РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 467 390** (13) **C2**

(51) МПК
G06F 21/00 (2006.01)
G06F 12/14 (2006.01)
G07C 5/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2009134528/08, 21.01.2008**

(24) Дата начала отсчета срока действия патента:
21.01.2008

Приоритет(ы):
(30) Конвенционный приоритет:
16.02.2007 DE 102007008293.4

(43) Дата публикации заявки: **27.03.2011** Бюл. № 9

(45) Опубликовано: **20.11.2012** Бюл. № 32

(56) Список документов, цитированных в отчете о поиске: **US 2005/0050342 A1, 03.03.2005. EA 006223 B1, 27.10.2005. WO 2006/000507 A1, 05.01.2006. WO 2006/010347 A1, 02.02.2006. EP 1049988 B1, 04.09.2002. RU 2277720 C2, 10.06.2006.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **16.09.2009**

(86) Заявка PCT:
EP 2008/050600 (21.01.2008)

(87) Публикация заявки PCT:
WO 2008/098817 (21.08.2008)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову

(72) Автор(ы):
КИММИХ Франц (DE),
ГЕРБЕР Рудольф (DE),
ГЕТЦ Манфред (DE)

(73) Патентообладатель(и):
КОНТИНЕНТАЛЬ АУТОМОТИВЕ ГМБХ (DE)

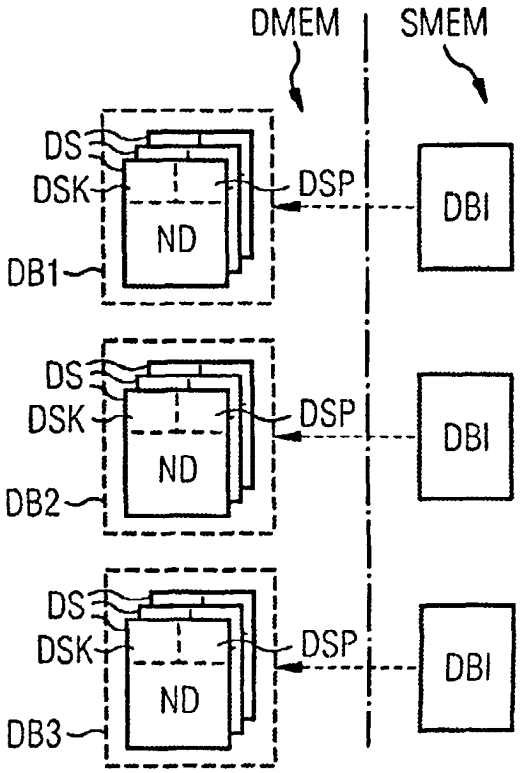
RU 2467390 C2

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ БЕЗОПАСНОГО ХРАНЕНИЯ И ДЛЯ БЕЗОПАСНОГО СЧИТЫВАНИЯ ПОЛЕЗНЫХ ДАННЫХ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в снижении продолжительности времени, которое должно использоваться для защиты целостности. Способ безопасного хранения полезных данных в цифровом тахографе, при котором полезные данные сохраняются в, по меньшей мере, одном блоке данных в, по меньшей мере, одной заданной логической области данных, с, по меньшей мере, одним блоком данных соотносится, соответственно, код опознавания блока данных, который включает в себя однозначный в соответствующей заданной области данных маркер однозначности, однозначный код опознавания области данных заданной области данных, в которой сохранен соответствующий блок данных, и логическую позицию соответствующего блока данных внутри соответствующей заданной области данных, и код опознавания блока данных сохраняется, для полезных данных и сопоставленного кода опознавания блока данных определяется и

сохраняется контрольное значение блока данных, с соответствующей заданной областью данных соотносится информация области данных и защищенным или безопасным образом сохраняется. 4 н. и 7 з.п. ф-лы, 7 ил.



ФИГ.2

RU 2467390 C2

RU 2467390 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 467 390** (13) **C2**

(51) Int. Cl.
G06F 21/00 (2006.01)
G06F 12/14 (2006.01)
G07C 5/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009134528/08, 21.01.2008**

(24) Effective date for property rights:
21.01.2008

Priority:
(30) Convention priority:
16.02.2007 DE 102007008293.4

(43) Application published: **27.03.2011** Bull. 9

(45) Date of publication: **20.11.2012 Bull. 32**

(85) Commencement of national phase: **16.09.2009**

(86) PCT application:
EP 2008/050600 (21.01.2008)

(87) PCT publication:
WO 2008/098817 (21.08.2008)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu

(72) Inventor(s):
KIMMIKh Frants (DE),
GERBER Rudol'f (DE),
GETTs Manfred (DE)

(73) Proprietor(s):
KONTINENTAL' AUTOMOTIVE GMBKh (DE)

RU 2467390 C2

(54) METHOD AND APPARATUS FOR SAFE STORAGE AND SAFE READING OF USEFUL DATA

(57) Abstract:

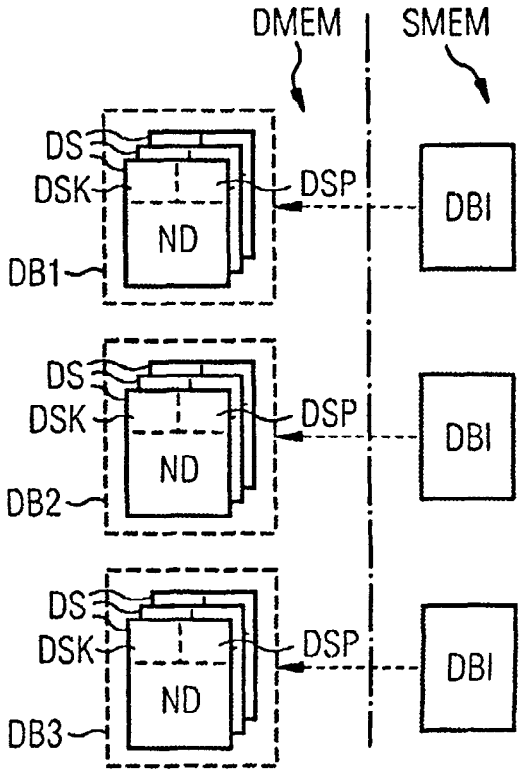
FIELD: physics, computer engineering.

SUBSTANCE: invention relates to computer engineering. The method for safe storage of useful data in a digital tachograph, wherein useful data are stored in at least one data unit in at least a given logic data region; at least one data unit is, respectively, associated with a data unit identification code which includes, in the corresponding given data region, a unique uniqueness marker, a unique data region identification code for the given data region, in which the corresponding data unit is stored, and a logic position for the corresponding data unit inside the corresponding given data region, and the data unit identification code is stored; for useful data and the matched data unit identification code, the control data unit value is determined and stored; data region information is associated with the corresponding given data region and then securely or safely stored.

EFFECT: shorter time to be used to protect integrity.

11 cl, 7 dwg

RU 2467390 C2



ФИГ.2

RU 2467390 C2

RU 2467390 C2

Изобретение относится к способу и устройству для безопасного хранения и для безопасного считывания полезных данных, в частности, в цифровом тахографе.

В WO 2005/098567 A1 раскрыто устройство с интегральной схемой. Интегральная схема включает в себя блок шифрования в качестве функционального модуля, посредством которого данные или программный код может зашифровываться и расшифровываться. Кроме того, для защиты от манипуляций предусмотрена защитная сенсорика в качестве функционального модуля, посредством которого, по меньшей мере, один рабочий параметр интегральной схемы может контролироваться. Защитный слой может быть выполнен на интегральной схеме и может контролироваться. Защитный слой должен быть разрушен, чтобы иметь возможность механически получить доступ к структуре интегральной схемы. Если разрушение защитного слоя распознается, то вызывается стирание защищаемых данных.

