Селекторы цифровых команд
Часть 3

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

Представлены возможные способы построения селекторов цифровых команд на основе многоустойчивых последовательностных устройств с псевдослучайным изменением состояния в процессе подбора кода включения.

При использовании параллельно-последовательного входного кода код включения селектора команд (СК) задается в виде определенного количества последовательных групп параллельного кода. При этом можно производить проверку каждой из групп последовательно без преобразования параллельно-последовательного кода в параллельный СК. В этом случае необходимо иметь несколько устойчивых состояний, количество которых равно количеству групп входного кода. Выходной сигнал (ВС) селектора может формироваться счетным устройством сигналов совпадения (СС) каждой из групп с эталонным значением после приема всего кода. Тогда уменьшение вероятности несанкционированного включения СК может быть достигнуто без смены эталонного значения кода включения путем переключения счетного устройства в случае ошибки набора любой из групп входного кода в исходное или предыдущее состояние. Таким образом, в процесс смены состояний СК при подборе кода вносится элемент случайности, который исключает возможность создания определенного (детерминированного) алгоритма подбора кода, обеспечивающего гарантированное включение СК, и увеличивает объем массива исчерпывающего перебора входных кодов. Селектор команд может быть построен по многоступенчатой схеме на основе счетного устройства в виде регистра сдвига или счетчика импульсов.

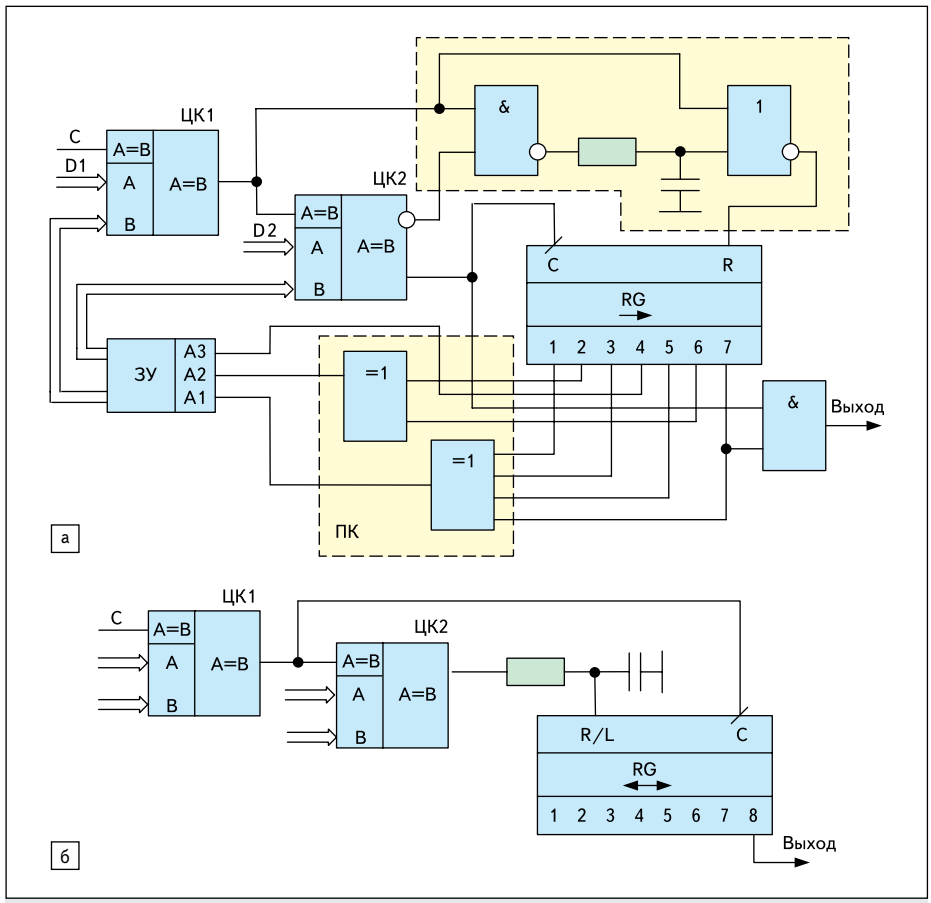

Рис. 1. СК на основе регистра с одновременной подачей команд подготовки и доступа

Схема СК на основе регистра сдвига со сбросом в исходное состояние представлена на рис. 1а.

В исходном состоянии регистр сдвига и цифровые компараторы ЦК1 и ЦК2 находятся в состоянии логического «0». На выходе формирователя импульсов сброса ФС присутствует уровень логического «0», конденсатор RC-цепи заряжен. На B-входы ЦК1 и ЦК2 из запоминающего устройства (ЗУ) подается первое эталонное значение кода. При поступлении первой группы разрядов входного кода с тактовым импульсом первая часть ее разрядов (код подготовки) поступает на A-вход ЦК1, а тактовый импульс — на вход «A=B». Если код подготовки не соответствует эталонному значению, состояние устройства не изменяется.

