов областей содержит размер области, идентифицирующий размер соответствующей области в подобъекте.

13. Способ по п.1, в котором упомянутый объект представляет собой объект заголовка для ASF файла.

14. Способ по п.13, в котором упомянутый новый объект дополнительно содержит идентификатор GUID (глобальный уникальный идентификатор).

15. Способ проверки достоверности цифровой сигнатуры для использования в комбинации с цифровым объектом, содержащим по меньшей мере один подобъект, причем упомянутый способ осуществляет проверку достоверности цифровой сигнатуры для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, причем способ предусматривает:

идентификацию области, соответствующей каждому из упомянутых спецификаторов области;

создание объекта данных, содержащего упомянутый массив и, для каждого из упомянутых спецификаторов области - упомянутую область, соответствующую упомянутому спецификатору области; и

проверку достоверности упомянутой цифровой сигнатуры, используемой для упомянутого объекта данных.

16. Способ по п.15, в котором упомянутый объект представляет собой объект заголовка для ASF файла.

17. Способ проверки достоверности цифровой сигнатуры для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутый способ осуществляет проверку достоверности цифровой сигнатуры для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, при этом способ предусматривает:

определение числа цифровых сигнатур, присутствующих в упомянутом цифровом объекте;

проверку достоверности каждой из упомянутых цифровых сигнатур.

18. Способ по п.17, который дополнительно предусматривает возврат значения ошибки, если число цифровых сигнатур, присутствующих в упомянутом цифровом объекте, равно

нулю.

19. Система для создания цифровой сигнатуры в цифровом объекте для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутая система обеспечивает цифровую сигнатуру для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем упомянутые подобъекты могут быть переупорядочены в объекте без нарушения достоверности цифровой сигнатуры, при этом упомянутая система включает в себя:

средство создания массива, позволяющее создать массив, который содержит, для каждой из упомянутых по меньшей мере одной областей, спецификатор области, идентифицирующий область;

средство подписи для создания цифровой сигнатуры на основании данных, содержащих каждую область и упомянутый массив; и

средство добавления подобъекта с сигнатурой, позволяющее добавлять подобъект с сигнатурой, содержащий упомянутый массив и упомянутую цифровую сигнатуру, в цифровой объект.

20. Система по п.19, в которой каждая из упомянутых по меньшей мере одной областей содержит подобъект из упомянутых по меньшей мере одного подобъектов.

21. Система по п.19, в которой каждый из упомянутых спецификаторов областей содержит контрольную сумму, вычисленную в соответствии с алгоритмом вычисления контрольной суммы.

22. Система по п.21, в которой упомянутую контрольную сумму подсчитывают для области.

23. Система по п.21, в которой упомянутую контрольную сумму подсчитывают для подобъекта, содержащего эту область.

24. Система по п.21, в которой упомянутый подобъект с сигнатурой содержит идентификатор алгоритма контрольной суммы, причем идентификатор идентифицирует используемый алгоритм вычисления контрольной суммы.

25. Система по п.21, в которой каждый из упомянутых спецификаторов областей содержит длину контрольной суммы.

26. Система по п.19, в которой упомянутый подобъект с сигнатурой содержит идентификатор алгоритма сигнатуры, идентифицирующий алгоритм сигнатуры, используемый для создания цифровой сигнатуры.

27. Система по п.19, в которой упомянутый подобъект с сигнатурой содержит идентификатор подписавшейся стороны, идентифицирующий подписавшуюся сторону, для верификации упомянутой цифровой сигнатуры.

28. Система по п.27, в которой упомянутый идентификатор подписавшейся стороны содержит цифровые сертификаты, необходимые для надежной идентификации и верификации открытого ключа упомянутой подписавшейся стороны.

29. Система по п.19, в которой каждый из упомянутых спецификаторов областей содержит значение смещения области, идентифицирующее начальное местоположение соответствующей области в подобъекте.

30. Система по п.19, в которой каждый из упомянутых спецификаторов областей содержит размер области, идентифицирующий размер соответствующей области в подобъекте.

31. Система по п.19, в которой упомянутый объект представляет собой объект заголовка для ASF файла.