US 2005/0050342 A1 раскрывает систему хранения данных для надежного хранения информации. Система хранения данных защищает от модифицирования информации, так как криптографическое проверочное значение, например контрольная сумма, является функцией данных, криптографического ключа и адреса блока данных. Информация надежным образом защищается, причем обеспечивается возможность доступа типа контрольной проверки для актуализации блоков данных.

Задачей изобретения является создание способа и устройства для безопасного хранения и способа и устройства для безопасного считывания полезных данных, которые являются надежными.

Эта задача решается признаками независимых пунктов формулы изобретения. Предпочтительные варианты осуществления изобретения приведены в зависимых пунктах формулы изобретения.

Согласно первому аспекту изобретение характеризуется способом и соответствующим устройством для безопасного хранения полезных данных. Полезные данные сохраняются в, по меньшей мере, одном блоке данных в, по меньшей мере, одной заданной логической области данных. С, по меньшей мере, одним блоком данных соотносится, соответственно, код опознавания блока данных, который включает в себя однозначный в соответствующей заданной области данных маркер однозначности, однозначный код опознавания области данных заданной области данных, в которой сохранен соответствующий блок данных, и логическая позиция соответствующего блока данных внутри соответствующей заданной области данных. Код опознавания блока данных сохраняется. К полезным данным и соответственно сопоставленному коду опознавания блока данных соответствующего блока данных определяется и сохраняется контрольное значение блока данных. С соответствующей заданной областью данных соотносится информация области данных, которая включает в себя код опознавания области данных, соответствующей заданной области данных. Информация области данных включает в себя, кроме того, информацию о, по меньшей мере, одной области значений маркера однозначности блоков данных, сохраненных в текущий момент в соответствующей заданной области данных. Соответствующая информация области данных защищенным или безопасным образом сохраняется.

Защищенное сохранение означает, что сохраненные таким образом данные сохраняются защищенным от манипуляций способом. Защищенное сохранение осуществляется предпочтительно в защищенной памяти, в которой данные электрически и/или механически защищены от манипуляций. Безопасное хранение означает, что сохраненные таким образом данные могут проверяться на предмет

манипуляций, например, путем проверки криптографически определенного контрольного значения, как, например, контрольного значения блока данных или криптографически определенной цифровой сигнатуры. Безопасное хранение имеет преимущество, состоящее в том, что сохраненные таким образом данные могут просто и надежно проверяться на их целостность и что данные, кроме того, не должны сохраняться в защищенной памяти. На основе, в общем случае, высокой стоимости защищенной памяти можно, таким образом, экономить затраты. Защищенное или безопасное хранение включает в себя, в частности, криптографически защищенное или безопасное хранение, то есть, в частности, использование криптографического ключа и/или криптографического алгоритма для обеспечения защищенности.

Посредством обеспечения контрольного значения блока данных можно надежно распознавать манипуляцию над полезными данными и/или соответствующим кодом опознавания данных. На основе кода опознавания области данных надежно распознается обмен блоком данных между различными заданными областями данных. Кроме того, на основе логической позиции блока данных внутри соответствующей заданной области данных надежно распознается замена блоков данных. На основе маркера однозначности и информации для, по меньшей мере, одной области значений маркера однозначности надежно распознаются так называемые атаки методом записи и повторной передачи шифрованных блоков. При таком методе атаки, например старый блок данных, который стал недействительным, однако имеет корректное контрольное значение блока данных, выдается как новый блок данных.

Посредством названных мер полезные данные сохраняются безопасным образом. Манипуляции полезными данными могут просто и надежно распознаваться. Кроме того, обеспечение кода опознавания блока данных, контрольного значения блока данных и информации области данных обеспечивает возможность быстрого доступа к полезным данным, в частности быструю безопасную запись и быстрое безопасное считывание и проверку полезных данных. Дополнительное преимущество состоит в том, что полезные данные и код опознавания блока данных не должны храниться в защищенной памяти.

В предпочтительном варианте выполнения безопасное хранение соответствующей информации области данных включает в себя определение общего или соответствующего контрольного значения области данных, по меньшей мере, одной информации области данных, по меньшей мере, одной заданной области данных и сохранение защищенным или безопасным образом. Преимуществом является то, что манипуляции над, по меньшей мере, одной информацией области данных надежно распознаются. Кроме того, по меньшей мере, одна информация области данных не должна, таким образом, сохраняться в защищенной памяти. Защищенная память может тем самым выполняться с особенно малой емкостью памяти и, соответственно, быть экономичной. Кроме того, целостность, по меньшей мере, одной информации области данных может проверяться просто, быстро и надежно.

В другом предпочтительном варианте осуществления с соответствующей заданной областью данных соотнесен список исключений ставших недействительными блоков данных. Соответствующий блок данных, который стал недействительным, регистрируется в списке исключений. Список исключений хранится защищенным или безопасным образом. За счет этого могут надежно предотвращаться атаки методом записи и повторной передачи блоков шифрованного текста. Кроме того, возможно

такое стирание блока данных, посредством которого последний становится недействительным, без угрозы целостности тех, которые находятся в заданной области данных.

В этой связи является предпочтительным, если посредством регистрации соответствующего, ставшего недействительным блока данных в списке исключений, соответствующий маркер однозначности заносится в список исключений, или в зависимости от него, по меньшей мере, одна область значений ставшего недействительным маркера однозначности заносится в список исключений или расширяется в списке исключений. Это имеет преимущество, заключающееся в том, что потребность в пространстве хранения для списка исключений мала, в особенности, если предусматривается, по меньшей мере, одна область значений ставших недействительными маркеров однозначности. Кроме того, список исключений можно просмотреть, таким образом, особенно быстро.

В другом предпочтительном варианте осуществления определяется текущий маркер времени и сохраняется в соответствующем коде опознавания блока данных. Тем самым связанные во времени блоки данных очень просто и быстро могут определяться, в особенности также в двух или более заданных областях данных.

Согласно второму аспекту изобретение характеризуется способом и соответствующим устройством для надежного считывания полезных данных. Считываются полезные данные, по меньшей мере, одного блока данных, которые сохранены в, по меньшей мере, одной заданной логической области данных. Считывается соотнесенный с, по меньшей мере, одним блоком данных код опознавания блока данных, который содержит маркер однозначности, однозначный в соответствующей заданной области данных, однозначный код опознавания области данных заданной области данных, в которой сохранен соответствующий блок данных, и логическую позицию соответствующего блока данных внутри соответствующей заданной области данных. Считывается контрольное значение блока данных, которое сохранено для полезных данных и соотнесенного кода опознавания блока данных соответствующего блока данных. Определяется соответствующее контрольное значение блока данных сравнения. Считывается информация области данных, соотнесенная с соответствующей заданной областью данных, которая включает в себя код опознавания области данных, соответствующей заданной области данных, и информацию для, по меньшей мере, одной области значений маркера однозначности блоков данных, сохраненных в текущий момент в соответствующей заданной области данных. Целостность полезных данных соответствующего считанного блока данных контролируется в зависимости от соответствующего кода опознавания блока данных, соответствующего контрольного значения блока данных, соответствующего контрольного значения блока данных сравнения и соотнесенной информации области данных.