Когда код подготовки соответствует эталонному значению, на выходе ЦК1 формируется положительный импульс, который разрешает сравнение второй части разрядов (код доступа) с эталонным значением. При их несоответствии состояние ЦК2 не изменяется. При этом на выходе элемента И-НЕ ФС устанавливается уровень логического «0». Конденсатор RC-цепи разряжается.

В момент окончания входного кода ЦК1 возвращается в состояние логического «0». При этом на выходе ФС формируется положительный импульс, подтверждающий состояние логического «0» регистра сдвига. Одновременно на выходе элемента И-НЕ восстанавливается уровень логической «1», вызывающий заряд конденсатора. Длительность выходного импульса ФС определяется временем заряда конденсатора до порога срабатывания элемента ИЛИ-НЕ.

Если же код доступа соответствует эталонному значению, ЦК2 переключается в состояние логической «1». На инверсном выходе ЦК2 формируется уровень логического «0», запрещающий разряд конденсатора ФС и формирование выходного импульса. На прямом выходе ЦК2 устанавливается уровень логической «1». В момент окончания

группы входного кода ЦК1 и ЦК2 переключаются в исходное состояние. Отрицательный перепад напряжения на прямом выходе ЦК2 вызывает переключение первого разряда регистра в состояние логической «1». На выходе преобразователя кодов ПК, а следовательно, и на адресных входах ЗУ устанавливается состояние «100», обеспечивающее выдачу на выход ЗУ второго эталонного значения кода.

Далее работа СК происходит аналогичным образом. При несоответствии кода подготовки эталонному значению состояние устройства не изменяется. При его соответствии эталонному значению возможны два варианта:

- Если код доступа не соответствует эталонному значению, производится сброс регистра в исходное состояние логического «0».
- Если код доступа соответствует эталонному значению, производится переключение регистра в следующее состояние.

ВС формируется с помощью элемента совпадения при поступлении группы разрядов входного кода, соответствующей эталонному значению, после переключения в состояние логической «1» седьмого разряда регистра. ПК обеспечивает преобразование параллельного выходного кода регистра (кода Джонсона) в отраженный двоичный код [1], пригодный для управления состоянием ЗУ.

Логику работы преобразователя поясним с помощью таблицы истинности, где *d* — сигналы кода Джонсона, *a* — сигналы двоичного кода.

Преобразователь строится на основе элементов «ИСКЛЮЧАЮЩЕЕ ИЛИ». При этом на входы элемента, формирующего младший разряд двоичного кода, подключаются выходы всех нечетных разрядов регистра. На входы элемента, формирующего второй разряд, подключаются выходы разрядов, номера которых становятся нечетными после деления на 2; на входы элемента, формирующего третий разряд, — выходы разрядов, номера которых становятся нечетными после деления на 4, и т. д. Установка элемента в цепи старшего разряда двоичного кода не нужна.

Сброс счетного устройства сигналом ошибки в предыдущее состояние может быть реализован при использовании реверсивного регистра сдвига. Способ управления состоянием реверсивного регистра сдвига в составе СК со сбросом в предыдущее состояние показан на рис. 1б. В данной схеме, в отличие от рис. 1а,

Таблица истинности преобразователя кода Джонсона в двоичный код

d1	d2	d3	d4	d5	d6	d7	a1	a2	a3
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0
1	1	0	0	0	0	0	1	1	0
1	1	1	0	0	0	0	0	1	0
1	1	1	1	0	0	0	0	1	1
1	1	1	1	1	0	0	1	1	1
1	1	1	1	1	1	0	1	0	1
1	1	1	1	1	1	1	0	0	1

