

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2014120112/08, 19.05.2014

(24) Дата начала отсчета срока действия патента:
19.05.2014

Приоритет(ы):

(22) Дата подачи заявки: 19.05.2014

(43) Дата публикации заявки: 27.11.2015 Бюл. № 33

(45) Опубликовано: 10.04.2016 Бюл. № 10

(56) Список документов, цитированных в отчете о
поиске: RU 2486682 C2, 27.06.2013. RU 2319308
C1, 10.03.2008. RU 2296432 C1, 27.03.2007. EP
2124377 A2, 25.11.2009.

Адрес для переписки:

302034, г.Орел, ул. Приборостроительная, 35,
Академия ФСО России, ОНТИ

(72) Автор(ы):

Иванцов Олег Владимирович (RU),
Богринцев Николай Викторович (RU),
Горохов Денис Евгеньевич (RU),
Селихов Игнат Андрианович (RU),
Тарасов Юрий Евгеньевич (RU)

(73) Патентообладатель(и):

Государственное казенное образовательное
учреждение высшего профессионального
образования Академия Федеральной службы
охраны Российской Федерации (Академия
ФСО России) (RU)(54) УСТРОЙСТВО СИНХРОНИЗАЦИИ НА ОСНОВЕ КОМБИНИРОВАННОГО ПРИМЕНЕНИЯ
ДВОЙСТВЕННОГО БАЗИСА ПОЛЯ $GF(2^k)$ И ВЫДЕЛЕНИЯ "СКОЛЬЗЯЩЕГО ОКНА" С
ОШИБКАМИ

(57) Реферат:

Изобретение относится к технике передачи дискретной информации и может быть использовано для синхронизации псевдослучайных последовательностей. Достижимым техническим результатом является снижение вероятности пропуска синхропосылки на канале связи с помехами. Устройство синхронизации на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения скользящего окна с ошибками

содержит первую и вторую одноканальные линии задержки на один бит, пять ключей, управляемый инвертор, блок сравнения, дешифратор, умножитель на [а], счетчик ошибок, счетчик положительных коэффициентов, умножитель обратных элементов, счетчик единиц (m - b), генератор обратных элементов $GF(2^k)$, генератор тактовых импульсов. 1 ил.



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) **ABSTRACT OF INVENTION**

(21)(22) Application: 2014120112/08, 19.05.2014

(24) Effective date for property rights:
19.05.2014

Priority:

(22) Date of filing: 19.05.2014

(43) Application published: 27.11.2015 Bull. № 33

(45) Date of publication: 10.04.2016 Bull. № 10

Mail address:

302034, g.Orel, ul. Priborostroitel'naja, 35, Akademiya
FSO Rossii, ONTI

(72) Inventor(s):

Ivantsov Oleg Vladimirovich (RU),
Bogrintsev Nikolaj Viktorovich (RU),
Gorokhov Denis Evgenevich (RU),
Selikhov Ignat Andrianovich (RU),
Tarasov Jurij Evgenevich (RU)

(73) Proprietor(s):

Gosudarstvennoe kazennoe obrazovatel'noe
uchrezhdenie vysshego professional'nogo
obrazovaniya Akademiya Federalnoj sluzhby
okhrany Rossijskoj Federatsii (Akademiya FSO
Rossii) (RU)(54) **DEVICE SYNCHRONIZATION BASED ON THE COMBINED APPLICATION OF THE DUAL BASIS OF GF (2^k) AND ALLOCATION OF "SLIDING WINDOW" ERRORS**

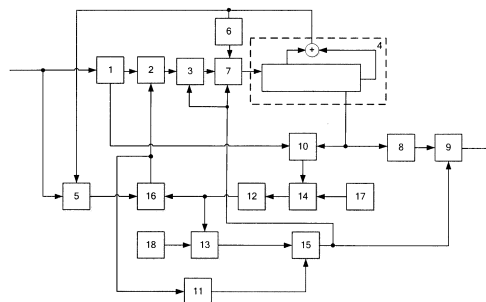
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to digital data transmission and can be used to synchronize pseudorandom sequence. Synchronization apparatus based on combined application of dual basis of GF (2^k) and release of sliding window with errors includes first and second one-channel delay line by one bit, five keys controlled inverter, comparator, descrambler, multiplier for [a], error counter, counter is positive coefficient multiplier inverse elements, counter units (m - b), inverse generator elements GF (2^k), clock generator.

