Селекторы цифровых команд. Часть 4

Геннадий ШИШКИН, д. т. н.
Дмитрий НИКОЛАЕВ, к. т. н.

В статье представлены возможные способы построения селекторов цифровых команд с защитой от быстрой блокировки.

Анализ базовых вариантов СК [1] показывает, что наилучшей совокупностью характеристик по простоте схемной реализации, объему массива исчерпывающего перебора входных кодов для несанкционированного включения и простоте санкционированного включения после попыток подбора кода обладает СК с блокировкой включения после L допустимых попыток подбора кода. При этом вероятность несанкционированного включения селектора с первой попытки подбора кода $P_1^Б = 1/2^n$, где n — количество разрядов кода включения, а объем массива исчерпывающего перебора кодов $M = N^2–N+1$, где $N = 2^n$.

Недостатком данного варианта СК является возможность временного вывода его из строя путем быстрой блокировки при неоднократной подаче на его вход кода, не соответствующего эталонному значению. При этом время потери работоспособности неприемлемо возрастает, когда по условиям эксплуатации легальному оператору неизвестен код разблокировки или требуется выяснение причин ускоренной блокировки и разработка мер по ее последующему недопущению.

Простейшим способом защиты СК от быстрой блокировки считается уменьшение количества фиксируемых ошибок набора кода включения путем фиксации только тех ошибочных входных кодов, часть разрядов которых совпала с эталонным значением.

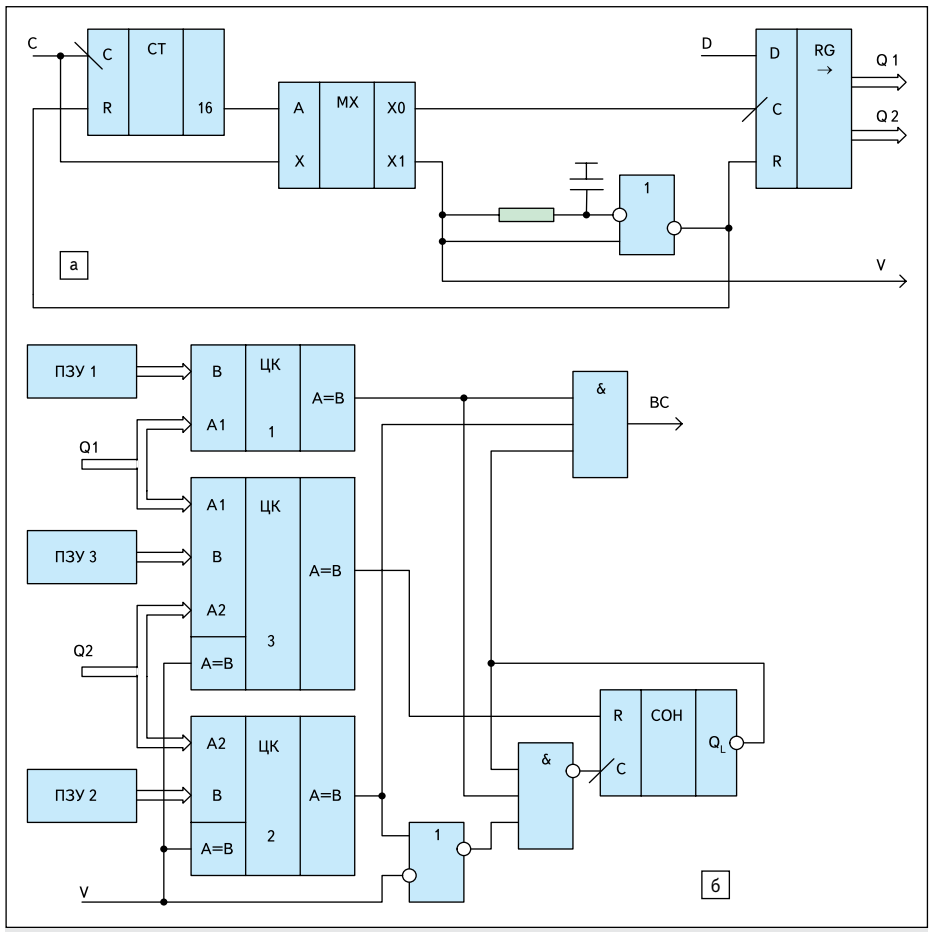

Рис. 1. СК с одновременным контролем группы разрядов:
а) схема блока преобразования входного кода; б) схема блока анализа кода

