

# Селекторы цифровых команд.

## Часть 1

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

**В первой части статьи рассматриваются базовые технические решения при производстве селекторов цифровых команд с представлением команд параллельным, последовательным, параллельно-последовательным или числоимпульсным кодом. Приводятся результаты анализа основных технических характеристик.**

Селекторы цифровых команд (СК) являются основными функциональными узлами электронных кодовых замков и других устройств, предназначенных для исключения несанкционированного доступа к различным физическим объектам и устройствам хранения конфиденциальной информации.

Выходной сигнал (ВС) разрешения доступа формируется в СК только при поступлении входной команды, соответствующей заданному эталонному значению кода включения. Следовательно, СК должен содержать, по крайней мере, запоминающее устройство (ЗУ) для хранения эталонного значения кода и устройство проверки входного кода на соответствие эталонному значению. Команда на вход СК может поступать в параллельном, последовательном, параллельно-последовательном (например, двоично-десятичном) или числоимпульсном коде. При использовании параллельного кода устройство проверки входного кода может быть выполнено в виде цифрового компаратора (ЦК). Соответствующая схема СК показана на рис. 1а.

В схему может быть введено устройство выбора разрядов (УВР) [1], предназначенное для выбора из  $n$  разрядов входного кода  $m$  контролируемых разрядов, поступающих на вход «В» ЦК, или устройство преобразования кода (УПК) [2, 3], осуществляющее инвертирование отдельных разрядов. Введение УВР способствует уменьшению схемных затрат для реализации ЗУ и ЦК за счет уменьшения

количества разрядов. При использовании УВР (УПК) эталонное значение кода включения определяется совместным действием ЗУ и УВР (УПК), что позволяет скрыть код включения СК от изготовителей ЗУ и УВР (УПК) в отдельности. Скрытию кода включения способствует также изменение порядка подключения разрядов входного кода к входам «В» цифрового компаратора. УПК может быть перенесено в цепь связи ЦК с ЗУ.

В изображенной на рис. 1а схеме обеспечено формирование сигнала ошибки (СО) при несовпадении входного кода с эталонным значением путем проверки состояния ВС во время действия тактового импульса по С-входу. Количество возможных значений эталонного кода  $N = 2^n$ .

Эталонное значение кода в данной схеме формируется путем задания состояния каждого разряда с помощью  $m$ -разрядного ЗУ. Однако эталонное значение кода может быть однозначно сформировано также путем задания состояния одного из разрядов с помощью одноразрядного ЗУ и последовательности смены состояний остальных разрядов. Схема соответствующего СК приведена на рис. 1б, где УЗК — устройство задания эталонного значения кода. УЗК содержит одноразрядное ЗУ и инверторы, обеспечивая инвертирование состояния отдельных разрядов в соответствии со структурой эталонного кода.

ЦК обеспечивает проверку соответствия состояния каждого  $(i+1)$ -го разряда входного кода состоянию  $i$ -го разряда измененного

кода на выходе УЗК, где  $1 \leq i \leq n-1$ ,  $n$  — количество разрядов эталонного значения кода. ЗУ может задавать состояние первого разряда входного кода или состояние  $n$ -го разряда измененного кода. В обоих случаях при смене эталона может потребоваться изменение выходной информации ЗУ, а во втором случае возможно сохранение выходной информации ЗУ при введении или исключении соответствующего инвертора в составе УЗК.

Максимальное количество инверторов в составе УЗК требуется при чередовании состояний логического «0» и логической «1» в эталонном коде. В этом случае для  $m$ -разрядного кода требуется  $(m-1)$  инверторов. Количество инверторов может быть уменьшено до 1 путем разделения всех разрядов кода включения в УПК на две группы с состоянием логического «0» и логической «1» соответственно и подключения одной группы к входам младших разрядов ЦК, а второй группы — к входам старших разрядов. Однако в этом случае необходимо изменять УПК при смене эталонного значения и место включения инвертора при изменении количества разрядов с состоянием логической «1». В представленной схеме поступление тактового импульса на вход СК не требуется. Сигнал, необходимый для формирования СО, создается элементом ИЛИ-НЕ.