EFFECT: achievable technical result is to reduce probability of missing initialization vector channel due to interference.

1 cl, 1 dwg



- 1 – первая ОЛЗ на один бит;
- 2 – управляемый инвертор;
- 3 – первый ключ;
- 4 – ЛРР с обратными связями на (n-1) бит;
- 5 – блок сравнения;
- 6 – вторая ОЛЗ на один бит;
- 7 – второй ключ;
- 8 – дешифратор;
- 9 – четвертый ключ;
- 10 – умножитель на [a];
- 11 – счетчик ошибок;
- 12 – счетчик положительных коэффициентов;
- 13 – третий ключ;
- 14 – умножитель обратных элементов;
- 15 – счетчик единиц (m-b);
- 16 – пятый ключ;
- 17 – генератор обратных элементов GF (2^k);
- 18 – генератор тактовых частот.

Фиг. 1

Изобретение относится к технике передачи дискретной информации и может быть использовано для синхронизации псевдослучайных последовательностей (ПСП).

В области синхронизации систем передачи данных существует проблема, связанная с устройствами, обеспечивающими синхронизацию в условиях интенсивных помех.

Устройством-аналогом является устройство в авторском свидетельстве СССР №698145, Н04L 7/02, опубликованном в 1979 году.

Недостатком данного аналога является высокая вероятность пропуска синхропосылки при снижении качества канала связи.

Наиболее близким техническим решением является устройство, реализованное на основе патента на изобретение №2486682, опубликованное 27.06.2013 г.

Известное устройство синхронизации рекуррентной последовательностью (РкП) содержит последовательно соединенные первую одноканальную линию задержки на один бит (ОЛЗ), на вход которой поступает входной сигнал, управляемый инвертор, первый ключ, линейный рекуррентный регистр (ЛРР) с обратными связями, блок сравнения, а также второй ключ, выход которого соединен со входом ЛРР с обратными связями. Кроме того, устройство содержит вторую ОЛЗ на один бит, выход которой соединен с первым входом второго ключа, а вход соединен с выходом ЛРР с обратными связями, другой выход которого подключен ко входу дешифратора, при этом на другой вход блока сравнения поступает входной сигнал. Далее по схеме: детектор качества, на вход которого поступает входной сигнал, блок сложения, один из входов которого соединен с выходом детектора качества, а второй вход соединен с выходом блока сравнения, инвертор единиц, вход которого соединен с выходом блока сложения. Далее: счетчик нулей («0») на (m-c) совпадений, вход которого соединен с выходом инвертора единиц, а выход соединен с управляющим входом второго ключа и управляющим входом первого ключа, счетчик нулей («0») на с совпадений, один вход которого соединен с выходом блока сложения, а выход соединен с управляющим входом инвертора единиц, третий ключ, первый вход которого соединен с выходом блока сложения, управляющий вход соединен с выходом счетчика нулей («0») на с совпадений, а выход соединен со вторым входом управляемого инвертора. Кроме того, счетчик ошибок, первый вход которого соединен с выходом блока сложения, второй (управляемый) вход соединен с выходом счетчика нулей («0») на с совпадений, а выход соединен с управляемым входом счетчика нулей («0») на (m-c) совпадений и управляемым входом счетчика нулей («0») на с совпадений, запоминающее устройство выбора количества исправляемых ошибок, выход которого подключен к третьему входу устройства выбора допустимого количества исправляемых ошибок.

Существенным недостатком этого устройства является необходимость дополнительного применения детектора качества канала, сравнительно высокая вероятность пропуска синхропосылки на канале связи с помехами из-за отсутствия механизма, обеспечивающего полный перебор зачетных отрезков ("окон") на РкП и их анализ возможности выделения ложного формирующего кодового вектора (ФКВ), а также сравнительно большое время, затрачиваемое на нахождение ФКВ, зависящего от вида характеристического полинома.

Задачей изобретения является создание «устройства синхронизации рекуррентной последовательностью на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками», снижающего вероятность пропуска синхропосылки на канале связи с помехами, которое позволит сократить время нахождения формирующего кодового вектора при сохранении точности синхронизации независимо от вида применяемого характеристического полинома, без

использования дополнительной информации с детектора качества.