Пример схемной реализации соответствующего СК с преобразованием последовательного входного кода в параллельный показан на рис. 1 [2]. Причем на рис. 1а приведена схема блока преобразования входного кода (БПК), а на рис. 1б — схема блока анализа кода (БА). В схемах использован 16-разрядный входной код, 8 разрядов которого используются для ограничения количества фиксируемых ошибок.

В исходном состоянии счетчик тактов СТ установлен в состояние логического «0». Поэтому первый тактовый импульс положительной полярности с С-входа проходит через мультиплексор на тактовый вход регистра сдвига, обеспечивая запись входной информации с D-входа селектора. Задним фронтом тактового импульса переключается счетчик тактов. Аналогичным образом в регистр записывается информация остальных пятнадцати разрядов входного кода. Разделение разрядов на две группы производится на выходах регистра. После переключения СТ задним фронтом шестнадцатого тактового импульса уровень логической «1» формируется на адресном входе мультиплексора. Поэтому семнадцатый тактовый импульс проходит на V-вход блока преобразования кода. По заднему фронту семнадцатого импульса элемент ИЛИ-НЕ формирует положительный импульс, обеспечивающий установку счетчика тактов и регистра сдвига в исходное состояние логического «0».

Информация с выходов регистра сдвига в параллельном коде поступает на соответствующие входы “A” первого, второго и третьего цифровых компараторов блока анализа. На входах “B” первого и второго цифровых компараторов задается эталонное значение кода включения из постоянных запоминающих устройств: ПЗУ1 и ПЗУ2 соответственно. ПЗУ3 задает на вход “B” третьего цифрового компаратора эталонное значение кода разблокировки.

После приема всех разрядов входного кода поступает положительный импульс на V-вход блока анализа. При этом разрешается сравнение входного кода с эталонными значениями.

Допустим, что счетчик ошибок набора кода (СОН) находится в исходном состоянии логического «0». Тогда при совпадении всех разрядов входного кода с эталонным значением кода включения формируется выходной сигнал (ВС). Если состояние первой группы разрядов (Q1) совпало с эталонным значением, а в состоянии отдельных разрядов второй группы Q2 присутствует ошибка, то положительный импульс с V-входа проходит через элементы ИЛИ-НЕ и И-НЕ на С-вход СОН и вызывает его переключение. После фиксации допустимого количества L ошибок на выходе СОН устанавливается уровень логического «0», блокируя его дальнейшее переключение по С-входу. При поступлении входного кода, соответствующего эталонному значению кода разблокировки, формируется положительный импульс на выходе третьего цифрового компаратора, устанавливающий СОН в исходное состояние логического «0». При обнаружении ошибки в первой группе разрядов входного кода состояние БА не изменяется.

Аналогичная схема селектора команд с поразрядным контролем последовательного входного кода показана на рис. 2 [3].