Безопасное считывание означает, что считанные таким образом данные проверяются на предмет манипуляций, например, путем проверки криптографически определенного контрольного значения, как, например, контрольного значения блока данных или криптографически определенной цифровой сигнатуры.

На основе контрольного значения блока данных надежным образом распознается манипуляция с полезными данными и/или соответствующим кодом опознавания блока данных. На основе кода опознавания области данных надежным образом распознается замена блока данных между различными заданными областями данных. Кроме того, на основе логической позиции блока данных внутри соответствующей

заданной области данных надежным образом распознается подмена блоков данных. На основе маркера однозначности и информации для, по меньшей мере, одной области значений маркеров однозначности надежным образом распознается так называемая атака методом записи и повторной передачи шифрованных блоков. При таком методе атаки, например, старый блок данных, который стал недействительным, однако имеет корректное контрольное значение, выдается как новый блок данных.

Посредством названных мер полезные данные сохраняются безопасным образом. Манипуляции над полезными данными могут просто и надежно распознаваться. Кроме того, обеспечение кода опознавания блока данных, контрольного значения блока данных и информации области данных обеспечивает возможность быстрого доступа к полезным данным, в частности быстрое безопасное считывание и проверку полезных данных.

В предпочтительном варианте осуществления второго аспекта считывается, по меньшей мере, одно общее или соответствующее контрольное значение области данных, по меньшей мере, одной информации области данных для, по меньшей мере, одной заданной области данных. Определяется соответствующее общее или соответствующее контрольное значение области данных сравнения, по меньшей мере, одной заданной области данных. Целостность полезных данных соответствующего блока данных проверяется в зависимости от, по меньшей мере, одного считанного контрольного значения области данных и, по меньшей мере, одного контрольного значения области данных сравнения. Предпочтительным является то, что надежным образом распознаются манипуляции с, по меньшей мере, одной информацией области данных. Кроме того, целостность, по меньшей мере, одной информации области данных проверяется просто, быстро и надежным образом.

В другом предпочтительном варианте осуществления второго аспекта осуществляется просмотр списка исключений ставших недействительными блоков данных соответствующей заданной области данных после регистрации соответствующего считанного блока данных. Целостность полезных данных в соответствующем блоке данных проверяется в зависимости от зарегистрированных в списке исключений ставших недействительными блоков данных. Список исключений, соотнесенный с соответствующей заданной областью данных, считывается защищенным или безопасным образом, то есть из защищенной от манипуляций памяти и/или проверяется на его целостность. Иначе говоря, проверка целостности полезных данных включает в себя, при необходимости, также проверку целостности списка исключений. За счет этого могут надежно предотвращаться атаки методом записи и повторной передачи блоков шифрованного текста. Кроме того, таким образом, стертый блок данных, который вследствие стирания стал недействительным, не может угрожать целостности данных, сохраненных в соответствующей заданной области данных.

В этой связи является предпочтительным, если целостность полезных данных в соответствующем блоке данных проверяется в зависимости от занесенных в список исключений ставших недействительными маркеров или в зависимости от, по меньшей мере, одной области значений ставших недействительными маркеров однозначности, которая занесена в список исключений. Это имеет преимущество, заключающееся в том, что потребность в пространстве хранения памяти для списка исключений мала, в особенности, если предусматривается, по меньшей мере, одна область значений ставших недействительными маркеров однозначности. Кроме того, список исключений можно просмотреть, таким образом, особенно быстро.

Примеры выполнения изобретения поясняются далее со ссылками на схематичные чертежи, на которых показано следующее:

Фиг.1 - цифровой тахограф,

Фиг.2 - первая форма выполнения логической конфигурации данных,

Фиг.3 - вторая форма выполнения логической конфигурации данных,

Фиг.4 - код опознавания блока данных,

Фиг.5 - информация области данных,

Фиг.6 - диаграмма процесса программы для безопасного хранения полезных данных, и

Фиг.7 - диаграмма процесса программы безопасного считывания полезных данных.

Элементы одинаковой структуры или функции на чертежах обозначены одинаковыми ссылочными позициями.

Цифровой тахограф TCO содержит защищенную память SMEM, память DMEM данных, часы RTC реального времени и, по меньшей мере, один блок считывания чип-карты, в который может вставляться чип-карта СК, например так называемая карта тахографа или заводская карта (фиг.1). Часы RTC реального времени предпочтительно выполнены защищенными от манипуляций и могут устанавливаться только уполномоченными лицами, которые могут удостоверять себя посредством соответствующей чип-карты СК, например посредством заводской карты по отношению к тахографу TCO. Тахограф TCO для определения путевой скорости транспортного средства, на котором тахограф TCO предпочтительным образом размещен, связан с, по меньшей мере, одним счетчиком RDS числа оборотов колеса. Тахограф TCO может также определяться как устройство для записи и/или считывания полезных данных ND.

Защищенная память SMEM предпочтительно защищена электрически и/или механически от манипуляций с сохраненными в ней данными. Например, защищенная память SMEM снабжается защитным слоем или защитной сеткой, которая, например, электрически контролируется. При повреждении защитного слоя или защитной сетки может предотвращаться доступ к данным, сохраненным в защищенной памяти SMEM, например, путем стирания данных. Защищенная память SMEM может также быть выполнена иным образом.

Память DMEM данных предпочтительно выполнена незащищенной, то есть, в частности, не защищена электрически и/или механически от манипуляций. Ввиду обычно более высокой стоимости защищенной памяти SMEM по отношению к памяти DMEM данных защищенная память SMEM имеет лишь малую емкость памяти по сравнению с памятью DMEM данных. Однако данные, сохраненные в памяти DMEM данных, также должны быть защищены. В частности, манипуляции с данными должны надежным образом распознаваться. Поэтому тахограф TCO выполнен таким образом, чтобы хранить данные в памяти DMEM данных безопасным образом и считывать из нее данные безопасным образом. Данные, сохраненные в памяти DMEM данных, для этого сохраняются с возможностью криптографической проверки на манипуляции и при считывании проверяются, чтобы иметь возможность установить целостность считываемых данных или распознать манипуляции.

Данные, сохраненные в памяти DMEM данных, включают в себя полезные данные ND, которые содержат, например, определяемую путевую скорость. Чип-карта СК может содержать другую защищенную память и другую память данных, соответствующие защищенной памяти SMEM и памяти DMEM данных тахографа TCO. Соответственно данные также могут безопасно храниться в другой памяти

данных чип-карты СК или безопасно считываться из нее.

На фиг.2 показана первая форма выполнения логической конфигурации данных для данных в памяти DMEM данных и защищенной памяти SMEM. Соответствующая логическая конфигурация данных может быть предусмотрена также в другой памяти данных чип-карты СК и в другой защищенной памяти чип-карты СК. В памяти DMEM данных предусмотрена, по меньшей мере, одна заданная область данных для хранения, соответственно, по меньшей мере, одного блока DS данных. Например, на фиг.2 представлены первая заданная область DB1 данных, вторая заданная область DB2 данных и третья заданная область DB3 данных. Но может также предусматриваться только одна заданная область данных. Также могут предусматриваться две или более трех заданных областей данных.