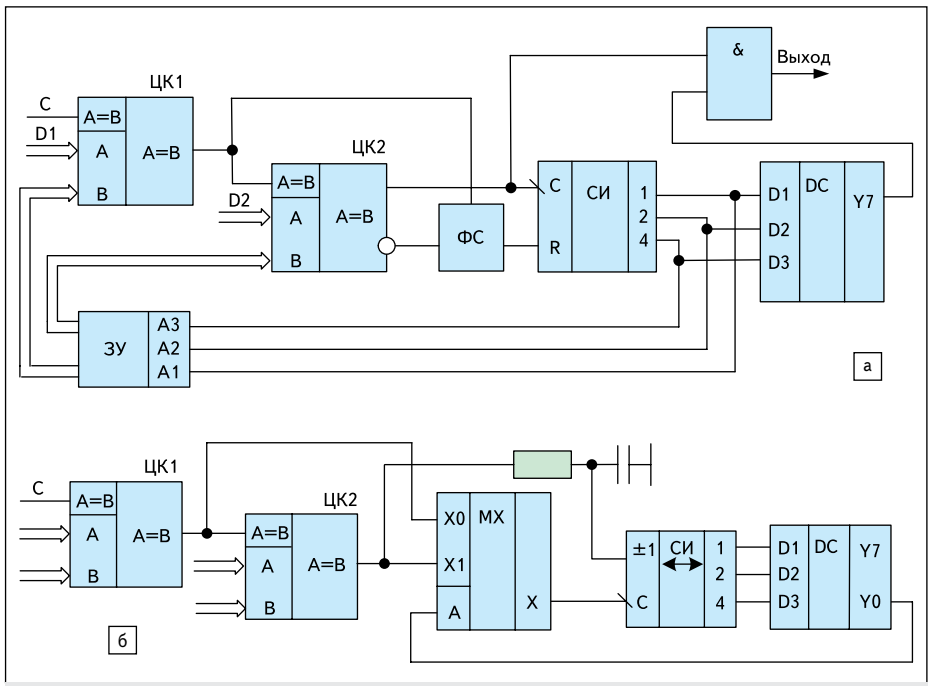

Рис. 2. СК на основе счетчика с одновременной подачей команд подготовки и доступа

ФС не требуется, переключение регистра производится выходным сигналом ЦК1, а не ЦК2. Выходной сигнал ЦК2 определяет направление сдвига информации: при соответствии кода доступа каждой группы входного кода эталонному значению производится сдвиг состояния логической «1» вправо, в противном случае регистр возвращается в предыдущее состояние путем сдвига информации влево. В схеме (рис. 1б) ВС формируется после переключения в состояние логической «1» восьмого (дополнительного по сравнению с рис. 1а) разряда регистра. В этом случае нет необходимости вводить элемент совпадения. Однако в любой из схем можно использовать любой способ формирования ВС.

Схема СК со сбросом в исходное состояние на основе счетчика импульсов представлена на рис. 2а. В данной схеме, в отличие от рис. 1а, не требуется преобразование выходного кода счетчика в код, приемлемый для управления состоянием ЗУ, но необходимо использование дешифратора для формирования ВС выходным сигналом ЦК2 после установки счетчика в состояние «111».

Способ управления состоянием реверсивного счетчика импульсов в составе СК со сбросом в предыдущее состояние показан на рис. 2б. Направление переключения счетчика, как и в схеме на рис. 1б, определяется выходным сигналом ЦК2: при совпадении кода доступа с эталонным значением счетчик работает в режиме сложения, в противном случае счетчик переключается в режим вычитания. В данной схеме, в отличие от рис. 1б, необходимо принимать меры для исключения возможности работы счетчика в режиме вычитания после установки в исходное состояние логического «0», поскольку в этом случае счетчик импульсов одним ошибочным кодом может переключиться в состояние «111» формирования ВС. С этой целью в схему вводится дешифратор состояния «000» счетчика и мультиплексор, разрешающий переключение счетчика из этого состояния только выходным сигналом ЦК2 (в режиме сложения).

ЦК1 в представленных схемах ограничивает возможность сброса регистра (счетчика) в исходное (предыдущее) состояние и таким образом усложняет процедуру включения СК (формирования ВС) путем подбора кода.

В представленных схемах возможно санкционированное включение СК после попыток подбора кода из любого состояния, как из исходного, при условии, что все эталонные значения, подаваемые на вход ЦК1, отличаются информацией хотя бы в одном разряде. Во всех остальных случаях санкционированное включение возможно только после приведения счетного устройства СК в исходное состояние. Установка СК в исходное из любого состояния производится путем подачи на вход групп разрядов входного кода, начиная со старших разрядов, коды подготовки которых соответствуют эталонным значениям, а коды доступа отличаются от эталонов.