Эта задача решается тем, что «устройство синхронизации рекуррентной последовательностью на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками» содержит последовательно соединенные первую одноканальную линию задержки на один бит (ОЛЗ), на вход которой поступает входной сигнал, управляемый инвертор, первый ключ. Кроме того, устройство содержит линейный рекуррентный регистр (ЛРР) с обратными связями, первый выход которого соединен с первым входом блока сравнения, на второй вход которого поступает входной сигнал, и входом второй ОЛЗ на один бит, а также второй ключ, первый вход которого соединен с выходом второй ОЛЗ на один бит, а выход соединен с входом ЛРР с обратными связями, второй выход которого подключен к входу дешифратора, а также устройство содержит счетчик ошибок и третий ключ. Помимо выше приведенных элементов, согласно изобретению, устройство дополнено: счетчиком единиц ($m-b$), выход которого соединен с управляющими входами первого и второго ключа, а первый вход - с выходом счетчика ошибок, в то время как второй вход соединен с выходом третьего ключа, четвертым ключом, к первому входу которого подключен выход счетчика единиц ($m-b$), а ко второму - выход дешифратора, умножителем на $[\alpha]$, первый вход которого параллельно подключен к выходам ячеек ЛРР с обратными связями ($n-1$) бит и первой ОЛЗ на 1 бит, счетчиком положительных коэффициентов, выход которого соединен с управляющим входом третьего ключа, генератором тактовых частот, выход которого подключен ко второму входу третьего ключа, умножителем обратных элементов, ко второму входу которого подключен выход умножителя на $[\alpha]$, а выход соединен с входом счетчика положительных коэффициентов, генератором обратных элементов $GF(2^k)$, выход которого соединен с первым входом умножителя обратных элементов, пятым ключом, вход которого соединен с выходом блока сравнения, а выход соединен с вторым входом управляющего инвертора и входом счетчика ошибок, управляющий вход пятого ключа соединен с выходом счетчика положительных коэффициентов.

Благодаря новым признакам, «устройство синхронизации рекуррентной последовательности на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками» обеспечивает снижение вероятности ложного выделения или пропуска синхропосылки на каналах связи с помехами с одновременным повышением вероятности правильной синхронизации, а также сокращает время нахождения формирующего кодового вектора за счет комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками без применения детектора качества канала. При этом исключается зависимость от вида применяемого характеристического полинома.

Проведенный анализ уровня техники позволил установить, что аналоги, характеризующиеся совокупностью признаков, тождественных всем признакам заявленного технического решения, отсутствуют, что указывает на соответствие условию патентоспособности «новизна».

Результаты поиска известных решений в данной и смежных областях техники с целью выявления признаков, совпадающих с отличительными от прототипа признаками заявленного объекта, показали, что они не следуют явным образом из уровня техники. Из уровня техники также не выявлена известность влияния предусматриваемых существенными признаками заявленного изобретения преобразований на достижение указанного технического результата. Следовательно, заявленное изобретение

соответствует условию патентоспособности «изобретательский уровень».

На фиг. 1 изображено заявляемое «устройство синхронизации на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками».

Промышленное применение изобретения обусловлено тем, что оно может быть осуществлено с помощью современной элементной базы с достижением указанного в изобретении назначения.

Предложенное «устройство синхронизации на основе комбинированного применения

двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками», содержит последовательно соединенные первую одноканальную линию задержки на один бит (ОЛЗ) (1), на вход которой поступает входной сигнал, управляемый инвертор (2) и первый ключ (3), а также линейный рекуррентный регистр (ЛРР) с обратными связями на (n-1) бит (4), первый выход которого соединен с первым входом блока сравнения (5), на второй вход которого поступает входной сигнал, и входом второй ОЛЗ на один бит (6), а также второй ключ (7), первый вход которого соединен с выходом второй ОЛЗ на один бит (6), а выход соединен со входом ЛРР с обратными связями на (n-1) бит (4), второй выход которого подключен ко входу дешифратора (8), а также устройство содержит счетчик ошибок (11) и третий ключ (13), согласно изобретению устройство дополнено: счетчиком единиц (m-b) (15), выход которого соединен с управляющими входами первого (3) и второго ключа (7), а первый вход - с выходом счетчика ошибок (11), в то время как второй вход соединен с выходом третьего ключа (13), четвертым ключом (9), к первому входу которого подключен выход счетчика единиц (m-b) (15), а ко второму - выход дешифратора (8), умножителем на $[\alpha]$ (10), первый вход которого параллельно подключен к выходам ячеек ЛРР с обратными связями (n-1) бит (4) и первой ОЛЗ на 1 бит (1), счетчиком положительных коэффициентов (12), выход которого соединен с управляющим входом третьего ключа (13), генератором тактовых частот (18), выход которого подключен ко второму входу третьего ключа (13), умножителем обратных элементов (14), ко второму входу которого подключен выход умножителя на $[\alpha]$ (10), а выход соединен с входом счетчика положительных коэффициентов (12), генератором обратных элементов $GF(2^k)$ (17), выход которого соединен с первым входом умножителя обратных элементов (14), пятым ключом (16), вход которого соединен с выходом блока сравнения (5), а выход соединен с вторым входом управляющего инвертора (2) и входом счетчика ошибок (11), управляющий вход пятого ключа (16) соединен с выходом счетчика положительных коэффициентов (12).