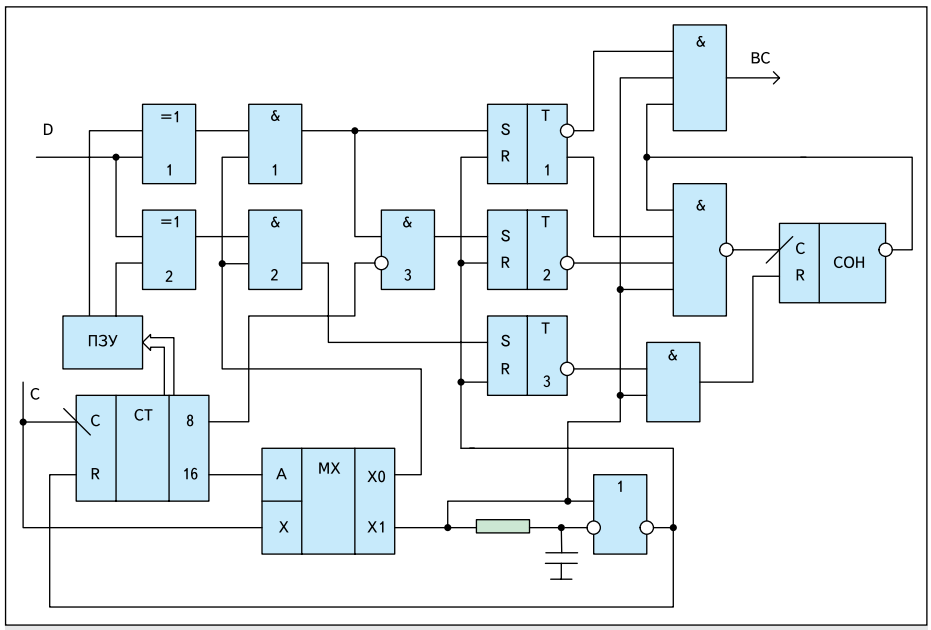

Рис. 2. СК с поразрядным контролем группы разрядов

В режиме ожидания счетчики и триггеры установлены в состояние логического «0». При этом мультиплексор передает сигналы с тактового входа устройства на входы первого и второго элементов И. Постоянное запоминающее устройство (ПЗУ) выдает на вход первого элемента «исключающее ИЛИ» эталонное значение первого разряда кода включения, а на вход второго элемента «исключающее ИЛИ» — эталонное значение первого разряда кода разблокировки. При совпадении сигнала с D-входа селектора с эталонным значением на выходе соответствующего элемента «исключающее ИЛИ» устанавливается уровень логического «0», в противном случае — уровень логической «1». Тактовые импульсы с помощью первого и второго элементов И производят опрос состояния соответствующих элементов «исключающее ИЛИ». При несовпадении разрядов входного кода с эталонным значением производится переключение соответствующих триггеров в состояние логической «1». Счетчик тактов СТ в процессе переключения тактовыми импульсами обеспечивает выдачу на выход ПЗУ всех разрядов эталонных значений кода включения и кода разблокировки.

После поступления восьми тактовых импульсов СТ запрещает прохождение сигналов на S-вход второго триггера. После шестнадцати импульсов СТ формирует положительный уровень сигнала на адресном входе мультиплексора. Поэтому семнадцатый импульс аналогично схемам, представленным на рис. 1, опрашивает состояние триггеров. Если все разряды входного кода совпали с эталонным значением кода включения, первый триггер остался в состоянии логического «0», и тактовый импульс проходит на выход ВС. Если были обнаружены ошибки в первой и второй группах разрядов, то первый и второй триггеры переключатся в состояние логической «1». В этом случае выходной сигнал не формируется, а счетчик ошибок набора кода остается в исходном состоянии. Если ошибки присутствовали только во второй группе разрядов, тактовый импульс обеспечивает переключение СОН. После достижения допустимого количества ошибок СОН запрещает формирование ВС и блокируется от дальнейшего переключения по С-входу. Для установки СОН в исходное состояние необходимо подать на вход селектора код разблокировки. По заднему фронту каждого семнадцатого импульса элемент ИЛИ-НЕ формирует положительный импульс, устанавливающий счетчик тактов и триггеры в состояние логического «0».

Таким образом, представленные технические решения обеспечивают определенную защиту от быстрой блокировки, но имеют недостаток, ограничивающий область их применения и связанный с однозначным разделением кода включения на две фиксированные группы разрядов. В этом случае злоумышленник может при одном из состояний разрядов второй группы провести перебор всех возможных состояний разрядов первой группы, а СОН в течение этой процедуры переключится не более одного раза и только при неправильном наборе состояний второй группы разрядов. Поэтому для несанкционированного включения селектора с первой попытки подбора кода злоумышленнику достаточно угадать состояние $(n–m)$ разрядов второй группы, где m — количество разрядов первой группы. В этом случае вероятность включения селектора с первой попытки увеличивается до значения $P_1 = 1/2^{n-m}$, что в 2^m раз больше вероятности несанкционированного включения базового варианта.