32. Система по п.31, в которой упомянутый новый объект дополнительно содержит идентификатор GUID.

33. Система для проверки достоверности цифровой сигнатуры для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутая система производит проверку достоверности цифровой сигнатуры для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной

областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, при этом система включает в себя:

средство идентификации области для идентификации области, соответствующей каждому из упомянутых спецификаторов области;

средство создания объекта данных, для создания объекта данных, содержащего упомянутый массив и, для каждого из упомянутых спецификаторов области, упомянутую область, соответствующую упомянутому спецификатору области; и

средство проверки достоверности для проверки достоверности упомянутой цифровой сигнатуры, используемой в упомянутом объекте данных.

34. Система по п.33, в которой упомянутый объект представляет собой объект заголовка для ASF файла.

35. Система для проверки достоверности цифровой сигнатуры для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутая система производит проверку достоверности цифровой сигнатуры по меньшей мере для одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, при этом упомянутая система включает в себя:

средство подсчета для определения числа цифровых сигнатур, присутствующих в упомянутом цифровом объекте;

средство проверки достоверности для проверки достоверности каждой из упомянутых цифровых сигнатур.

36. Система по п.35, которая дополнительно содержит:

средство возврата значения ошибки, если число цифровых сигнатур, присутствующих в упомянутом цифровом объекте, равно нулю.

37. Считываемый компьютером носитель, содержащий команды для обеспечения цифровой сигнатуры для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутый считываемый компьютером носитель обеспечивает цифровую сигнатуру для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем упомянутые подобъекты могут быть переупорядочены в объекте без нарушения достоверности цифровой сигнатуры, при этом упомянутые команды предусматривают операции:

создание массива, содержащего для каждой из упомянутых по меньшей мере одной областей, спецификатор области, идентифицирующий упомянутую область;

формирование цифровой сигнатуры на основании данных, которые содержат каждую область и упомянутый массив; и

добавление подобъекта с сигнатурой, содержащего упомянутый массив и упомянутую цифровую сигнатуру, в цифровой объект.

38. Считываемый компьютером носитель по п.37, в котором каждая из упомянутых по меньшей мере одной областей содержит подобъект из упомянутых по меньшей мере одного подобъектов.

39. Считываемый компьютером носитель по п.37, в котором каждый из упомянутых спецификаторов области содержит контрольную сумму, вычисленную в соответствии с алгоритмом вычисления контрольной суммы.

40. Считываемый компьютером носитель по п.39, в котором упомянутую контрольную сумму подсчитывают для области.

41. Считываемый компьютером носитель по п.39, в котором упомянутую контрольную сумму подсчитывают для подобъекта, содержащего область.

42. Считываемый компьютером носитель по п.39, в котором упомянутый подобъект с сигнатурой содержит идентификатор алгоритма вычисления контрольной суммы для

идентификации используемого алгоритма вычисления контрольной суммы.

43. Считываемый компьютером носитель по п.39, в котором каждый из упомянутых спецификаторов области содержит длину контрольной суммы.

44. Считываемый компьютером носитель по п.37, в котором упомянутый подобъект с сигнатурой содержит идентификатор алгоритма сигнатуры для идентификации алгоритма сигнатуры, используемого для создания цифровой сигнатуры.

45. Считываемый компьютером носитель по п.37, в котором упомянутый подобъект с сигнатурой содержит идентификатор подписавшейся стороны, идентифицирующий подписавшуюся сторону, для верификации упомянутой цифровой сигнатуры.

46. Считываемый компьютером носитель по п.45, в котором упомянутый идентификатор подписавшейся стороны содержит цифровые сертификаты, необходимые для надежной идентификации и верификации открытого ключа упомянутой подписавшейся стороны.

47. Считываемый компьютером носитель по п.37, в котором каждый из упомянутых спецификаторов областей содержит значение смещения области, идентифицирующее начальное местоположение соответствующей области в подобъекте.

48. Считываемый компьютером носитель по п.37, в котором каждый из упомянутых спецификаторов областей содержит размер области, идентифицирующий размер соответствующей области в подобъекте.