Счетчик ошибок работает следующим образом: от каждой приходящей логической «1» продвигает состояние счетчика на шаг вперед, каждый приходящий логический «0» оставляет состояние счетчика в прежнем состоянии. Данный счетчик реализован на ЖК-триггерах.

Каждая из двух одноканальных линий задержки выполнена на одноступенчатом D-триггере. Он реализован на базе двухвходового двунаправленного ключа. При подаче на вход синхронизации С напряжения логического «0» ключ SW1 открывается, обеспечивая прохождение сигнала со входа D на вход Q триггера. При появлении на входе синхронизации С напряжения логической «1» открывается ключ SW2, замыкается цепь обратной связи, что обеспечивает хранение сигнала, записанного в триггер. Закрытый ключ SW1 исключает влияние изменений входных сигналов на состояние триггера.

Управляемый инвертор реализован на стробируемом буферном инверторе, который имеет два входа R - стробирующий и EZ - управляющий. Функция инвертора выполняется при подаче на входы R и Алогического «0».

Четвертый, пятый ключ представляет собой одновходовый двунаправленный ключ, выполненный на МОП транзисторах р-типа, управляемых сигналами, поступающими на вход С ключа.

Счетчики (m-b) «1» и положительных коэффициентов работают следующим образом: от каждой приходящей логической «1» счетчик становится в исходное состояние, а каждый приходящий логический «0» продвигает состояние счетчика на шаг вперед. Данные счетчики реализованы на JK-триггерах.

Устройство выбора допустимого количества исправляемых ошибок реализовано с помощью переключателей и четырехразрядного компаратора, предназначенного для сравнения модулей двух четырехразрядных чисел. К одному сравниваемому входу А подключается счетчик ошибок, а к четырехразрядному входу В переключатели, коммутацией которых обеспечивается выбор допустимого порога ошибок. В случае когда $A=B$ и $A>B$ соответственно на первом и втором выходах компаратора устанавливается напряжение логического «0».

Генератор обратных элементов поля $GF(p^k)$, при каждом сдвиге формирующий очередной элемент поля, выполнен:

- на регистре сдвига, реализованном на JK-триггерах;
- на к ячейках памяти с обратными связями, реализованных на одноступенчатых D-триггерах;
- на сумматорах, реализованных на двухвходовых логических элементах «ИЛИ-НЕ»;
- на умножителях на коэффициенты характеристического многочлена, реализованных на двухвходовых триггерах Шмита.

Умножитель на $[\alpha]$ выполняет функцию генерации коэффициентов α и их умножение на значения ячеек ЛРР. Данное устройство выполнено:

- на регистре сдвига, реализованном на JK-триггерах;
- на к ячейках памяти, реализованных на одноступенчатых D-триггерах;
- на схеме деления на производную $P'(\epsilon)$, реализованной на элементах сложения по mod2;
- на умножителе, реализованном на двухвходовых логических элементах «И-НЕ».

При этом на вход регистра с каждым тактом подаются поочередно коэффициенты многочлена $P(x)$, начиная с коэффициента p_0 по p_{k-1} включительно. До начала подачи коэффициентов p_i на вход регистра его ячейки должны быть установлены в нулевое состояние.

Устройство умножения выполнено на двухвходовых логических элементах "И-НЕ".

Величина счетчика «1», учитывающего b совпадений, выбирается такой, чтобы при минимальном его значении обеспечить контроль за безошибочным заполнением ЛРР на приеме. Для этого размер счетчика b выбирается в пределах $5 \div 40$.