Для исключения указанного недостатка необходимо убрать жесткую привязку контролируемых разрядов первой группы к их месту в составе входного кода, сохранив только их количество при произвольном расположении.

Пример схемной реализации соответствующего селектора цифровых команд [4] приведен на рис. 3.

В режиме ожидания все триггеры и счетчики установлены в состояние логического «0». ПЗУ выдает на вход первого элемента «исключающее ИЛИ» эталонное значение первого разряда кода включения, а на вход второго элемента «исключающее ИЛИ» — эталонное значение первого разряда кода разблокировки. При совпадении информации на D-входе селектора с эталонным значением на прямом выходе элемента «исключающее ИЛИ» устанавливается уровень логического «0», а на инверсном выходе — уровень логической «1». При несовпадении информации состояние выходного сигнала инвертируется. Первый тактовый импульс, поступающий на С-вход селектора, опрашивает состояние элементов «исключающее ИЛИ» с помощью элементов И. При несовпадении информации с эталонным значением кода включения на выходе первого элемента И формируется положительный импульс, переключающий первый триггер, осуществляющий фиксацию ошибок набора кода, в состояние логической «1». При совпадении информации положительный импульс формируется на выходе второго элемента И и вызывает переключение счетчика совпадений разрядов (ССР). При совпадении входной информации с эталонным значением первого разряда кода разблокировки, не совпадающим со значением кода включения, переключается первый триггер, а при несовпадении — второй триггер.

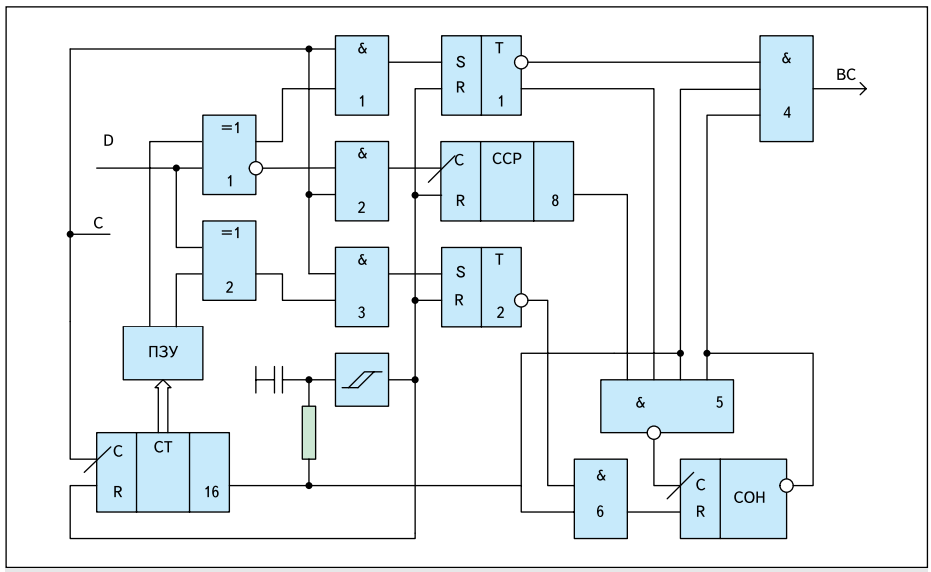

Рис. 3. СК с контролем ошибок и совпадений

По заднему фронту тактового импульса переключается счетчик тактов и обеспечивает выдачу на выход ПЗУ вторых разрядов эталонных значений кода включения и кода разблокировки. Далее работа селектора происходит аналогичным образом.

После переключения счетчика тактов последним (например, шестнадцатым) тактовым импульсом на его выходе формируется положительный уровень, поступающий на входы четвертого, пятого и шестого элементов И. При этом в случае безошибочного набора кода включения формируется выходной сигнал ВС. В случае безошибочного набора кода разблокировки подтверждается исходное состояние счетчика ошибок набора кода (СОН). Если же наблюдались отдельные ошибки в наборе кода включения, и количество совпадений разрядов достигло порогового значения (в данной схеме — 8), происходит переключение СОН. При достижении порогового значения ошибочных кодов включения производится его блокировка от дальнейшего переключения по С-входу и запрет формирования ВС. Если количество совпадений не достигло порогового значения, состояние СОН не изменяется.

