

Изобретение относится к системе передачи данных с, по меньшей мере, одним терминалом и, по меньшей мере, одним переносным носителем данных, который снабжен энергонезависимым (не теряющим информацию) полупроводниковым накопителем, который содержит, по меньшей мере, первую область значений, действующую в качестве счетчика и представляющую списываемое со счета денежное значение, а также к способу перезагрузки области значений переносного носителя данных.

Такой переносной носитель данных является, например, обычной сегодня микросхемной карточкой, которая используется, например, в качестве телефонной карточки. В этом случае стационарный терминал является пригодным для работы с карточками телефонных аппаратов. Такие микросхемные карточки, выполненные в виде простых накопительных карточек, содержат энергонезависимый полупроводниковый накопитель, например, EEPROM, который служит в основном в качестве счетчика заранее оплаченных и подлежащих списанию со счета телефонных единиц. EEPROM может быть при этом включен согласно EP-B 0321727 или, соответственно, US-A-5001332 так, что он работает как многоступенчатый подобный счетам счетчик. Значение карточки и, тем самым, емкость счетчика устанавливается путем записи и, тем самым, блокирования областей счетчика, которые больше не должны быть разрешенными. Перед этой установкой счетчик всегда имеет максимальную емкость. Сегодня обычные телефонные карточки могут использоваться только однократно и после использования выбрасываются. Такие микросхемные карточки называют электронными кошельками. Применяемые для этой цели микросхемные карточки целесообразны только тогда, когда они могут быть перезаряжены, то есть если их содержимое может быть снова увеличено, после того как известная сумма была списана. Это увеличение значения состояния счетчика происходит на специальных загрузочных терминалах, на которых пользователь или путем оплаты наличными, посредством кредитной карточки, или указания номера счета может занести желаемую сумму на свою карточку. При перезагрузке счетчика микросхемной карточки вследствие конструкции EEPROM может требоваться вначале стереть большую область счетчика или весь счетчик, это означает, что временно устанавливается слишком высокая емкость счетчика. Только затем новое значение состояния счетчика может быть установлено посредством нового ограничения емкости счетчика за счет операций программирования.

Если бы пользователь во время между стиранием значения счетчика и новым программированием вынул карточку из терминала, то он получил бы записанной слишком высокую сумму, за счет чего становится возможной манипуляция для злоупотребления. Кроме того, возможно, что пользователь манипулирует обменом данных между терминалом и карточкой так, что таким образом также может быть занесена слишком высокая сумма.

Манипуляции данных на пути передачи можно воспрепятствовать посредством так называемой электронной подписи. Подлежащие передаче данные могут, кроме того, кодироваться посредством секретного кода и могут декодироваться только определенным, однозначно придаваемым в соответствии отправителю данных, кодом, за счет чего отправитель является однозначно идентифицируемым и данные не могут манипулироваться, так как ключ кодирования является секретным. Для такого кодирования и декодирования требуется дорогой и очень быстрый вычислительный блок, что возможно только с дорогими микропроцессорами, которые, например, используются в уже известных криптокарточках.

В качестве прототипа предлагаемого изобретения принята система передачи данных, которая состоит из, по меньшей мере, одного терминала и, по меньшей мере, одного переносного носителя данных, который снабжен энергонезависимым полупроводниковым накопителем, который содержит, по меньшей мере, первую служащую в качестве счетчика, представляющую списываемое денежное значение, область значений (EP 0 398 545 A1, МПК⁶ G07F7/08, 1990 г.).

За прототип предлагаемого способа принят также способ перезагрузки переносного носителя данных посредством терминала системы передачи данных, при котором осуществляют считывание терминалом, по меньшей мере, одной области значений энергонезависимого полупроводникового накопителя (EP 0 398 545 A1, МПК⁶ G07F7/08, 1990 г.).