Значение количества исправляемых ошибок на зачетном отрезке (ЗОТ) зависит от расстояния Хемминга d_0 . Так как каждый зачетный отрезок, выделяемый на псевдослучайной последовательности (ПСП) - это укороченный КМД код, обладающий минимальным кодовым расстоянием d_0 , где n - длина кода, а k - длина информационной части кода, то M может выбираться в пределах $0 \leq M \leq (m-c)(d_0-1)/k$ без опасности повышения вероятности ложного фазирования. Это подтверждают эксперименты, проведенные на имитационной модели.

Работа устройства происходит в два этапа. На первом этапе кодовый вектор k на основе применения двойственного базиса поля $GF(2^k)$ должен быть найден за возможно кратчайшее время и с большей вероятностью по сравнению с другими известными определителями M -последовательностей.

Если выделяемые k -элементные участки не содержат ошибок и принадлежат M -последовательности, то с каждым тактом на выходе устройства умножения будет появляться один и тот же результат. Счетчик положительных коэффициентов (на b), работающий как пороговое устройство, по числу одинаковых результатов умножения сигналов с умножителя на $[a]$ и генератора обратных элементов $GF(2^k)$, выделяемых последовательно, позволяет обнаружить искомую M -последовательность.

На втором этапе осуществляется формирование местной ПСП на основе правильного формирующего кодового вектора k и побитное сравнение с рекуррентной последовательностью, которая принимается из канала связи.

Второй этап анализа оставшейся части "скользящего окна" величиной $(m-b)$ необходим для того, чтобы убедиться в неслучайном происхождении небольшого участка $(k+b)$ линейной рекуррентной последовательности (ЛРП). Для этого используется схема определителя ЛРП по выделенному "скользящему окну" с ошибками, который позволяет уменьшить вероятность пропуска (не обнаружения) рекуррентной последовательности на канале связи с помехами.

Возможность обнаружения и исправления ошибок в "скользящем окне" объясняется тем, что "зачетный участок" обладает свойствами $(n; k; d)$ блочного кода.

С помощью замкнутого пятого ключа (16) к анализу поступающей из канала связи РкП подключаются управляемый инвертор (2) и счетчик ошибок (11). Замыкание ключа 3 (13) обеспечивает подключение генератора тактовой частоты (18) к счетчику единиц на $(m-b)$ (15). Если количество ошибок, попавшее в "скользящее окно", не превышает $(d_{\min}-1)$, то они обнаруживаются и исправляются управляемым инвертором (2).

Успешное распознавание ЛРП произойдет в том случае, если за время анализа на вход приемника поступит безошибочный участок рекуррентной последовательности, длина которого не менее $(k+b)$, при условии,

что при дальнейшем анализе $(m-b)$ части "окна" количество ошибок не превысит $(d_{\min}-1)$.

Если до того как счетчик единиц $(m-b)$ (15) достигнет своего порога, на вход устройства поступит больше $(d_{\min}-1)$ ошибочных элементов, то на выходе счетчика ошибок (11) выделится сигнал "1", который установит счетчик единиц на $(m-b)$ (15) в нулевое состояние, и поиск рекуррентной последовательности продолжится вновь.

Экспериментальная проверка характеристик «устройства синхронизации на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками» была выполнена на ЭВМ в среде объектно-ориентированного программирования Borland C ++ Builder 6.

Результаты тестирования показали, что предложенное обеспечивает снижение вероятности пропуска синхропосылки на канале связи с $P_{\text{ош}}=10^{-2}$ на 20% за счет безошибочного выделения и уменьшения размера формирующего кодового вектора, что соответствует достижению заявленных результатов.