Различные заданные области данных могут быть предусмотрены для различных типов данных или структур данных. Однако также могут несколько заданных областей данных предназначаться для одинаковых типов данных или структур данных. Кроме того, также может быть предусмотрено хранение различных типов данных или структур данных совместно в одной из заданных областей данных. Например, одна из заданных областей данных может быть предусмотрена для безопасного хранения полученной путевой скорости в качестве полезных данных ND. Другая из заданных областей данных может быть предусмотрена для безопасного хранения момента ввода и момента извлечения чип-карты СК в/из блока считывания чип-карты СК тахографа ТСО в качестве полезных данных ND. Однако могут также храниться другие или дополнительные полезные данные ND.

Блоки DS данных, которые могут храниться в заданных областях данных, включают в себя, соответственно, полезные данные ND, код DSK опознавания блока данных и контрольное значение DSP блока данных. Контрольное значение DSP блока данных формируется на основе полезных данных ND и кода DSK опознавания блока данных соответствующего блока DS данных. Контрольное значение DSP блока данных формируется предпочтительно криптографическим способом, например, как цифровая сигнатура или как код аутентификации сообщения, обозначаемый как MAC. Однако контрольное значение DSP блока данных может также формироваться иным образом. Код DSK опознавания блока данных и контрольное значение DSP блока данных логически сопоставлены соответствующему блоку DS данных, однако не должны вместе с полезными данными ND храниться в соответствующей заданной области данных. Код DSK опознавания блока данных и контрольное значение DSP блока данных соответствующего блока DS данных могут также храниться в другом месте, например на другом носителе данных.

По меньшей мере, одна заданная область данных предпочтительно выполнена как кольцевое ЗУ с заданным максимальным числом MAX_DS блоков DS данных, которые могут сохраняться в соответствующем кольцевом ЗУ, то есть в соответствующей заданной области данных. Соответствующее кольцевое ЗУ отличается тем, что блоки DS данных следуют только друг за другом, сохраняться могут в заданных позициях POS, и при сохранении блока DS данных, который заново сохраняется в кольцевом ЗУ, соответствующий самый старый блок DS данных в кольцевом ЗУ перезаписывается, если достигнуто максимальное число MAX_DS блоков DS данных в соответствующем кольцевом ЗУ, то есть соответствующее кольцевое ЗУ заполнено. По меньшей мере, одна заданная область данных может, однако, выполняться и иным образом.

Для тахографа ТСО максимальное число MAX_DS блоков DS данных

предпочтительно задано так, что полезные данные ND, которые предположительно должны сохраняться в течение заданного промежутка времени, могут сохраняться в соответствующих кольцевых ЗУ, не приводя к перезаписи более старых блоков DS данных. Например, заданный промежуток времени составляет один год. Но заданный промежуток времени может задаваться также более коротким или более длинным.

Соответствующей заданной области данных сопоставляется соответственно информация DBI области данных. В первом примере выполнения соответствующая информация DBI области данных сохранена в защищенной памяти. Тем самым соответствующая информация DBI области данных защищена от манипуляций. Фиг.3 показывает форму выполнения конфигурации данных. Во второй форме выполнения конфигурации данных предусмотрено, что соответствующая информация DBI области данных сохранена в памяти DMEM данных. Чтобы иметь возможность распознавать манипуляции над одной из информаций DBI области данных, предусмотрено, что определяется контрольное значение DBP области данных для соответствующей информации DBI области данных или совместно для двух или более или для всех информаций DBI области данных и сохраняется в защищенной памяти SMEM. Тем самым в защищенной памяти SMEM требуется особенно мало пространства хранения.

Фиг.4 показывает код DSK опознавания блока данных. Код DSK опознавания блока данных соответствующего блока DS данных содержит маркер ES однозначности, код DBK опознавания области данных и логическую позицию POS соответствующего блока DS данных внутри соответствующей заданной области данных. Кроме того, код DSK опознавания блока данных может также включать в себя маркер времени, который предпочтительно формируется часами RTC реального времени. Маркер ES однозначности выполнен таким образом, что он является соответственно однозначным для каждого блока DS данных и соответствующей заданной области данных. Это включает то, что уже использованный и ставший недействительным маркер ES однозначности в соответствующей заданной области данных вновь не используется для нового блока DS данных и что новый и до сих пор не использовавшийся в соответствующей заданной области данных маркер ES однозначности формируется и используется для блока DS данных, который был изменен. Предпочтительным образом маркер ES однозначности выполнен как последовательное текущее число, например, из множества целых чисел или из множества натуральных чисел. Маркер ES однозначности может также выполняться иным образом, например, как модифицированный маркер времени. Модификация предусматривается, чтобы предотвратить повторное появление того же самого маркера ES однозначности, когда время переустанавливается. Код DBK опознавания области данных является однозначной ссылкой на заданную область данных, с которой сопоставлен соответствующий блок DS данных.

На фиг.5 показана информация DBI области данных. Информация DBI области данных включает в себя код DBK опознавания области данных и информацию для, по меньшей мере, одной области значений маркера ES однозначности блоков DS данных, сохраненных в текущий момент в соответствующей заданной области данных. Эта информация включает в себя, в частности, маркер ES_MIN однозначности с наименьшим значением всех сохраненных в текущий момент блоков DS данных соответствующей области данных. Кроме того, эта информация может включать в себя также маркер ES_MAX однозначности с наибольшим значением всех сохраненных в текущий момент блоков DS данных соответствующей области данных. С помощью маркера ES_MIN однозначности с наименьшим значением и

маркера ES_MAX однозначности с наибольшим значением задается диапазон значений маркера ES однозначности. Маркер ES однозначности только тогда действителен, если он находится внутри такого диапазона значений. За счет стирания, изменения или добавления блоков DS данных к соответствующей заданной области данных информация для, по меньшей мере, одной области значений маркера ES однозначности в информации DBI области данных соответственно согласуется. В особенности может быть предусмотрено, что два или более диапазона значений маркера ES однозначности предусматриваются в соответствующей информации DBI области данных, если последовательность маркеров ES однозначности блоков DS данных в соответствующей заданной области данных имеет один или более пропусков. Такие пропуски могут возникать, например, за счет стирания блока DS данных или нескольких блоков DS данных. Под стиранием здесь также понимается то, что стираемый блок DS данных маркируется как стертый или недействительный. Недействительным соответствующий блок DS данных становится также, например, вследствие того, что его маркер ES однозначности не находится внутри, по меньшей мере, одного диапазона значений маркера ES однозначности. Множество диапазонов значений маркера ES однозначности могут сохраняться или считываться, например, как связанный список или как несколько связанных списков.

В качестве альтернативы или дополнительно, может предусматриваться список AL исключений, который сопоставлен соответствующей информации DBI области данных. В списке AL исключений зарегистрированы стертые, то есть ставшие недействительными, блоки DS данных. Для этого, например, соответствующий маркер ES однозначности заносится в список AL исключений. Может быть также предусмотрено, что диапазон значений ставших недействительными маркеров ES однозначности для соответственно ставшего недействительным блока DS данных заносится в список AL исключений, или уже занесенный в список AL исключений диапазон значений ставших недействительными маркеров ES однозначности расширяется в зависимости от того маркера ES однозначности, который должен маркироваться как недействительный. Тем самым, блок DS данных действителен только в том случае, если его соответствующий маркер ES однозначности лежит в, по меньшей мере, одном диапазоне значений маркера ES однозначности и его соответствующий маркер ES однозначности не занесен в список AL исключений. Список AL исключений предпочтительно сохраняется защищенным или безопасным образом, чтобы предотвратить несанкционированное манипулирование списком AL исключений.