EP 0 398 545 A1 описывает способ и устройство для запоминания данных в энергонезависимом полупроводниковом накопителе, который имеет, по меньшей мере, две области, в которые попеременно записывают следующие друг за другом данные. При этом каждая область может характеризоваться путем энергонезависимой установки флажка как действующий к определенному моменту времени, - например, моменту включения - накопитель. Так как каждому накопителю поставлен в соответствии собственный флажок, который может принимать два состояния, может, однако, случиться, что оба флажка принимают то же самое состояние. Поэтому в известном изобретении необходимо определять действительно действующее состояние путем "арбитражной" логики.

В "нормальном случае" режима запоминания в известном устройстве оба флажка к определенному моменту времени всегда занимают то же самое установленное состояние, конечно, флажок, который не был установлен в последнее время, устанавливается в исходное состояние. Это означает, что всегда необходима операция записи и стирания, что требует дополнительного времени. Кроме того, после списания определенной суммы известная схема (или микросхемная карточка) не подлежит перезагрузке. Помимо этого, ее конструктивное исполнение практически не защищено от недобросовестных манипуляций на пути обмена данных между терминалом и карточкой.

Недостаток известного способа заключается в невозможности повышения емкости переносного носителя данных после списания известной суммы, а также осуществления надежной защиты устройства от злоупотреблений со стороны пользователя.

В основу изобретения поставлена задача обеспечения возможности перезагрузки после списания известной суммы и предохранения от злоупотреблений системы передачи данных с терминалом и

переносным носителем данных путем оснащения энергонезависимого полупроводникового накопителя второй областью значений, соединения первой и второй области значений с энергонезависимым флаговым накопителем, принимающим два состояния, каждое из которых соответствует одной из областей значений, в результате чего при введении карточки в терминал и приложении рабочего напряжения только одна из обеих областей значений становится энергонезависимо активируемой при временно активированной второй области значений, которая в случае отключения рабочего напряжения или при новом начале процесса загрузки становится деактивированной и может снова временно активироваться, что при попытке удаления карточки из терминала недобросовестным пользователем и последующем ее использовании вызывает ситуацию, при которой энергонезависимо активируемая область значений будет активироваться и далее при деактивировании в этот момент временно активированной области значений.

В основу изобретения поставлена также задача повышения степени защиты от недобросовестных манипуляций на пути обмена данными между терминалом и переносным носителем данных и повышения эффективности использования способа перезагрузки переносного носителя данных посредством терминала путем считывания терминалом старого значения состояния счетчика областей значений из переносного носителя данных, вычисления нового значения состояния счетчика и передачи его от терминала к переносному носителю данных, записи нового значения состояния счетчика в энергонезависимо разрешаемую область значений энергонезависимого полупроводникового накопителя и приведения области значений с новым значением состояния счетчика в энергонезависимо разрешаемую, в результате чего при введении карточки в терминал и приложении рабочего напряжения только одна из обеих областей значений становится энергонезависимо активируемой при временно активированной второй области значений, которая в случае отключения рабочего напряжения или при новом начале процесса загрузки становится деактивированной и может снова временно активироваться, что при попытке удаления карточки из терминала недобросовестным пользователем и последующем ее использовании вызывает ситуацию, при которой деактивировании в этот момент временно активированной области значений.

Поставленная задача достигается за счет того, что в системе передачи данных с терминалом и переносным носителем данных, которая состоит из, по меньшей мере, одного терминала и, по меньшей мере, одного переносного носителя данных, снабженного энергонезависимым полупроводниковым накопителем, который содержит, по меньшей мере, первую служащую в качестве счетчика, представляющую списываемое денежное значение, область значений, согласно изобретению, энергонезависимый полупроводниковый накопитель содержит вторую, служащую в качестве счетчика, область значений, первая и вторая области значений энергонезависимого накопителя через логическую схему выбора соединены с энергонезависимым флаговым накопителем, включенным с возможностью принятия только двух состояний, одно из которых соответствует той из обеих областей значений, которая является энергонезависимо разрешаемой для считывания или счета, но заперта относительно загрузки, а другое соответствует другой области значений, которая является временно разрешаемой для загрузки только энергонезависимо при активировании в определенный момент времени только одной из областей значений.