Одновременная подача команд подготовки и доступа в схемах на рис. 1 и 2 требует соответствующего количества линий связи. Уменьшение количества линий связи достигается при последовательной подаче этих команд. Способы построения СК в этом случае показаны на рис. 3. На рис. 3а приведена схема управления счетным устройством с использованием отдельных компараторов проверки кодов подготовки (ЦК1) и доступа (ЦК2). Выход R нужен при построении

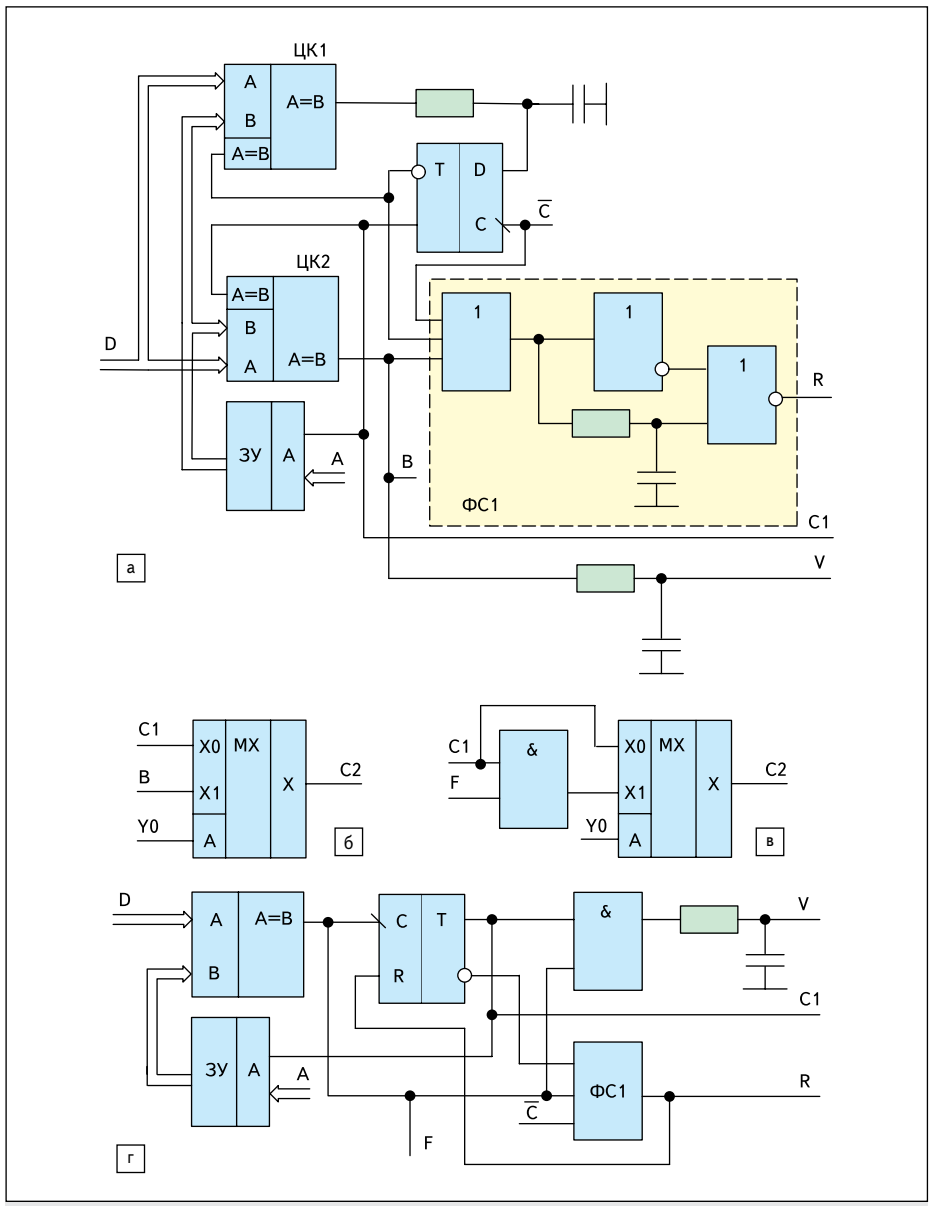

Рис. 3. СК с последовательной подачей команд подготовки и доступа

СК со сбросом в исходное состояние, выход V — для управления направлением переключения счетного устройства при построении СК со сбросом в предыдущее состояние. Выход C1 подключается к тактовым входам регистров или суммирующего счетчика. При использовании реверсивного счетчика счетный импульс формируется схемой (рис. 3б), где Y0 — выходной сигнал дешифратора нулевого состояния счетчика. На A-вход подаются выходные сигналы счетчика или преобразователя кода ПК.

В исходном состоянии триггер находится в состоянии логического «0». При этом разрешается работа ЦК1, работа ЦК2 запрещена сигналом логического «0» по входу «A=B». На B-вход ЦК1 подается эталонное значение кода подготовки.

Если код подготовки не соответствует эталонному значению, состояние схемы не изменяется. В противном случае на выходе ЦК1 формируется положительный импульс. Поэтому по заднему фронту тактового импульса триггер переключается в состояние логической «1», запрещая работу ЦК1, разрешая работу ЦК2 и обеспечивая подачу на B-вход ЦК2 эталонного значения кода доступа. При поступлении на D-вход СК кода доступа, соответствующего эталонному значению, на выходе ЦК2 формируется положительный импульс, устанавливающий уровень логической «1» на V-выходе и запрещающий срабатывание формирователя импульса сброса ФС1. В этом случае по заднему фронту тактового импульса триггер переключается в состояние логического «0», формируя соответствующий сигнал на выходе C1 и вызывая переключение счетного устройства.