Кроме того, является предпочтительным, чтобы в соответствующей информации области данных предусмотреть новейшую позицию NPOS сохраненного последним блока DS данных в соответствующей заданной области данных, и/или позицию хранения SPOS следующей к записываемой позиции POS в соответствующей заданной области данных, и/или число ANZ_DS блоков DS данных, которые сохранены в соответствующей заданной области данных, и/или максимальное число MAX_DS блоков DS данных, которые могут быть сохранены в соответствующей заданной области данных. За счет обеспечения этой информации в соответствующей информации DBI области данных можно особенно просто и быстро осуществлять доступ к блокам DS данных соответствующей заданной области данных. Однако не обязательно все эти информации предусматривать в информации DBI области данных. Например, максимальное число MAX_DS блоков DS данных, которые могут быть сохранены в соответствующей заданной области данных, также может кодироваться

постоянным образом в программе, которая выполняет безопасную запись и/или считывание. Кроме того, при необходимости, позиция записи SPOS может определяться из другой информации, в частности, если, по меньшей мере, одна заданная область данных выполнена как кольцевое ЗУ. Например, в качестве позиции записи SPOS может определяться позиция POS, следующая за новейшей позицией NPOS с учетом максимального числа MAX_DS блоков DS данных. Кроме того, при необходимости, маркер ES_MAX однозначности с наибольшим значением может определяться в зависимости от новейшей позиции NPOS и позиции записи SPOS и поэтому может не предусматриваться. Кроме того, при необходимости, новейшая позиция NPOS и позиция записи SPOS могут не предусматриваться, если предусмотрено число ANZ_DS блоков DS данных в соответствующей заданной области данных.

Фиг.6 показывает диаграмму процесса программы для безопасной записи полезных данных ND. Программа начинается на этапе S1. На этапе S2 полезные данные ND сохраняются в, по меньшей мере, одном блоке DS данных. Соответствующий блок DS данных сопоставлен заданной области данных. Это сопоставление осуществляется, например, в зависимости от типа данных или структуры данных сохраняемых полезных данных ND. На этапе S3 генерируется соответствующий код DSK опознавания блока данных и сохраняется для соответствующего блока DS данных. На этапе S4 может предусматриваться, что генерируется временной маркер ZS и и сохраняется в соответствующем коде DSK опознавания блока данных.

На этапе S5 определяется соответствующее контрольное значение DSP блока данных в зависимости от соответствующих полезных данных ND и соответствующего кода DSK опознавания блока данных. Соответствующее контрольное значение DSP блока данных сохраняется для соответствующего блока DS данных. На этапе S6 генерируется соответствующая информация DBI области данных для соответственно сопоставленной заданной области данных и сохраняется или, если она уже сохранена, актуализируется. Это касается особенно информации о, по меньшей мере, одной области значений маркера ES однозначности и, при необходимости, новейшей позиции NPOS, позиции записи SPOS и/или числа ANZ_DS блоков DS данных. Сохранение информации DBI области данных осуществляется предпочтительно защищенным образом в защищенной памяти SMEM или безопасным образом в памяти DMEM данных. В последнем случае на этапе S7 генерируется соответствующее или общее контрольное значение DBP области данных и сохраняется защищенным образом в защищенной памяти SMEM. Программа завершается на этапе S8.

Также может быть предусмотрен этап S9, который выполняется, например, вместо этапов с S2 по S5, чтобы блок DS данных или два или более блока DS данных стереть или маркировать как недействительные. Соответствующий блок DS данных для этого регистрируется в предусмотренном списке AL исключений, например, путем занесения соответствующего маркера ES однозначности или путем занесения или согласования диапазона значений или нескольких диапазонов значений ставших недействительными маркеров ES однозначности.

На основе сохраненных таким образом данных может проверяться целостность полезных данных ND. Манипулирование полезными данными ND или кодом DSK опознавания блока данных и/или, при обстоятельствах, информацией DBI области данных, то есть нарушение целостности полезных данных ND может распознаваться таким образом. Проверка осуществляется при безопасном считывании полезных данных ND.

Фиг.7 показывает диаграмму процесса программы для безопасного считывания полезных данных ND. Программа начинается на этапе S10. На этапе S11 считываемые полезные данные ND считываются из соответствующих блоков DS данных. Кроме того, на этапе S12 считывается код DSK опознавания блока данных соответственно сопоставленного блока DS данных. На этапе S13 считывается соответствующее контрольное значение DSP блока данных соответствующего блока DS данных. Кроме того, в зависимости от считанных полезных данных ND и соответственно сопоставленного кода DSK опознавания блока данных определяется соответственно сопоставленное контрольное значение VDSP блока данных сравнения. Определение контрольного значения VDSP блока данных сравнения осуществляется предпочтительно таким же способом, что и определение контрольного значения DSP блока данных в безопасной памяти полезных данных ND. Это, однако, зависит от типа контрольного значения DSP блока данных. Кроме того, на этапе S14 может предусматриваться считывание списка AL исключений, который сопоставлен информации DBI области данных, соответствующей заданной области данных, и, при необходимости, проверка на его целостность.

На этапе S15 проверяется, равно ли контрольное значение VDSP блока данных сравнения контрольному значению DSP блока данных. Кроме того, на этапе S15 может проверяться, зарегистрирован ли соответствующий блок DS данных в списке AL исключений. Если определенное контрольное значение VDSP блока данных сравнения не равно соответствующему контрольному значению DSP блока данных или если соответствующий блок DS данных зарегистрирован в списке AL исключений, то программа продолжается на этапе S16, на котором устанавливается, что целостность полезных данных ND нарушена. Программа затем завершается на этапе S17.

Однако если контрольное значение VDSP блока данных сравнения равно контрольному значению DSP блока данных и если соответствующий блок DS данных не зарегистрирован в списке AL исключений, то программа продолжается на этапе S18. На этапе S18 считывается информация DBI области данных, соответствующей заданной области данных. При необходимости, на этапе S19 предусмотрено, что считывается соответствующее и общее контрольное значение DBP области данных и определяется контрольное значение VDBP области данных сравнения соответственно значению DBP области данных. На этапе S20 проверяется, является ли информация в коде DSK опознавания блока данных и в информации DBI области данных достоверной. Например, проверяется, находится ли сохраненный в коде DSK опознавания блока данных маркер ES однозначности внутри, по меньшей мере, одной области данных маркеров ES однозначности. Кроме того, проверяется, совпадает ли код DBK опознавания области данных. Кроме того, предпочтительно проверяется, соответствует ли соответствующая позиция POS, которая сохранена в соответствующем коде DSK опознавания блока данных, фактической позиции POS соответствующего блока DS данных в соответственно сопоставленной заданной области данных. Кроме того, может проверяться, равно ли контрольное значение VDBP области данных сравнения контрольному значению DBP области данных. Если информация в коде DSK опознавания блока данных и в информации DBI области данных не является достоверной или контрольное значение VDBP области данных сравнения не совпадает с контрольным значением DBP области данных, то программа продолжается на этапе S16 и на этапе S17 завершается. В противном случае программа продолжается на этапе S21, на котором устанавливается, что

целостность полезных данных ND имеет место и с высокой вероятностью отсутствуют манипуляции с ними. Программа завершается на этапе S17.

Последовательность соответствующих этапов программ согласно фиг.6 и фиг.7 может быть реализована иным образом. Например, последовательность считывания полезных данных ND, кода DSK опознавания блока данных, информации DBI области данных, контрольного значения DSP блока данных, контрольного значения DBP области данных является несущественной. Кроме того, последовательность проверки может также быть иной, то есть проверки на этапах S15 и S20 могут выполняться в другой последовательности. Соответственно, последовательность записи полезных данных ND, кода DSK опознавания блока данных, информации DBI области данных, контрольного значения DSP блока данных, контрольного значения DBP области данных является несущественной.