Положительный перепад сигнала с выхода счетчика тактов одновременно поступает на вход интегрирующей RC-цепи и с определенной задержкой вызывает переключение триггера Шмитта в состояние логической «1», что приводит к сбросу СТ, ССР и триггеров в исходное состояние логического «0» и окончание ВС. Длительность выходного сигнала определяется временем заряда конденсатора RC-цепи до порога срабатывания триггера Шмита, а длительность его выходного импульса — временем разряда конденсатора от порога срабатывания до порога отпускания триггера Шмитта.

Схема на рис. 3 отличается тем, что в ней, кроме счетчика совпадений разрядов, использованы триггеры фиксации ошибок набора кода включения и кода разблокировки. При этом код разблокировки может подаваться в любой момент, в том числе и до блокировки СОН.

На рис. 4 приведена схема селектора [5] без использования триггеров фиксации ошибок, отличающаяся от схемы, изображенной на рис. 3, тем, что на выходе ПЗУ включен мультиплексор, выдающий на вход элемента «исключающее ИЛИ» эталонное значение кода разблокировки только после блокировки селектора. Данное свойство схемы может быть получено также при использовании ПЗУ с дополнительным адресным входом в соответствии с рис. 4б, где АР — адрес разряда кода, АЭ — адрес эталонного значения.

В схеме (рис. 4а) после поступления всех разрядов входного кода на выходе СТ формируется положительный перепад напряжения. Если к этому моменту во входном коде не было допущено ни одной ошибки, то состояние ССР совпадает с состоянием СТ, и на выходе первого элемента И формируется выходной сигнал. Если ошибки во входном коде были, но количество совпадений достигло порогового значения, то производится переключение СОН. После набора порогового количества ошибочных кодов СОН блокируется по входу, запрещает формирование ВС и переключает мультиплексор на передачу эталонного значения кода разблокировки. После безошибочного набора кода разблокировки состояние ССР соответствует состоянию СТ.

Положительный перепад напряжения поступает также на вход интегрирующей RC-цепи. После заряда конденсатора до порога срабатывания триггер Шмитта устанавливается в состояние логической «1» и переключает в это состояние мажоритарный элемент. Положительный импульс триггера Шмитта устанавливает СТ и ССР в состояние логического «0», но мажоритарный элемент остается в состоянии логической «1» из-за влия-