Если код доступа не соответствует эталонному значению, на выходе ЦК2, а следовательно, и на V-выходе сохраняется уровень логического «0». Во время тактового импульса трехвходовой элемент ИЛИ-НЕ ФС1 переключается, разряжая конденсатор RC-цепи. Поэтому при окончании тактового импульса ФС1 формирует положительный импульс, длительность которого определяется временем заряда конденсатора до порога срабатывания двухвходового элемента ИЛИ-НЕ. Значит, приведенная схема управления обеспечивает работоспособность СК с любым вариантом счетного устройства.

Схема управления счетным устройством СК с использованием общего компаратора проверки кодов подготовки и доступа приведена на рис. 3в. Схема ФС1 соответствует рис. 3а. В исходном состоянии триггер находится в состоянии логического «0». При этом запрещается запуск формирователя сброса ФС1 и прохождение выходного сигнала ЦК через элемент И. При поступлении на D-вход кода подготовки, совпадающего с эталонным значением, на выходе ЦК формируется импульс, по заднему фронту которого триггер переключается в состояние логической «1». На B-вход ЦК подается эталонное значение кода доступа. При совпадении входного кода доступа с эталонным значением выходной сигнал ЦК проходит через элемент И, устанавливая уровень логической «1» на V-выходе. Запуск ФС1 не происходит. По заднему фронту выходного импульса ЦК триггер переключается в состояние логического «0», формируя переключающий сигнал по выходу C1 для переключения регистров и суммирующего счетчика.

Если входной код доступа не совпадает с эталонным значением, на V-выходе сохраняется уровень логического «0» и запускается ФС1, формирующий положительный импульс по R-выходу, который переключает триггер в состояние логического «0», формируя переключающий сигнал на выходе C1. При использовании счетного устройства на основе реверсивного счетчика счетный импульс формируется схемой, изображенной на рис. 3г.

При использовании последовательного входного кода технические решения СК принимают вид, представленный на рис. 4. На рис. 4а показана общая часть схема управления всех возможных вариантов СК. В исходном состоянии на входах C, D, S1, S2 устройства присутствует уровень логического «0». Конденсатор RDC-цепи формирователя импульсов (ФИ) разряжен. На выходе триггера Шмитта присутствует уровень логической «1», удерживающий счетчик тактов СТ и триггеры в состоянии логического «0». При этом триггер T0 разрешает прохождение сигналов через элемент ИЛИ-НЕ на S-вход триггера T1. На выходе ЗУ присутствует информация эталонного значения первого разряда кода подготовки группы разрядов первой части кода включения. При поступлении положительного тактового импульса на C-вход конденсатор RDC-цепи быстро заряжается, триггер Шмитта устанавлива-

ется в состояние логического «0», разрешая переключение счетчика тактов и триггеров. Если информация на D-входе устройства совпадает с эталонным значением, на выходе элемента ИСКЛЮЧАЮЩЕЕ ИЛИ присутствует уровень логического «0», на выходе элемента И-НЕ — уровень логической «1», обеспечивающий отсутствие сигналов переключения на S-входах триггеров T1 и T2. Если информация на D-входе не совпадает с эталонным значением, выходной сигнал логического «0» элемента И-НЕ вызывает переключение триггеров T1 и T2 в состояние логической «1». По заднему фронту тактового импульса переключается счетчик тактов, обеспечивая выдачу на выход ЗУ второго разряда эталонного значения кода. Во время паузы между тактовыми импульсами состояние триггера Шмитта не изменяется. Далее работа происходит аналогичным образом.

После приема кода подготовки счетчик тактов обеспечивает переключение триггера T0 сигналом с выхода Q_n, запрещая прохождение сигналов на S-вход триггера T1. Если все разряды кода подготовки совпали с эталонами, триггер T1 остается в состоянии логического «0», при наличии ошибок триггер переключается в состояние логической «1». После приема кода доступа по заднему фронту тактового импульса счетчик тактов формирует по входу $Q_д$ положительный перепад напряжения, который передается на выход C1 схемы. К этому моменту триггер T2 может находиться в состоянии логического «0», если не было ошибок в наборе входного кода, или в состоянии логической «1» при наличии ошибок. После окончания последнего тактового импульса конденсатор RDC-цепи медленно разряжается. При достижении напряжением на конденсаторе порога отпускания триггер Шмитта переключается в состояние логической «1», устанавливая счетчик тактов и триггеры в состояние логического «0» и заканчивая выходные сигналы. При поступлении последующих групп входного кода устройство (рис. 4а) работает аналогичным образом.