Логическая схема выбора выполнена управляемой сигналом управления загрузкой, который обуславливает временное активирование неэнергонезависимо разрешаемой первой или второй области значений и временное деактивирование энергонезависимо разрешаемой первой или второй области значений, причем логическая схема выбора и энергонезависимый полупроводниковый накопитель связаны посредством переключающего устройства, включенного с возможностью соединения программирующей логической схемы и верифицирующей логической схемы с соответственно активной первой или второй областью значений в зависимости от, по меньшей мере, одного выходного сигнала логической схемы выбора.

В предлагаемой системе передачи данных носитель данных содержит первое разрешающее устройство, включенное с возможностью формирования сигнала управления загрузкой только после удостоверения подлинности терминала, а энергонезависимый флаговый накопитель выполнен управляемым от сигнала программирования, вызывающего преобразование временно разрешаемой первой или второй области значений в энергонезависимо разрешаемую первую или вторую область значений.

Кроме того, носитель данных содержит второе разрешающее устройство, включенное с возможностью формирования сигнала программирования только после удостоверения подлинности терминала.

Энергонезависимый полупроводниковый накопитель содержит служащую в качестве энергонезависимого счетного устройства область разрешения, подключенную с возможностью энергонезависимой регистрации каждой попытки для получения разрешения и различия последующих процедур разрешения.

Поставленная задача достигается также за счет того, что в способе перезагрузки переносного носителя данных посредством терминала системы передачи данных, при котором терминалом осуществляют считывание значения состояния, по меньшей мере, одной области значений энергонезависимого полупроводникового накопителя, согласно изобретению, осуществляют считывание старого значения состояния счетчика энергонезависимо разрешаемой первой или второй области значений из переносного носителя данных посредством терминала, вычисление нового значения состояния счетчика из старого значения состояния счетчика и заданных в терминал, подлежащих занесению данных в терминал, передачу нового значения состояния счетчика от терминала к переносному носителю данных, запись нового значения состояния счетчика в активированную сигналом управления загрузкой только энергонезависимо разрешаемую первую или вторую область значений

энергонезависимого полупроводникового накопителя, изменение состояния флагового накопителя до состояния, при котором первая или вторая область значений с новым значением состояния счетчика становится разрешаемой энергонезависимо.

После записи нового значения состояния счетчика в активированную сигналом управления загрузкой только энергозависимо разрешаемую первую или вторую области значений энергонезависимого полупроводникового накопителя, осуществляют формирование подписи нового значения состояния счетчика в переносном носителе данных и передачу подписи к терминалу, определение подписи нового значения состояния счетчика в терминале и сравнение обеих подписей, причем изменение состояния флагового накопителя до состояния, при котором первая или вторая область значений с новым значением состояния счетчика становится разрешаемой энергонезависимо, производят только после совпадения обеих подписей, и при их несовпадении процесс прерывают.

После считывания старого значения состояния счетчика энергонезависимо разрешаемой первой или второй области значений из переносного носителя данных посредством терминала осуществляют считывание специфичных для переносного носителя данных из переносного носителя данных посредством терминала, формирование запроса и определение ответа из запроса и, по меньшей мере, части специфичных данных и старого значения состояния счетчика в терминале, передачу запроса и ответа от терминала к переносному носителю данных, определение ответа из запроса в переносном носителе данных и сравнение обоих ответов.

Кроме того, после шага записи нового значения состояния счетчика в активированную сигналом управления загрузкой только энергозависимо разрешаемую первую или вторую области значений энергонезависимого полупроводникового накопителя, или определения подписи нового значения состояния счетчика в терминале и сравнения обеих подписей, осуществляют считывание специфичных для переносного носителя данных из переносного носителя данных посредством терминала, создание запроса и определение ответа из запроса и, по меньшей мере, части специфичных данных и старого значения состояния счетчика в терминале, передачу запроса и ответа от терминала к переносному носителю данных, определение ответа из запроса в переносном носителе данных и сравнение обоих ответов, причем только при совпадении обоих ответов изменяют состояние флагового накопителя до состояния, при котором первая или вторая область значений с новым состоянием значения счетчика становится разрешаемой энергонезависимо, и при их несовпадении способ прерывают.