49. Считываемый компьютером носитель по п.37, в котором упомянутый объект представляет собой объект заголовка для ASF файла.

50. Считываемый компьютером носитель по п.49, в котором упомянутый новый объект дополнительно содержит идентификатор GUID.

51. Считываемый компьютером носитель, содержащий команды для проверки достоверности цифровой сигнатуры, для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутые команды производят проверку достоверности цифровой сигнатуры по меньшей мере для одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, при этом команды для осуществления действий предусматривают операции:

идентификацию области, соответствующей каждому из упомянутых спецификаторов области;

создание объекта данных, содержащего упомянутый массив и, для каждого из упомянутых спецификаторов области, упомянутую область, соответствующую упомянутому спецификатору области; и

проверку достоверности упомянутой цифровой сигнатуры с использованием в упомянутом объекте данных.

52. Считываемый компьютером носитель по п.51, в котором упомянутый объект представляет собой объект заголовка для ASF файла.

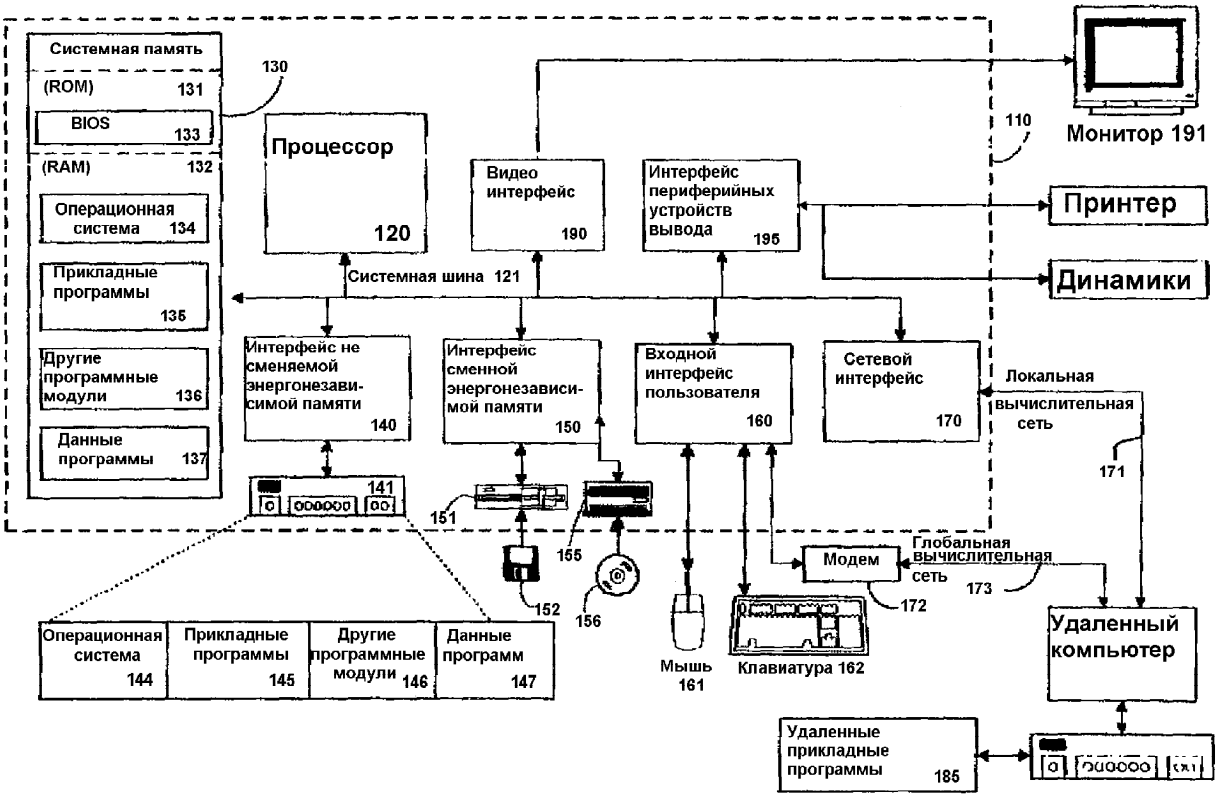
53. Считываемый компьютером носитель, содержащий команды для проверки достоверности цифровой сигнатуры для использования в комбинации с цифровым объектом, который содержит по меньшей мере один подобъект, причем упомянутые команды производят проверку достоверности цифровой сигнатуры для по меньшей мере одной области, при этом каждая из упомянутых по меньшей мере одной областей состоит из всего или части одного из упомянутых по меньшей мере одного подобъекта, причем массив содержит спецификаторы областей для каждой из упомянутых по меньшей мере одной областей, при этом команды для осуществления действий предусматривают:

определение числа цифровых сигнатур, присутствующих в упомянутом цифровом объекте;

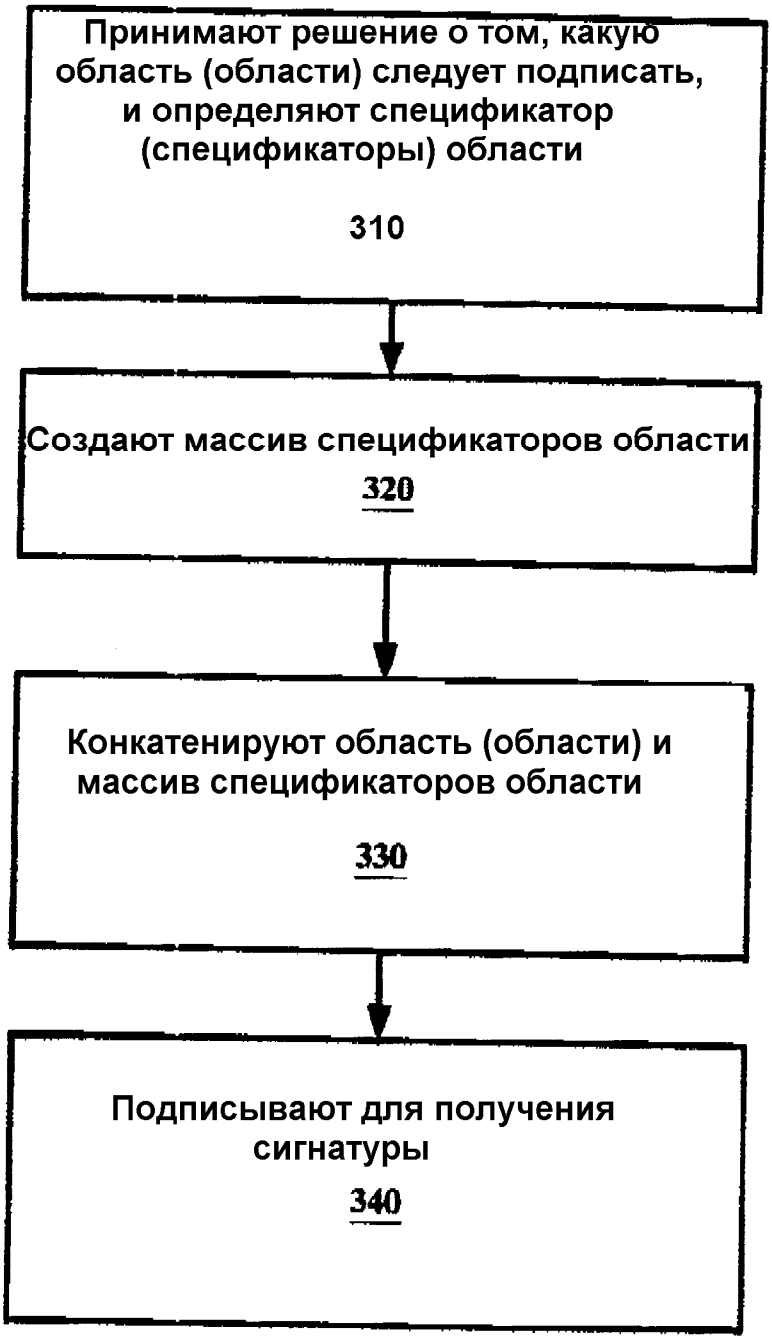
проверку достоверности каждой из упомянутых цифровых сигнатур.