Подключение реверсивного регистра сдвига к схеме (рис. 4а) производится в соответствии с рис. 4б, аналогично рис. 1б. При этом триггер T2 выполняет функцию ЦК2, определяя направление сдвига информации. Функцию ЦК1 выполняет триггер T1, определяя возможность сдвига информации, и счетчик тактов, сигнал C1 которого задает момент сдвига.

Подключение реверсивного счетчика импульсов производится в соответствии с рис. 4в, аналогично рис. 2б. При этом сигнал C1 счетчика тактов определяет не только момент переключения реверсивного счетчика, но и момент формирования ВС.

Способ подключения входных цепей регистра сдвига (суммирующего счетчика импульсов) в составе СК со сбросом в исходное состояние показан на рис. 4г. При этом, в отличие от рис. 1а и 2а, введение специального формирователя импульса сброса необязательно.

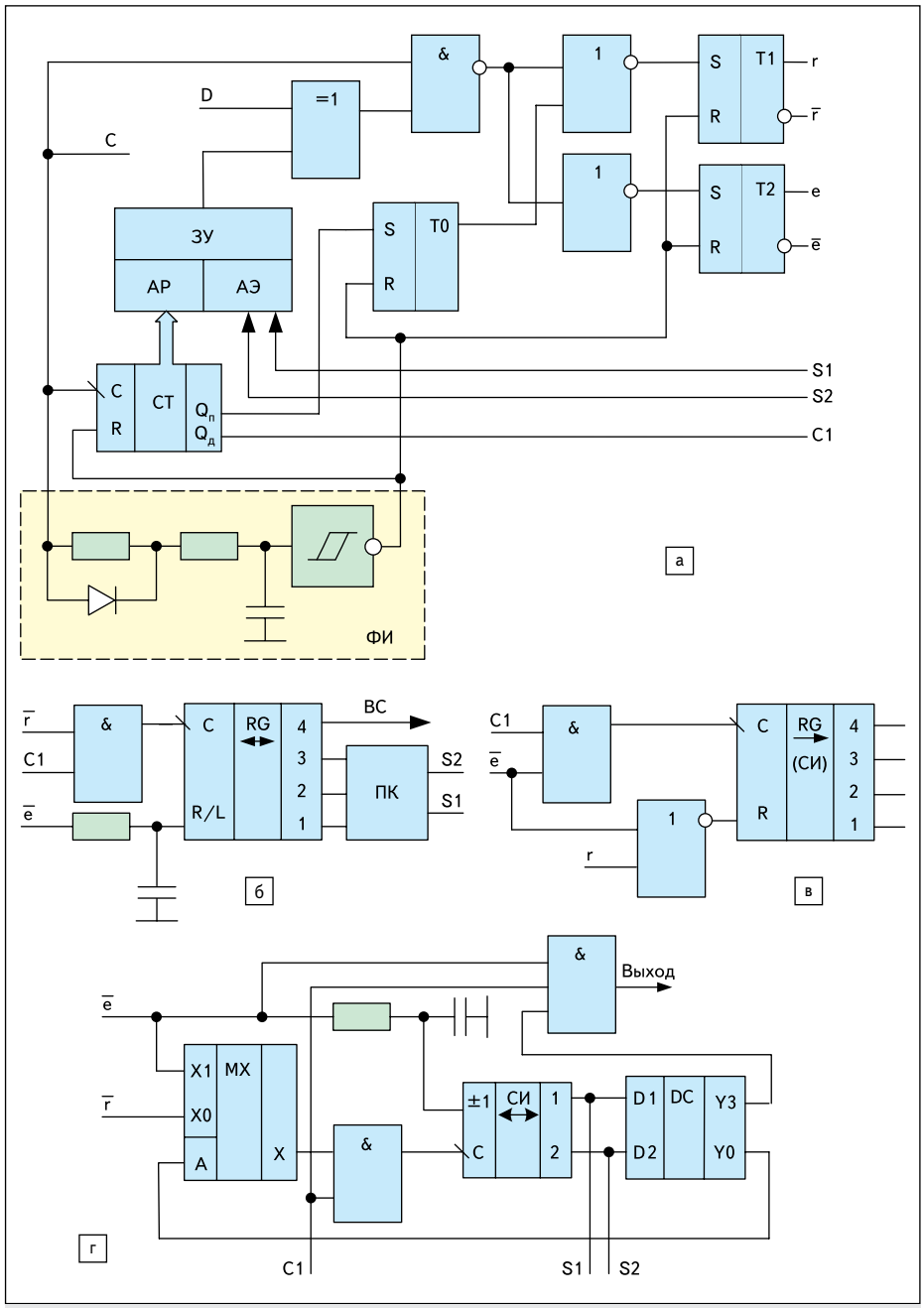

Рис. 4. СК с управлением последовательным кодом

Вывод селекторов команд, представленных на рис. 4, из промежуточных состояний после попыток подбора кода производится аналогично соответствующим устройствам (рис. 1 и 2).