За счет безопасного хранения полезных данных ND и за счет безопасного считывания полезных данных ND манипуляции с полезными данными ND распознаются просто и надежно. Распознаваемые манипуляции включают в себя изменение полезных данных ND, кода DSK опознавания блока данных и, при обстоятельствах, информации DBI области данных. Кроме того, манипуляции могут включать в себя изменение положения POS блоков DS данных внутри их соответствующей заданной области данных, замену блоков DS данных между различными заданными областями данных и замену информации DBI области данных. Кроме того, распознаются так называемые атаки методом записи и повторной передачи шифрованных блоков за счет того, что предусматривается маркер ES однозначности и учитывается информация для, по меньшей мере, одной области значений маркеров ES однозначности внутри соответствующей заданной области данных.

Преимущество состоит в том, что только над незначительными количествами данных необходимо проводить криптографические вычисления для определения соответствующего контрольного значения DSP блока данных и контрольного значения VDSP блока данных сравнения и, при необходимости, для определения соответствующего или общего контрольного значения DBP области данных и контрольного значения VDBP области данных сравнения. Моделирование показало, что продолжительность времени, которое должно использоваться для защиты целостности, за счет безопасной записи или безопасного считывания согласно вышеописанному выполнению при больших объемах данных может быть снижено в два-три раза. Доступ к соответствующему блоку DS данных, то есть безопасная запись или безопасное считывание соответствующего блока DS данных, может осуществляться особенно быстро. Безопасная запись или безопасное считывание согласно вышеописанному выполнению особенно тогда предпочтительны, когда безопасным образом сохраненные блоки DS данных не подлежат никаким изменениям или лишь редким изменениям.

Безопасная запись или безопасное считывание согласно вышеописанному выполнению могут использоваться не только в тахографах TCO. Другие устройства в автомобильной области, например приборы управления, или в другой технической области также могут получить выгоды из безопасной записи или безопасного считывания. Например, могут также программные коды, и/или характеристики, и/или другие данные в качестве полезных данных ND записываться и/или считываться безопасным образом.

Формула изобретения

1. Способ безопасного хранения полезных данных (ND) в цифровом тахографе (TC), при котором

полезные данные (ND) сохраняются в, по меньшей мере, одном блоке (DS) данных в, по меньшей мере, одной заданной логической области данных, с, по меньшей мере, одним блоком (DS) данных соотносится, соответственно, код (DSK) опознавания блока данных, который включает в себя однозначный в соответствующей заданной области данных маркер (ES) однозначности, однозначный код (DBK) опознавания области данных заданной области данных, в которой сохранен соответствующий блок (DS) данных, и логическую позицию (POS) соответствующего блока (DS) данных внутри соответствующей заданной области данных, и код (DSK) опознавания блока данных сохраняется,

для полезных данных (ND) и соответственно сопоставленного кода (DSK) опознавания блока данных соответствующего блока (DS) данных определяется и сохраняется контрольное значение (DSP) блока данных, с соответствующей заданной областью данных соотносится информация (DBI) области данных, которая включает в себя код (DBK) опознавания области данных соответствующей заданной области данных и информацию о, по меньшей мере, одной области значений маркеров (ES) однозначности блоков (DS) данных, сохраненных в текущий момент в соответствующей заданной области данных, и соответствующая информация (DBI) области данных защищенным или безопасным образом сохраняется.

2. Способ по п.1, в котором безопасное хранение соответствующей информации (DBI) области данных включает в себя определение и сохранение защищенным или безопасным образом общего или соответствующего контрольного значения (DBP) области данных для, по меньшей мере, одной информации (DBI) области данных из, по меньшей мере, одной заданной области данных.

3. Способ по любому из предыдущих пунктов, в котором

с соответствующей заданной областью данных соотнесен список (AL) исключений ставших недействительными блоков (DS) данных,

соответствующий блок (DS) данных, который стал недействительным, регистрируется в списке (AL) исключений, и

список (AL) исключений сохраняется защищенным или безопасным образом.

4. Способ по п.3, в котором посредством регистрации соответствующего, ставшего недействительным блока (DS) данных в списке (AL) исключений соответствующий маркер (ES) однозначности заносится в список исключений, или в зависимости от него, по меньшей мере, одна область значений ставших недействительными маркеров (ES) однозначности заносится в список (AL) исключений или расширяется в списке (AL) исключений.

5. Способ по п.1, в котором определяется текущий маркер (ZS) времени и сохраняется в соответствующем коде (DSK) опознавания блока данных.

6. Способ безопасного считывания полезных данных (ND) в цифровом тахографе (TC), при котором

считываются полезные данные (ND), по меньшей мере, одного блока (DS) данных, которые сохранены в, по меньшей мере, одной заданной логической области данных,

считывается соотнесенный с, по меньшей мере, одним блоком (DS) данных код (DSK) опознавания блока данных, который содержит маркер (ES) однозначности, однозначный в соответствующей заданной области данных, однозначный код (DBK) опознавания области данных заданной области данных, в которой сохранен

соответствующий блок (DS) данных, и логическую позицию (POS) соответствующего блока (DS) данных внутри соответствующей заданной области данных,

считывается контрольное значение (DSP) блока данных, которое сохранено для полезных данных (ND) и соотнесенного кода (DSK) опознавания блока данных соответствующего блока (DS) данных, и определяется соответствующее контрольное значение (VDSP) блока данных сравнения,

считывается информация (DBI) области данных, соотнесенная с соответствующей заданной областью данных, которая включает в себя код (DBK) опознавания области данных соответствующей заданной области данных и информацию для, по меньшей мере, одной области значений маркеров (ES) однозначности блоков (DS) данных, сохраненных в текущий момент в соответствующей заданной области данных, и

целостность полезных данных (ND) соответствующего считанного блока (DS) данных контролируется в зависимости от соответствующего кода (DSK) опознавания блока данных, соответствующего контрольного значения (DSP) блока данных, соответствующего контрольного значения (VDSP) блока данных сравнения и соотнесенной информации (DBI) области данных.

7. Способ по п.6, в котором

считывается, по меньшей мере, одно общее или соответствующее контрольное значение (DBP) области данных для, по меньшей мере, одной информации (DBI) области данных из, по меньшей мере, одной заданной области данных,

определяется соответствующее общее или соответствующее контрольное значение (VDBP) области данных сравнения для, по меньшей мере, одной информации (DBI) области данных из, по меньшей мере, одной заданной области данных, и

целостность полезных данных (ND) в соответствующем блоке (DS) данных проверяется в зависимости от, по меньшей мере, одного считанного контрольного значения (DBP) области данных и, по меньшей мере, одного контрольного значения (VDBP) области данных сравнения.

8. Способ по п.6 или 7, в котором

осуществляется просмотр списка (AL) исключений ставших недействительными блоков (DS) данных соответствующей заданной области данных после регистрации соответствующего считанного блока (DS) данных, и

целостность полезных данных (ND) в соответствующем блоке (DS) данных проверяется в зависимости от зарегистрированных в списке (AL) исключений ставших недействительными блоков (DS) данных.

9. Способ по п.8, в котором целостность полезных данных (ND) в соответствующем блоке (DS) данных проверяется в зависимости от занесенных в список (AL) исключений ставших недействительными маркеров (ES) однозначности или в зависимости от, по меньшей мере, одной области значений ставших недействительными маркеров (ES) однозначности, которая занесена в список (AL) исключений.