В предлагаемом способе для формирования подписи значения состояния счетчика или для создания ответа применяют изменяющееся с каждой операцией загрузки значения, причем формирование подписи или ответа производят посредством генератора псевдослучайных чисел.

При этом применяют значение, которое отображает состояние загрузочного счетчика, установленного с возможностью счета каждой операции загрузки, либо отображает состояние регистра подписи, в который записывают подпись старого значения энергонезависимо разрешаемой первой или второй области значений.

В способе также применяют значение, которое отображает состояние регистра подписи, в который в качестве подписи значения состояния счетчика посредством генератора псевдослучайных чисел при каждой новой операции загрузки записывают новое значение, причем перед каждым вычислением ответа загрузки записывают новое значение, причем перед каждым вычислением ответа изменяют энергонезависимо значение состояния счетчика ответов и используют его в качестве изменяющегося значения.

Т.о., согласно предлагаемому изобретению, в энергонезависимом полупроводниковом накопителе содержится вторая область значений, причем только одна из обеих областей значений является активируемой энергонезависимо, а соответственно вторая область значений может активироваться только временно.

Активируемая энергонезависимо область означает, что информация, которая из обеих областей значений была определена последней как область значений, с которой можно производить списывание, остается сохраненной также после отключения рабочего напряжения или при прерывании процесса загрузки. Это означает, что только временно активированная область значений после отключения рабочего напряжения или при прерывании процесса загрузки и повторном включении рабочего напряжения или при новом начале процесса загрузки является снова деактивированной и должна еще раз временно активироваться. Только после успешного и корректной перезагрузки микросхемной карточки, то есть после корректного ограничения емкости счетчика только временно активированной области значений соответственно сумме из остаточного значения и заданного в терминале подлежащего занесению значения, только временно активированная область значений включается как энергонезависимо активируемая, за счет чего ранее энергонезависимо активированная область значений деактивируется и для новой операции загрузки вначале может активироваться только временно.

Таким образом, если мошенник попытается бы в процессе загрузки только временно активированной области значений после стирания значения счетчика и перед новым ограничением емкости счетчика в соответствии с подлежащим заданию значением удалить карточку из терминала, то при следующем использовании, то есть при следующем приложении рабочего напряжения, энергонезависимо активируемая область значений и далее активировалась бы, а только временно активированная область значений была бы деактивирована.

В предпочтительном усовершенствованном варианте изобретения области значений энергонезависимого накопителя через логическую схему выбора соединены с энергонезависимым флаговым накопителем, состояние которого определяет энергонезависимо активированную область

значений. При отключении рабочего напряжения состояние энергонезависимого флагового накопителя сохраняется, причем определенное состояние всегда придано в соответствие одной и той же области значений.

Для временного активирования другой области значений согласно изобретению на логическую схему выбора подаётся сигнал управления загрузкой. Этот сигнал управления загрузкой имеет в своем нейтральном состоянии, то есть состоянии после приложения рабочего напряжения, например, уровень логического нуля "0" и для временного активирования вновь заряжаемой области значений переключается соответственно на уровень "1".

Выходной сигнал или выходные сигналы управляют переключающим устройством, которое соединяет области значений с программирующей логической схемой и верифицирующей логической схемой. Область значений активируется таким образом только за счет того, что она соединяется с программирующей логической схемой и верифицирующей логической схемой.

Изобретение описывается ниже более подробно на примере выполнения с помощью одной фигуры. При этом фигура показывает в схематической форме загрузочный терминал, а также введенный в него переносной носитель записи. Существенные для изобретения схемы обеих частей системы передачи данных представлены в виде блок-схемы.