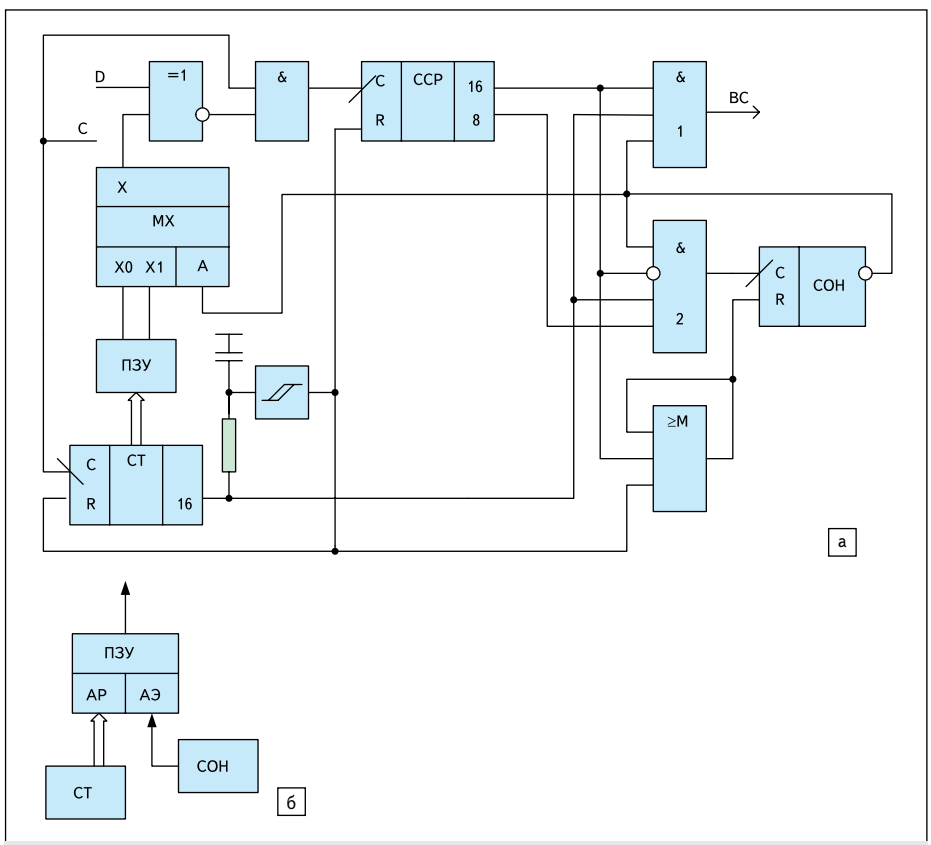

Рис. 4. СК с контролем совпадений

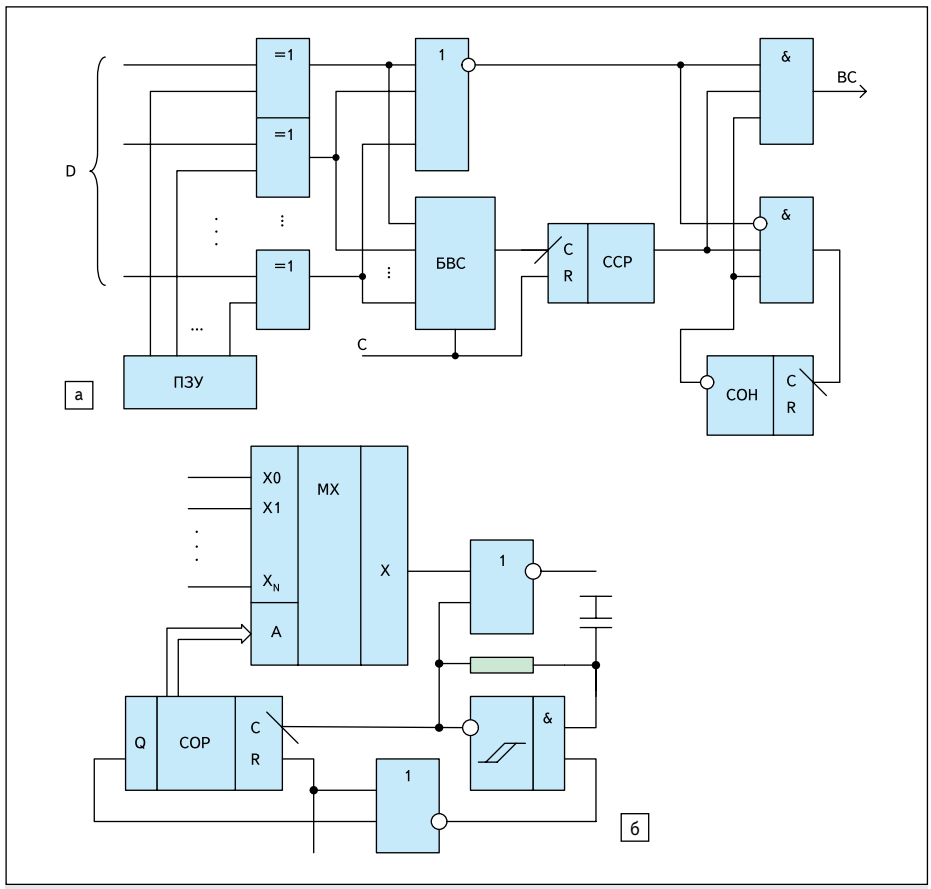

Рис. 5. СК с управлением параллельным кодом

ния обратной связи, обеспечивая надежное обнуление СОН. В данной схеме обнуление СОН происходит и при безошибочном наборе кода включения.