54. Считываемый компьютером носитель по п.53, причем упомянутый считываемый компьютером носитель с командами для осуществления действий дополнительно

предусматривает возврат значения ошибки, если число цифровых сигнатур, присутствующих в упомянутом цифровом объекте, равно нулю.


Компьютер 100
Системная память
(ROM) 131
BIOS 133
(RAM) 132
Операционная система 134
Прикладные программы 135
Другие программные модули 136
Данные программы 137
130
Процессор 120
Видео интерфейс 190
Интерфейс периферийных устройств вывода 195
110
Монитор 191
Принтер
Динамики
Системная шина 121
Интерфейс не сменяемой энергонезависимой памяти 140
Интерфейс сменной энергонезависимой памяти 150
Входной интерфейс пользователя 160
Сетевой интерфейс 170
Локальная вычислительная сеть
171
141
151
155
152
156
Модем
Глобальная вычислительная сеть
173
172
Удаленный компьютер
Операционная система 144
Прикладные программы 145
Другие программные модули 146
Данные программ 147
Мышь 161
Клавиатура 162
Удаленные прикладные программы 185

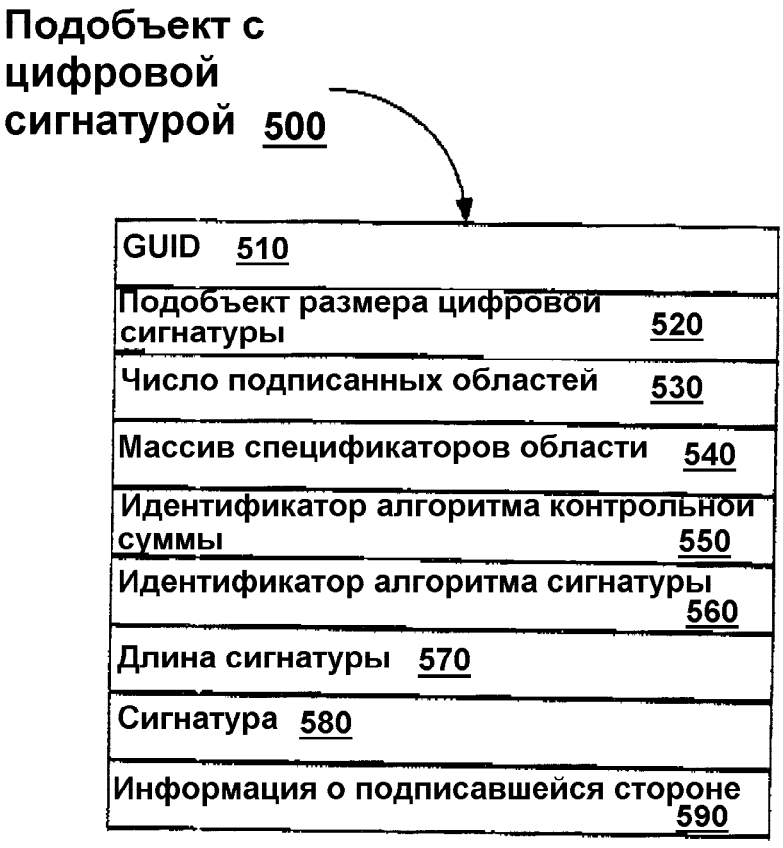
ФИГ. 1


Принимают решение о том, какую область (области) следует подписать, и определяют спецификатор (спецификаторы) области
310
Создают массив спецификаторов области
320
Конкатенируют область (области) и массив спецификаторов области
330
Подписывают для получения сигнатуры
340

ФИГ. 3


Идентифицируют область (области) в массиве спецификаторов областей
410
Конкатенируют область (области) и массив спецификаторов областей
420
Проверяют сигнатуру
430

ФИГ. 4


Подобъект с цифровой сигнатурой 500
GUID 510
Подобъект размера цифровой сигнатуры 520
Число подписанных областей 530
Массив спецификаторов области 540
Идентификатор алгоритма контрольной суммы 550
Идентификатор алгоритма сигнатуры 560
Длина сигнатуры 570
Сигнатура 580
Информация о подписавшейся стороне 590

ФИГ. 5