Переносной носитель данных, в дальнейшем называемый карточкой, причем возможными являются также другие виды выполнения, введен на фигуру в загрузочный терминал системы передачи данных. Карточка содержит энергонезависимый полупроводниковый накопитель NVM, который предпочтительным образом может быть реализован в виде EEPROM. Этот накопитель NVM разделен при этом на несколько областей, две из которых служат в качестве областей значений WBA, WBB. Эти области значений WBA, WBB выполнены предпочтительным образом в виде многоступенчатых счетчиков и, например, подключены согласно EP-B 0321727 или, соответственно, US-A 5001332. Такие счетчики являются вычитающими счетчиками, если они в стертом или загруженном состоянии имеют логическое состояние "1" и тем самым максимальную, определенную количеством счетных ступеней и бит на ступень емкость счетчика. Путем записи подходящего количества верхних ступеней или, соответственно, некоторых бит самой нижней из этих верхних ступеней емкость счетчика может быть ограничена, и с этого заданного значения он считает вниз до конечного значения "0".

Области значений WBA, WBB через переключающее устройство SV соединены с программирующей логической схемой PL и верифицирующей логической схемой VL. При этом программирующая логическая схема PL и верифицирующая логическая схема VL являются составными частями устройства управления ST. Внутри устройства управления ST соединительные линии частей схемы представлены штриховыми линиями, чем должно быть показано, что соответствующие соединительные линии к устройству управления ST внутри устройства управления ST могут быть соединены также с другими не представленными частями устройства управления ST.

Программирующая логическая схема PL служит для программирования или, соответственно, записи областей значений WBA, WBB, а верифицирующая логическая схема VL для верификации или, соответственно, проверки записанных областей, правильно ли они записаны. Предпочтительным образом верифицирующая логическая схема VL служит также для создания электронной подписи значащего состояния.

Переключающее устройство SV управляется логической схемой выбора AL так, что только одна из областей значений WBA, WBB соединена с программирующей логической схемой PL и верифицирующей логической схемой VL и таким образом является активированной. Логическая схема выбора AL со своей стороны управляется флаговым накопителем FS и через сигнал управления зарядом LAD устройством управления ST. Логическая схема выбора AL, например, может быть образована логической схемой "исключающее ИЛИ" (EXOR) с одним неинвертирующим и одним инвертирующим выходом. Флаговый накопитель FS является энергонезависимым накопителем и управляется сигналом PROG от устройства управления ST. Флаговый накопитель FS может принимать два состояния, причем каждое из этих состояний придано в соответствие одной области значений WBA, WBB. Так как состояние флагового накопителя FS запомнено энергонезависимо, при приложении рабочего напряжения к карте, то есть, например, за счет введения карточки в терминал, активируется соответствующая запомненному состоянию область значений WBA или соответственно WBB. Сигнал управления загрузкой LAD для этого принимает при приложении рабочего напряжения определенное состояние. Только после изменения значения состояния сигнала управления загрузкой LAD посредством переключающего устройства SV, которое управляется соответственно логической схемой выбора AL, временно активируется другая область значений WBB или соответственно WBA, а активированная до сих пор область значений WBA или, соответственно, WBB деактивируется. Временно потому, что значение состояния сигнала управления загрузкой является энергозависимым (теряющим информацию) и при отключении рабочего напряжения, что, например, происходит при удалении карточки из загрузочного терминала, снова принимает свое определенное неактивное состояние так, что после любого отключения рабочего напряжения или после каждого прерывания процесса загрузки снова является активируемой или, соответственно, активирована область значений, определенная флаговым накопителем FS.

За счет сигнала программирования PROG от устройства управления ST к флаговому накопителю FS может быть произведено энергонезависимо изменение состояния флагового накопителя и тем самым смена активированной или, соответственно, активируемой области значений.

Энергонезависимый накопитель NVM содержит в качестве дальнейших областей накопитель значения подписи SIDSP, который поясняется позднее, загрузочный счетчик LZ, которым могут считаться операции загрузки, область KSD, в которой запомнены специфичные для карточки данные, и область GC, в которой запомнен секретный код.