В схемах (рис. 4) доступ к счетному устройству СК ограничен условием правильного набора кода подготовки каждой из групп разрядов входного кода. При ограничении доступа условием правильного набора определенного количества m разрядов каждой группы входного кода [3] схема управления (рис. 4а) принимает вид, представленный на рис. 5а. В данной схеме вместо триггера T1 (рис. 4а) установлен счетчик сигналов совпадения (ССС) состояния разрядов входного кода с эталонным значением, формирующий выходные сигналы после поступления m сигналов совпадения. Наличие ошибок во входном коде, как и в схеме на рис. 4а, фиксируется триггером.

На рис. 5б представлен вариант схемы управления, в которой ССС после поступления m сигналов совпадения формируется перепад напряжения на выходе Q_m, разрешающий доступ к счетному устройству, а при условии совпадения всех n разрядов с эталонным значением формируется перепад напряжения на выходе Q_n, свидетельствующий об отсутствии ошибок во входном коде.

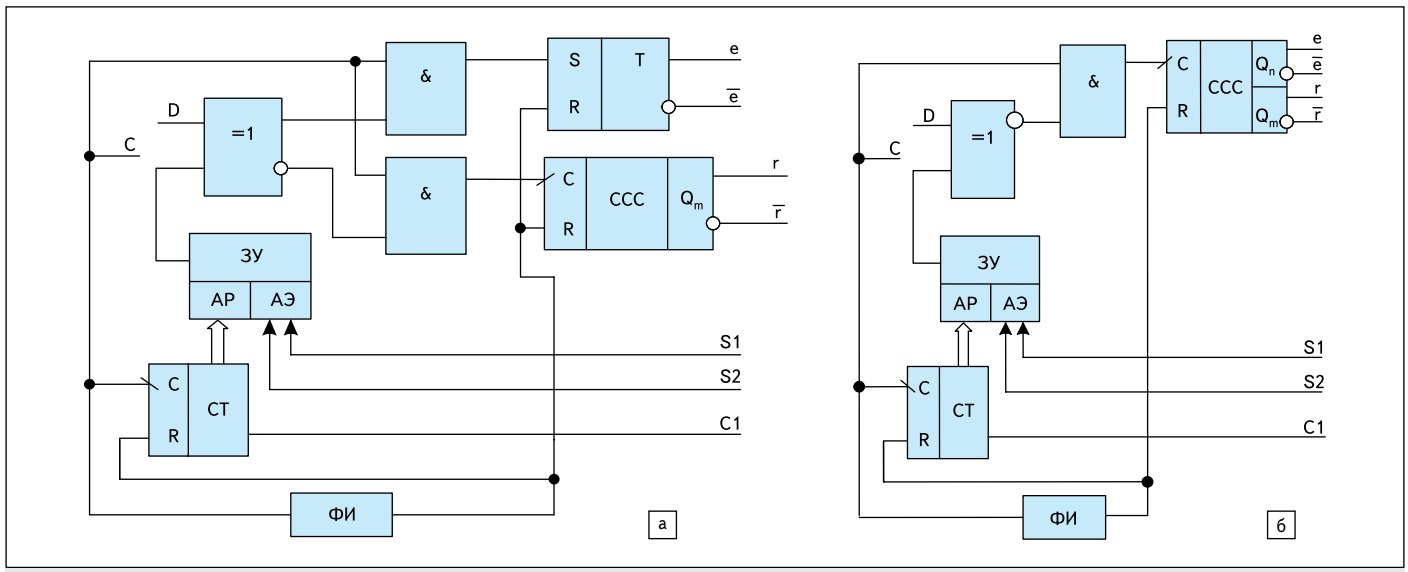

Рис. 5. СК с проверкой количества правильно набранных разрядов

В показанных на рис. 4, 5 технических решениях входной код задается по частям. При этом счетное устройство переключается после проверки каждой из групп разрядов, между которыми необходимо делать перерыв. Варианты СК с управлением непрерывным последовательным кодом на основе счетчиков импульсов с переключением их по результатам проверки каждого из разрядов входного кода представлены на рис. 6. Необходимо отметить, что емкость счетчиков импульсов в данных схемах должна быть больше, чем в схемах, приведенных на рис. 4, поскольку она должна соответствовать суммарному количеству разрядов входного кода, а не количеству его частей. Однако в этом случае не требуется использование счетчика тактов, триггеров и некоторых других элементов.