10. Цифровой тахограф, который выполнен с возможностью

сохранения полезных данных (ND) в, по меньшей мере, одном блоке (DS) данных в, по меньшей мере, одной заданной логической области данных, соответствующего соотнесения с, по меньшей мере, одним блоком (DS) данных кода (DSK) опознавания блока данных, который включает в себя однозначный в соответствующей заданной области данных маркер (ES) однозначности, однозначный код (DBK) опознавания области данных заданной области данных, в которой сохранен соответствующий

блок (DS) данных, и логическую позицию (POS) соответствующего блока (DS) данных внутри соответствующей заданной области данных, и сохранения кода (DSK) опознавания блока данных,

определения контрольного значения (DSP) блока данных для полезных данных (ND) и соответственно относящегося кода (DSK) опознавания блока данных соответствующего блока (DS) данных и сохранения контрольного значения (DSP) блока данных,

соотнесения с соответствующей заданной областью данных информации (DBI) области данных, которая включает в себя код (DBK) опознавания области данных из соответствующей заданной области данных и информацию о, по меньшей мере, одной области значений маркеров (ES) однозначности блоков (DS) данных, сохраненных в текущий момент в соответствующей заданной области данных, и защищенного или безопасного сохранения соответствующей информации (DBI) области данных.

11. Цифровой тахограф, который выполнен с возможностью

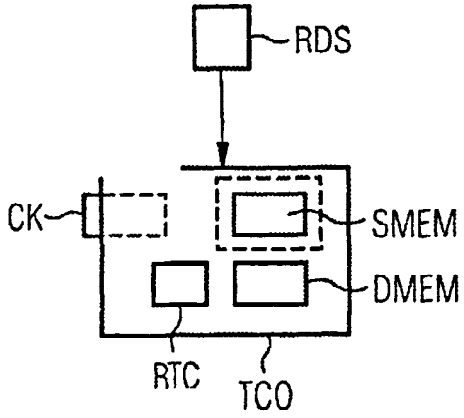
считывания полезных данных (ND), по меньшей мере, одного блока (DS) данных, которые сохранены в, по меньшей мере, одной заданной логической области данных,

считывания соотнесенного с, по меньшей мере, одним блоком (DS) данных кода (DSK) опознавания блока данных, который содержит маркер (ES) однозначности, однозначный в соответствующей заданной области данных, однозначный код (DBK) опознавания области данных заданной области данных, в которой сохранен соответствующий блок (DS) данных, и логическую позицию (POS) соответствующего блока (DS) данных внутри соответствующей заданной области данных,

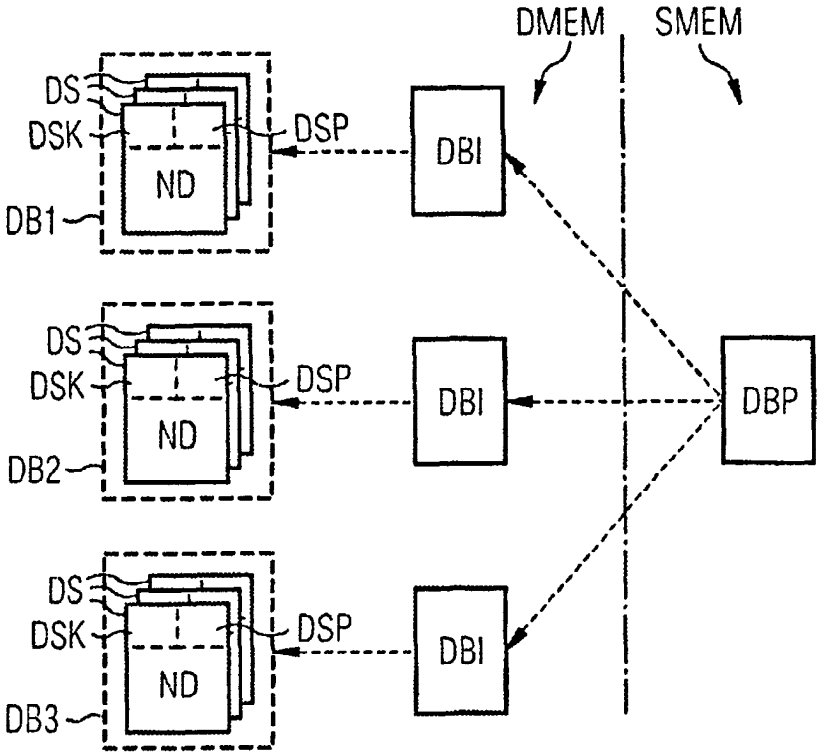
считывания контрольного значения (DSP) блока данных, которое сохранено для полезных данных (ND) и соотнесенного кода (DSK) опознавания блока данных соответствующего блока (DS) данных, и определения соответствующего контрольного значения (VDSP) блока данных сравнения,

считывания информации (DBI) области данных, соотнесенной с соответствующей заданной областью данных, которая включает в себя код (DBK) опознавания области данных из соответствующей заданной области данных и информацию для, по меньшей мере, одной области значений маркеров (ES) однозначности блоков (DS) данных, сохраненных в текущий момент в соответствующей заданной области данных, и

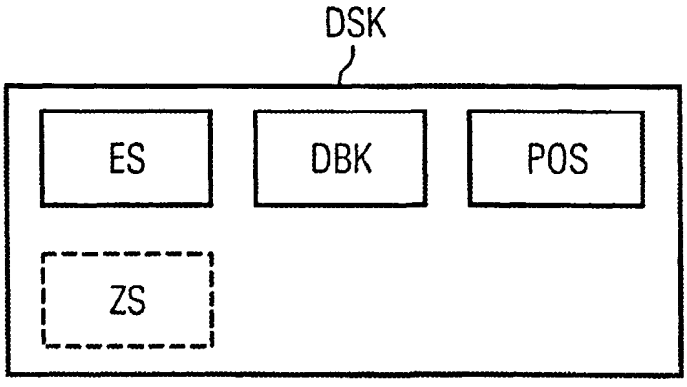
проверки целостности полезных данных (ND) соответствующего считанного блока (DS) данных в зависимости от соответствующего кода (DSK) опознавания блока данных, соответствующего контрольного значения (DSP) блока данных, соответствующего контрольного значения (VDSP) блока данных сравнения и соотнесенной информации (DBI) области данных.