В устройстве управления ST, кроме того, содержится генератор PZG псевдослучайных чисел, который находится в функциональном соединении с верифицирующей логической схемой VI и, кроме того, соединен с регистром подписи SIGSP, загрузочным счетчиком LZ, областью KSD и областью секретного кода GC энергонезависимого накопителя NVM. Этот генератор PZG псевдослучайных чисел предпочтительным образом выполнен согласно EP-A 0616429.

Также в загрузочном терминале содержится устройство управления STT, которое также содержит верифицирующую логическую схему VLT и генератор PZGT псевдослучайных чисел, причем оба генератора PZG псевдослучайных чисел и PZGT должны быть идентичными, если карточка и терминал являются подлинными. Устройство управления ST карточки и устройство управления STT терминала находятся в соединении друг с другом через линии LT1, LT2, чтобы иметь возможность обмениваться данными.

К началу процесса загрузки терминал считывает специфичные для карточки данные, актуальное состояние активированной и тем самым списываемой области значений WBA или, соответственно, WBB, а также значение состояния загрузочного счетчика LZ и значение регистра подписи SIGSP. Из специфичных для карточки данных подлинный терминал может, например, посредством таблицы определить секретный код карточки. Эти данные, а также другое случайное число, так называемый запрос (Challenge) вводятся в терминале в генератор PZGT псевдослучайных чисел, который вычисляет ответ (Response). Как запрос, так и ответ передают после этого на карточку. Там, также на основе данных, вычисляется ответ и сравнивается посредством компаратора, который также содержится в устройстве управления ST, с ответом, переданным от терминала. При совпадении терминал удостоверяется как подлинный, так как он, во первых, был в состоянии определить правильный секретный код и, кроме того, имеет правильный генератор PZGT псевдослучайных чисел.

Генератор PZG псевдослучайных чисел или, соответственно, PZGT служит также для того, чтобы создавать электронную подпись содержания областей значений WBA, WBB, то есть их значений состояния счетчиков. Так как выходной сигнал генератора псевдослучайных чисел зависит от секретного кода карточки и может быть довычислен только с этим секретным кодом, при совпадении выходных сигналов генератора PZG псевдослучайных чисел или, соответственно, PZGT должен применяться тот же самый секретный код. Таким образом, выходной сигнал генератора псевдослучайных чисел может быть однозначно придан в соответствие определенной карточке, что обозначается как подпись карточки под значением состояния счетчика.

Для того, чтобы путем анализа многих вычислительных операций нельзя было определить конструкцию генератора псевдослучайных чисел и введенные данные, одно или несколько введенных значений являются переменными и изменяются также с каждой вычислительной операцией. Одним из таких значений является значение состояния загрузочного счетчика LZ, которое с каждой новой операцией загрузки и таким образом с каждой новой операцией занесения повышается на единицу или, соответственно, устанавливается в исходное состояние, если емкость счетчика исчерпана.

Другим значением является содержимое накопителя подписи SIGSP. В него вписывается результат предыдущего счета генератора псевдослучайных чисел, которым является подпись предыдущего значения состояния счетчика. Таким образом обеспечивается, что выходной сигнал генератора PZG псевдослучайных чисел повторяется только с пренебрежимо малой вероятностью и таким образом не может быть проанализирован.

В накопителе значения подписи SIGSP в варианте выполнения изобретения в качестве значения подписи операции загрузки через загрузочный терминал при каждой операции загрузки может непосредственно вписываться новое значение.