На рис. 6а приведена схема СК со сбросом в исходное состояние. Структура данной схемы соответствует представленным ранее техническим решениям и дополнительных пояснений не требует. Для вывода данного СК из произвольного промежуточного состояния после попыток подбора кода в исходное состояние необходимо задать на D-вход состояние, инверсное состоянию первого разряда эталонного значения, и подать $(n-1)$ тактовых импульсов.

На рис. 6б приведена схема СК со сбросом в предыдущее состояние. В данной схеме, в отличие от рис. 2б и 4в, переключение счетчика из исходного состояния в режиме вычитания исключается с помощью двух элементов И-НЕ. ВС формируется аналогично рис. 6а. Для вывода данного селектора из неизвестного промежуточного состояния необходим специальный, недоступный для злоумышленника вход сброса счетчика.

Селекторы команд, аналогичные изображенным на рис. 6а и 6б, можно построить и на основе регистров сдвига. Однако в этом случае требуются многоразрядные регистры и сложные схемы преобразователей кодов, что существенно ограничивает возможность их использования.

Представленные в данной статье технические решения селекторов цифровых команд расширяют арсенал средств разработчиков электронной аппаратуры и способствуют улучшению ее технических характеристик. ■

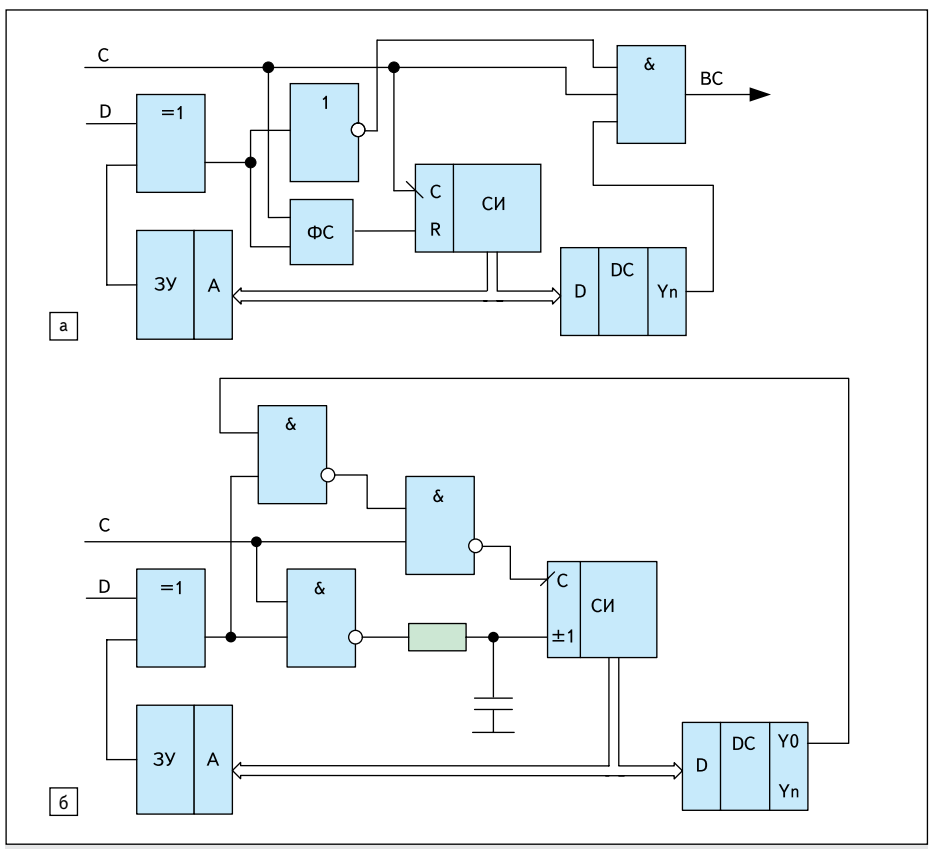

Рис. 6. СК с управлением непрерывным последовательным кодом

Продолжение следует

Литература

1. Шишкин Г. И. Помехозащищенные цифровые устройства. Саров: РФЯЦ-ВНИИЭФ, 1999.
2. Шишкин Г., Николаев Д. Селекторы цифровых команд. Часть 1 // Компоненты и технологии. 2009. № 6.
3. Шишкин Г., Николаев Д. Селекторы цифровых команд. Часть 2 // Компоненты и технологии. 2009. № 8.