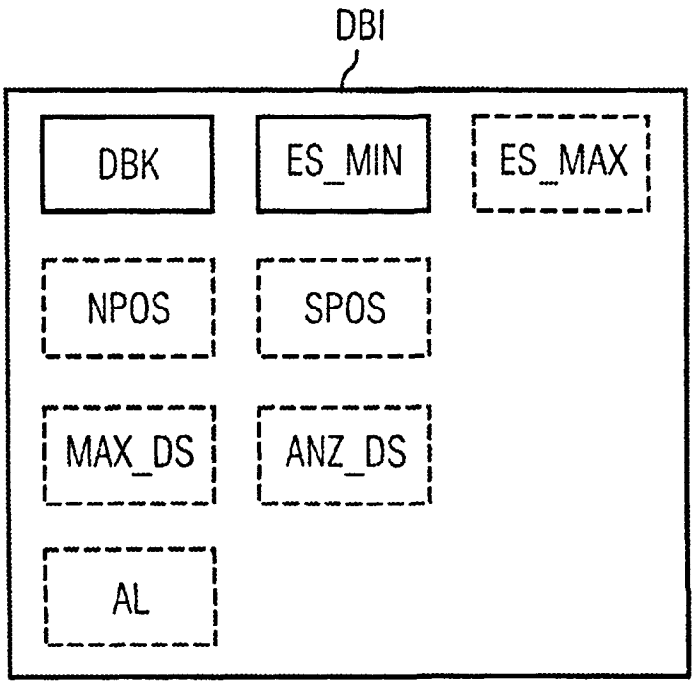
ФИГ.1



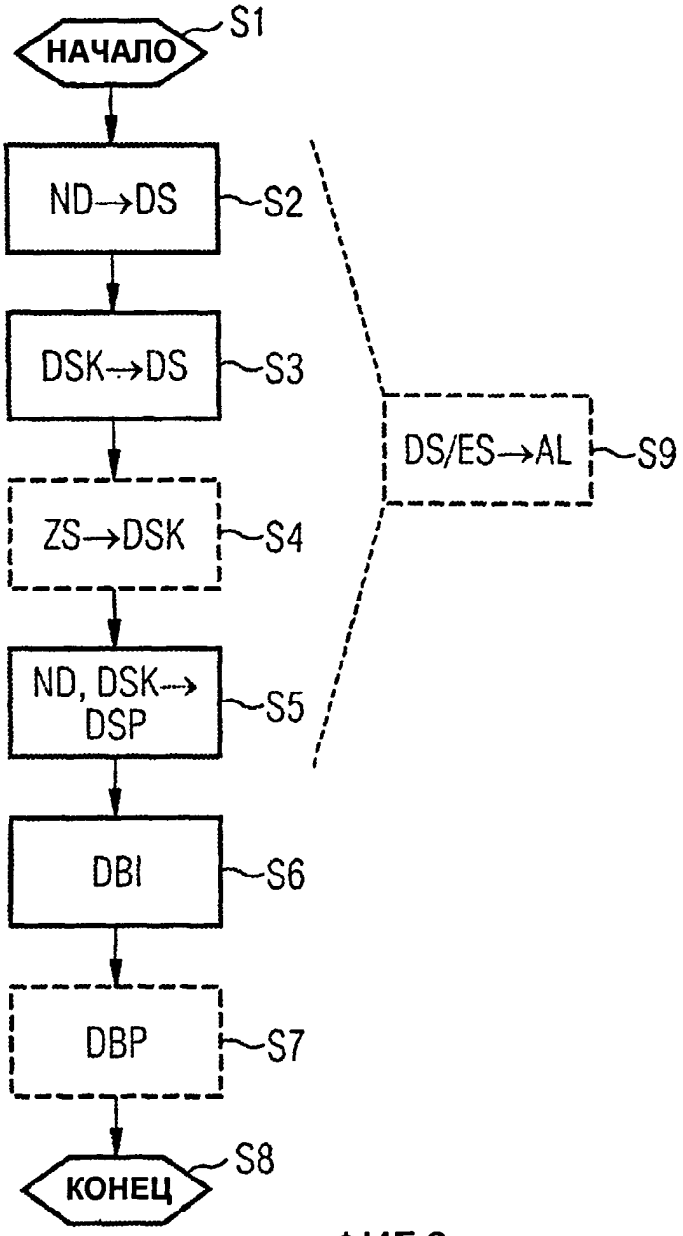
ФИГ.3



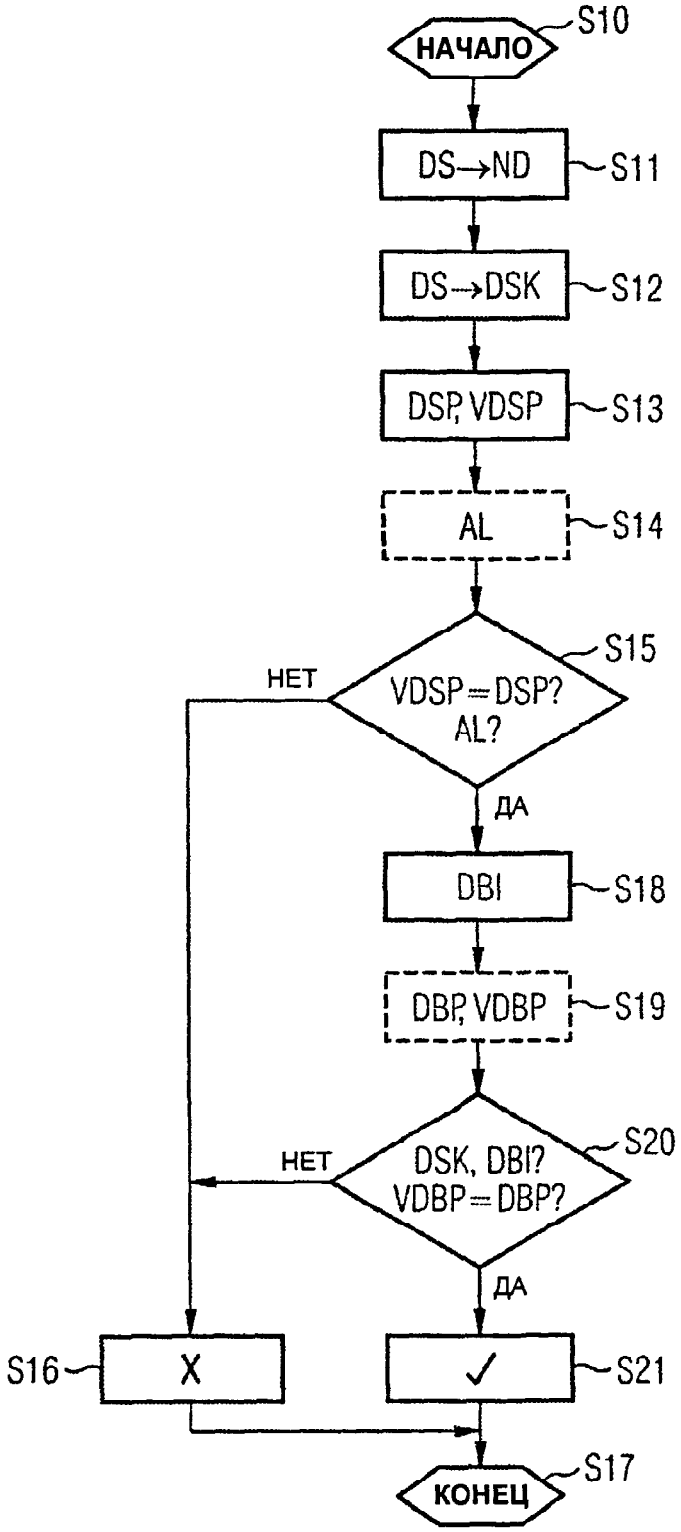
ФИГ.4



ФИГ.5


НАЧАЛО
S1
ND→DS
S2
DSK→DS
S3
ZS→DSK
S4
ND, DSK→ DSP
S5
DBI
S6
DBP
S7
КОНЕЦ
S8
DS/ES→AL
S9

ФИГ.6


НАЧАЛО
S10
DS→ND
S11
DS→DSK
S12
DSP, VDSP
S13
AL
S14
VDSP=DSP?
AL?
S15
НЕТ
ДА
DBI
S18
DBP, VDBP
S19
DSK, DBI?
VDBP=DBP?
S20
НЕТ
ДА
S16
X
✓
S21
КОНЕЦ
S17

ФИГ.7