Интегрирующая RC-цепь обеспечивает формирование длительности ВС при заряде конденсатора до порога срабатывания триггера Шмитта и формирование длительности импульса обнуления счетчиков при разряде конденсатора от порога срабатывания до порога отпускания триггера Шмитта.

Представленные на рис. 3 и 4 селекторы обеспечивают фиксацию всех возможных вариантов ошибочных входных кодов, количество совпадений разрядов которых с эталонными значениями достигает пороговой величины, что исключает недостаток селекторов, показанных на рис. 1, 2, и позволяет сохранить вероятность включения селектора с первой попытки подбора кода на уровне базового варианта. Количество фиксируемых входных кодов можно определить как число сочетаний из n по m [6]. При $n = 16$ и $m = 8$ $C_n^m = 12\,870$ вместо одного в схемах на рис. 1, 2. В рассмотренном случае перекрываются все возможные пути приближения входного кода к эталонному значению кода включения.

При использовании параллельно-последовательного входного кода в схеме на рис. 1 емкость счетчика тактов и регистра сдвига уменьшается до количества параллельных посылок, но количество регистров возрастает до количества разрядов в каждой посылке. При этом суммарное количество разрядов регистров сохраняется. При использовании параллельного входного кода необходимость в блоке преобразования кода отпадает, но при поступлении входного кода должен формироваться сигнал на V-входе блока анализа.

В схеме селектора на рис. 2 для управления параллельно-последовательным кодом необходимо уменьшить емкость счетчика тактов до количества параллельных посылок и заменить элементы «исключающее ИЛИ» на цифровые компараторы, количество разрядов которых и количество разрядов по каждому выходу ПЗУ должно быть равно количеству разрядов в каждой из посылок. При этом в каждой группе разрядов должно быть целое число параллельных посылок. Управление параллельным кодом в данной схеме так же, как и в схемах на рис. 3 и 4, не может быть реализовано.

Аналог схемы на рис. 3 с управлением параллельным кодом показан на рис. 5а, где БВС — блок выделения совпадений, схема которого приведена на рис. 5б.

В исходном состоянии на С-входе устройства поддерживается уровень логической «1», удерживающий счетчик совпадений разрядов (ССР) и счетчик опроса разрядов (СОР) БВС в состоянии логического «0». При этом работа генератора на основе триггера Шмитта запрещена. На его выходе удерживается уровень логической «1».

При поступлении информации на D-вход селектора происходит ее поразрядное сравнение с эталонным значением кода включения с помощью элементов «исключающее ИЛИ». При совпадении входного кода с эталонным значением на выходах всех элементов «исключающее ИЛИ» присутствует уровень логического «0», а на выходе элемента ИЛИ-НЕ — уровень логической «1». Если счетчик ошибок набора кода находится в исходном состоянии логического «0», на его инверсном выходе присутствует уровень логической «1». При поступлении на С-вход селектора одновременно с входной информацией уровня логического «0» разрешается переключение ССР и СОР и работа генератора, который вызывает переключение СОР и последовательный опрос с помощью мультиплексора состояния всех элементов «исключающее ИЛИ». Если на выходе элемента «исключающее ИЛИ» присутствует уровень логического «0», на выходе БВС формируется положительный импульс, вызывающий переключение ССР. При достижении ССР порогового значения на его выходе формируется уровень логической «1», вызывающий формирование ВС. Если во входном коде были ошибки, то выходной сигнал ССР вызывает переключение СОН.

После опроса состояния всех элементов «исключающее ИЛИ» на выходе Q ССР формируется уровень логической «1», запрещающий дальнейшую работу генератора и формирование импульсов на выходе БВС. После этого входную информацию можно снимать. Установка СОН в исходное состояние кодом разблокировки может быть реализована в данной схеме аналогично рис. 1. Многовходовой элемент ИЛИ-НЕ в данной схеме может быть исключен при использовании ССР в соответствии с рис. 4.

Аналог селектора (рис. 3) с управлением параллельно-последовательным кодом приведен на рис. 6.