Соответствующая изобретению операция загрузки протекает простейшим образом так, что после введения карточки в загрузочный терминал, и тем самым после приложения рабочего напряжения, определенная за счет состояния флагового накопителя FS область значений WBA или WBB активирована и считывается терминалом. Путем изменения значения состояния сигнала управления загрузкой LAD другая область значений WBA или WBB временно активируется, а активированная перед этим область временно деактивируется. После этого теперь активированная область значений WBB или WBA стирается, причем ее счетчик принимает слишком большую емкость. После этого в терминале из старого значения состояния счетчика и введенного пользователем в терминал подлежащей зачислению суммы определяется новое значение состояния счетчика и переносится на карточку. Если бы пользователь перед этим удалил карточку из терминала, то он получил бы зачисленной слишком высокую сумму, если бы программирование области значений уже произошло бы окончательно и энергонезависимо. За счет нового введения карточки в терминал согласно изобретения снова активируется та же область значений WBA или WBB со старым значением состояния счетчика, так как состояние флагового накопителя FS еще не было изменено. Только если новое значение состояния счетчика было запрограммировано во временно активированную область значений WBB или WBA, состояние флагового накопителя FS за счет сигнала PROG от устройства управления ST изменяется, за счет чего новая область значений является активируемой энергонезависимо и активируется при каждом новом приложении рабочего напряжения, то есть при каждом введении карточки в терминал, например, чтобы списать деньги.

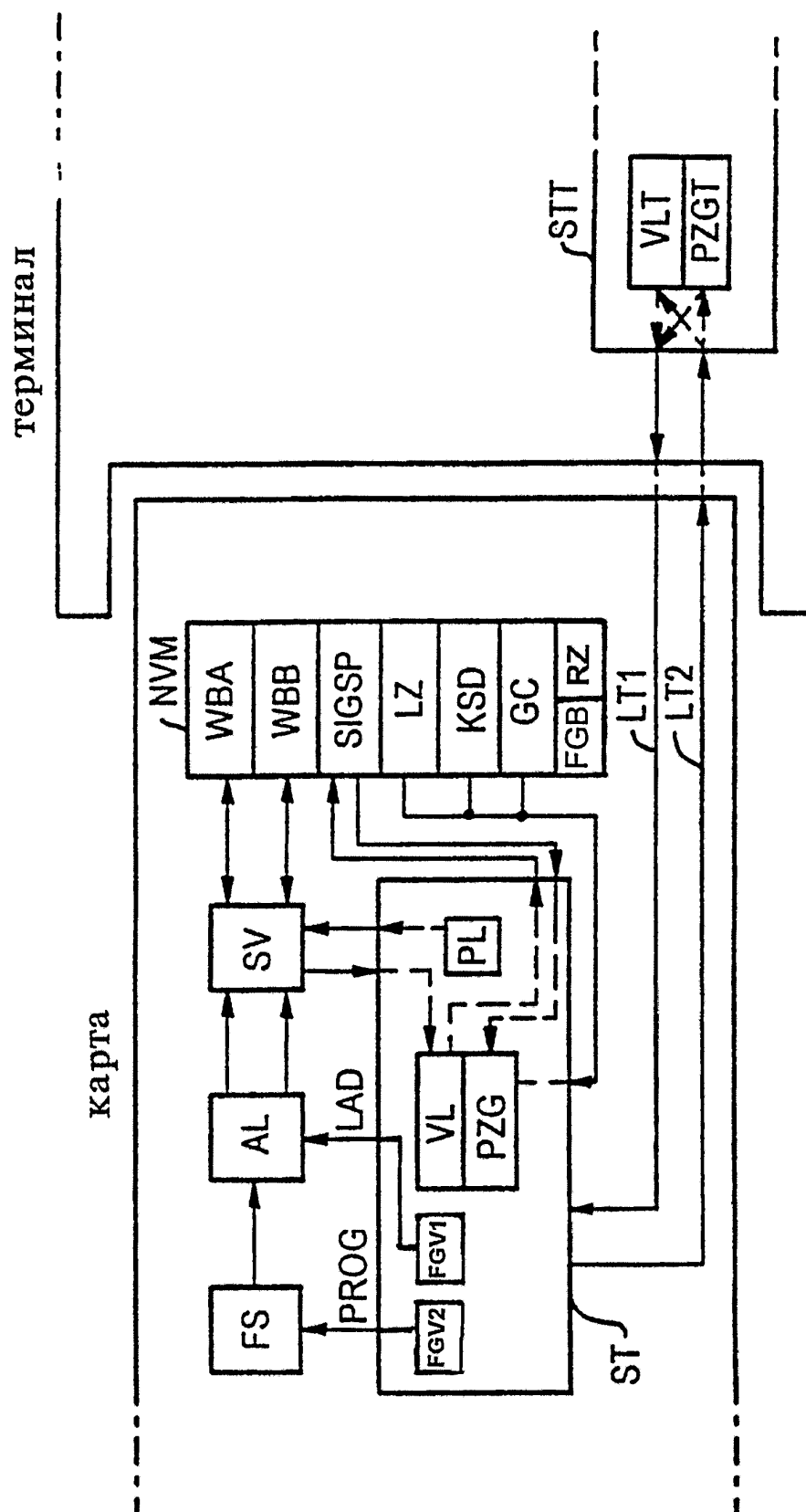
Чтобы исключить манипуляции с новым значением состояния счетчика при передаче от терминала на карточку, в соответствующей изобретению форме дальнейшего усовершенствования способа после передачи нового значения состояния счетчика к карточке там, согласно выше описанному способу, подписывается значение состояния счетчика. Подпись затем передается на терминал и там сравнивается с также определенной подписью. При совпадении обеспечивается, что к карточке было передано правильное значение состояния счетчика. При несовпадении операция загрузки прерывается, таким образом, неправильное значение состояния счетчика не имеет никакого влияния на более поздние операции списывания со счета, так как состояние флагового накопителя FS еще не было изменено. Оно изменяется только после распознавания совпадения подписей и передачи соответствующего сигнала от терминала к карте.