Формула изобретения

Устройство синхронизации на основе комбинированного применения двойственного

базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками, подключенное к
 выходу канала связи и содержащее последовательно соединенные первую
 одноканальную линию задержки на один бит (ОЛЗ), на вход которой поступает сигнал
 из канала связи, управляемый инвертор и первый ключ, а также линейный рекуррентный
 5 регистр (ЛРР) с обратными связями на $(n-1)$ бит, первый выход которого соединен с
 первым входом блока сравнения, на второй вход которого поступает входной сигнал
 из канала связи, и входом второй ОЛЗ на один бит, а также второй ключ, первый вход
 которого соединен с выходом второй ОЛЗ на один бит, а выход соединен с входом
 10 ЛРР с обратными связями на $(n-1)$ бит, второй выход которого подключен к входу
 дешифратора, счетчик ошибок и третий ключ, согласно изобретению дополнено:
 счетчиком единиц $(m-b)$, выход которого соединен с управляющими входами первого
 и второго ключа, а первый вход с выходом счетчика ошибок, в то время как второй
 вход соединен с выходом третьего ключа, четвертым ключом, к первому входу которого
 15 подключен выход счетчика единиц $(m-b)$, а ко второму - выход дешифратора,
 умножителем на $[\alpha]$, первый вход которого параллельно подключен к выходам ячеек
 ЛРР с обратными связями $(n-1)$ бит и первой ОЛЗ на 1 бит, счетчиком положительных
 коэффициентов, выход которого соединен с управляющим входом третьего ключа,
 генератором тактовых частот, выход которого подключен ко второму входу третьего
 20 ключа, умножителем обратных элементов, ко второму входу которого подключен
 выход умножителя на $[\alpha]$, а выход соединен с входом счетчика положительных
 коэффициентов, генератором обратных элементов $GF(2^k)$, выход которого соединен с
 первым входом умножителя обратных элементов, пятым ключом, вход которого
 соединен с выходом блока сравнения, а выход соединен с вторым входом управляющего
 25 инвертора и входом счетчика ошибок, управляющий вход пятого ключа соединен с
 выходом счетчика положительных коэффициентов.

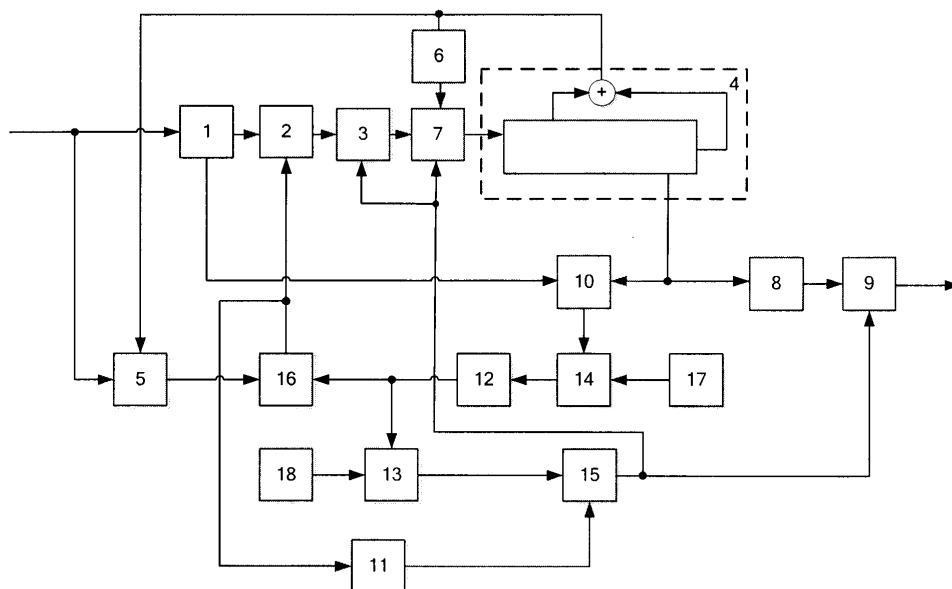
30

35

40

45

Устройство синхронизации на основе комбинированного применения двойственного базиса поля $GF(2^k)$ и выделения "скользящего окна" с ошибками



Фиг. 1

- 1 – первая ОЛЗ на один бит;
- 2 – управляемый инвертор;
- 3 – первый ключ;
- 4 – ЛРР с обратными связями на $(n-1)$ бит;
- 5 – блок сравнения;
- 6 – вторая ОЛЗ на один бит;
- 7 – второй ключ;
- 8 – дешифратор;
- 9 – четвертый ключ;
- 10 – умножитель на $[a]$;
- 11 – счетчик ошибок;
- 12 – счетчик положительных коэффициентов;
- 13 – третий ключ;
- 14 – умножитель обратных элементов;
- 15 – счетчик единиц $(m-b)$;
- 16 – пятый ключ;
- 17 – генератор обратных элементов $GF(2^k)$;
- 18 – генератор тактовых частот.