Емкость счетчика тактов в данной схеме определяется количеством параллельных посылок входного кода. Количество элементов «исключающее ИЛИ» равно количеству разрядов в параллельной посылке. БВС выделяет совпадения разрядов входного кода с эталонными значениями последовательно для каждой из параллельных посылок. ССР суммирует совпадения разрядов. Формирование ВС и переключение СОН проводится аналогично схеме, показанной на рис. 3. В соответствии с рис. 3 может быть организован и сброс СОН в исходное состояние с учетом замены второго элемента «исключающее ИЛИ» на цифровой компаратор, количество разрядов которого равно количеству разрядов параллельной посылки входного кода, и соответствующей организации ПЗУ. RS-триггер и два элемента ИЛИ-НЕ на его S-входе можно исключить при организации работы селектора в соответствии со схемой на рис. 4.

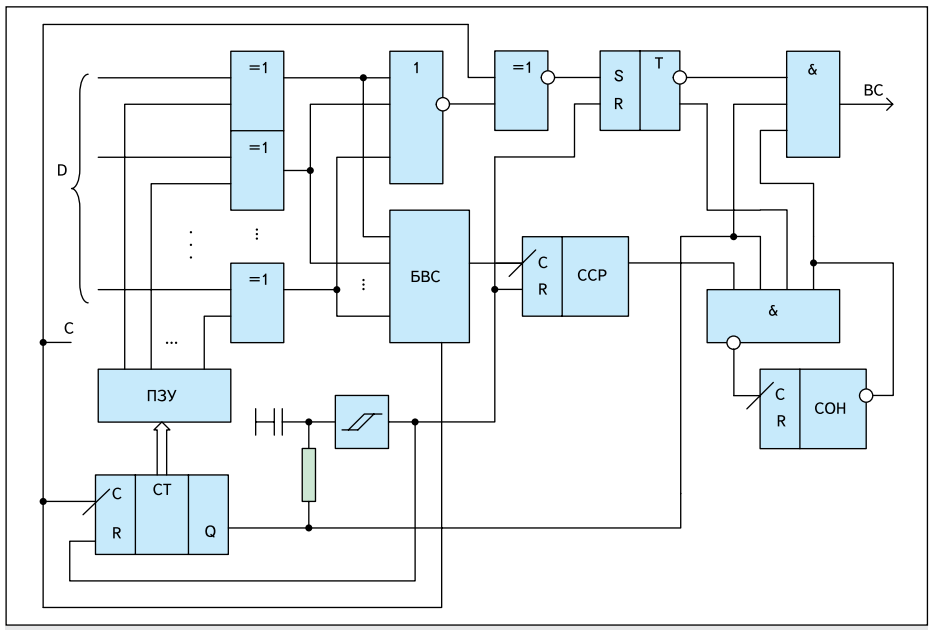

Рис. 6. СК с управлением параллельно-последовательным кодом

Литература

1. Николаев Д. Б., Шишкин Г. И. Селекторы цифровых команд. Часть 1 // Компоненты и технологии. 2009. № 6.
2. Патент № 2239037 РФ, МКИ E05B47/00. Устройство управления электронного замка / Р. Ф. Зубаеров, С. В. Панкратов, Г. И. Шишкин // Изобретения. Полезные модели. 2004. № 30.
3. Патент № 2247205 РФ, МКИ E05B47/00. Устройство управления кодового замка / Р. Ф. Зубаеров, О. А. Островский, С. В. Панкратов, Г. И. Шишкин // Изобретения. Полезные модели. 2005. № 6.
4. Патент № 2345203 РФ, МКИ E05B49/00. Устройство управления электронного замка / А. А. Котуранов, А. П. Мартынов, Г. И. Шишкин // Изобретения. Полезные модели. 2009. № 3.
5. Патент № 2239037 РФ, МКИ E05B47/00. Устройство управления электронного замка / А. А. Котуранов, А. П. Мартынов, Г. И. Шишкин // Изобретения. Полезные модели. 2009. № 3.
6. Выгодский М. Я. Справочник по элементарной математике. М. : Наука, 1976.