В дальнейшей форме развития соответствующего изобретению способа терминал должен удостоверять свою подлинность по отношению к карточке, прежде чем может начинаться операция загрузки. За счет этого обеспечивается, что никакой фальшивый загрузочный прибор не может быть использован для занесения суммы на карточку. Для этого удостоверения подлинности из считанных терминалом с карты данных и запроса вычисляются ответ, который вместе с запросом передают к карточке и там сравнивают с также определенным посредством запроса и данных карточки ответом. Только при совпадении ответов могут создаваться сигнал управления загрузкой LAD, а также сигнал программирования PROG, и тем самым начинаться операция загрузки. Для этой цели в переносном носителе данных предусмотрены разрешающие устройства FGV1, FGV2, которые подходящим образом управляются от устройства управления ST. Такая операция загрузки стартуется при этом, например, за счет повышения значения состояния загрузочного счетчика LZ или за счет фиктивного (Dummy-) программирующего импульса. Фиктивный (Dummy-) программирующий импульс при этом является программирующим импульсом на недействительный адрес энергонезависимого накопителя NVM, который распознается устройством управления карточки ST как управляющая команда.

Также после старта операции загрузки, после того, как терминал подтвердил свое полномочие и сигнал управления загрузкой LAD создан, обманщик мог бы оказать воздействие на значение состояния счетчика и вызвать программирующий сигнал PROG для энергонезависимого активирования значения состояния счетчика независимо от терминала. В дальнейшей форме усовершенствования соответствующего изобретению способа терминал перед созданием программирующего сигнала PROG должен еще раз доказать свои полномочия, это значит, еще раз удостоверить свою подлинность. Создание ответа при этом соответствует созданию ответа при первой проверке полномочий для старта операции загрузки.

Чтобы помешать повторению ответа, который выдается носителем данных в рамках вычисления подписи и может использоваться для создания программирующего сигнала PROG, для создания ответа соответствующим изобретению способом применяется значение, изменяющееся при каждом вычислении ответа. Это значение поставляется счетчиком ответа RZ, который энергонезависимо изменяют перед каждым вычислением ответа и значение состояния счетчика которого оказывает воздействие на вычисление ответа. Счетчик ответа RZ предпочтительным образом реализован как область энергонезависимого накопителя.

За счет соответствующей изобретению системы передачи данных и соответствующего изобретению способа достигается надежная перезагрузка переносного носителя данных, например, микросхемной карточки.



Фиг.