Схемные решения СК, показанные на рис. 1, могут использоваться также при представлении входной информации в последовательном коде после преобразования его в па-

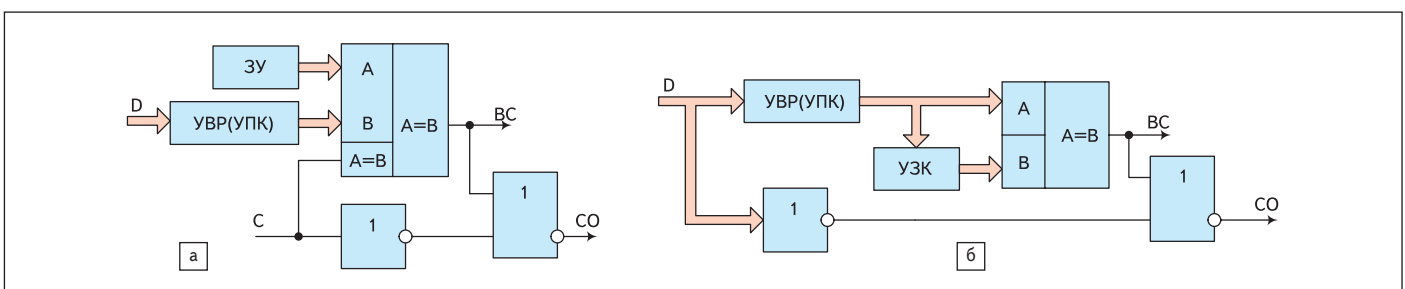


Рис. 1. Способы проверки параллельного кода

раллельный код с помощью схемы на основе регистра с последовательным приемом и параллельной выдачей информации. В схеме может использоваться счетчик тактов (СТ), который разрешает выдачу информации после приема всех разрядов входного кода.

Момент окончания приема кода можно определить без счетчика тактов, если ввести во входной код дополнительный нулевой разряд с записью в него сигнала логической «1». Появление на выходе последнего разряда регистра сигнала логической «1» будет признаком окончания приема входного кода. При этом все разряды регистра при отсутствии тактовых импульсов должны удерживаться в состоянии логического «0». В схеме со счетчиком тактов это не требуется. Сигнал окончания приема входного кода можно использовать для формирования СО.

Преобразователь последовательного кода в параллельный может быть функционально совмещен с УВР и УЗК схемы рис. 1б. Схема соответствующего СК показана на рис. 2а. В данной схеме счетчик тактов обеспечивает запись входной информации одновременно в два регистра RG1 и RG2 преобразования последовательного кода в параллельный. При этом ЗУ совместно с элементом И выполняет функцию УВР, а совместно с элементом «исключающее ИЛИ» — функцию УЗК по преобразованию кода. Способ подключения регистров к ЦК соответствует рис. 1б. Одноразрядное ЗУ на рис. 2а не показано. При этом надо иметь в виду, что изготовителю ЗУ практически известно эталонное значение кода включения СК. Для скрытия кода включения необходимо вместо одного двухразрядного ЗУ использовать два одноразрядных ЗУ от разных изготовителей при наличии выбора разрядов или перемешивание номеров разрядов на входах ЦК.

Схема формирователя импульсов (ФИ) показана на рис. 2б. При отсутствии тактовых импульсов на выходе ФИ присутствует уровень логической «1», удерживающий счетчик тактов в состоянии логического «0». При поступлении первого тактового импульса конденсатор RDC-цепи быстро заряжается, переключая триггер Шмитта в состояние логического «0» и разрешая переключение СТ по заднему фронту тактовых импульсов. Последний тактовый импульс с номером  $n$  вызывает появление на выходе  $Y_n$  сигнала, разрешающего работу цифрового компаратора и формирование сигнала BC или СО. Если последующие тактовые импульсы не поступают, конденсатор RDC-цепи медленно разряжается. При достижении напряжением на конденсаторе порога отпущения триггера Шмитта на выходе ФИ восстанавливается уровень логической «1», сбрасывающий СТ в состояние логического «0». Если же подача входной информации не прекращается, что возможно при попытках подбора кода, то тактовый импульс с номером  $n+1$  запретит формирование сигнала  $Y_n$ , вынудит злоумыш-

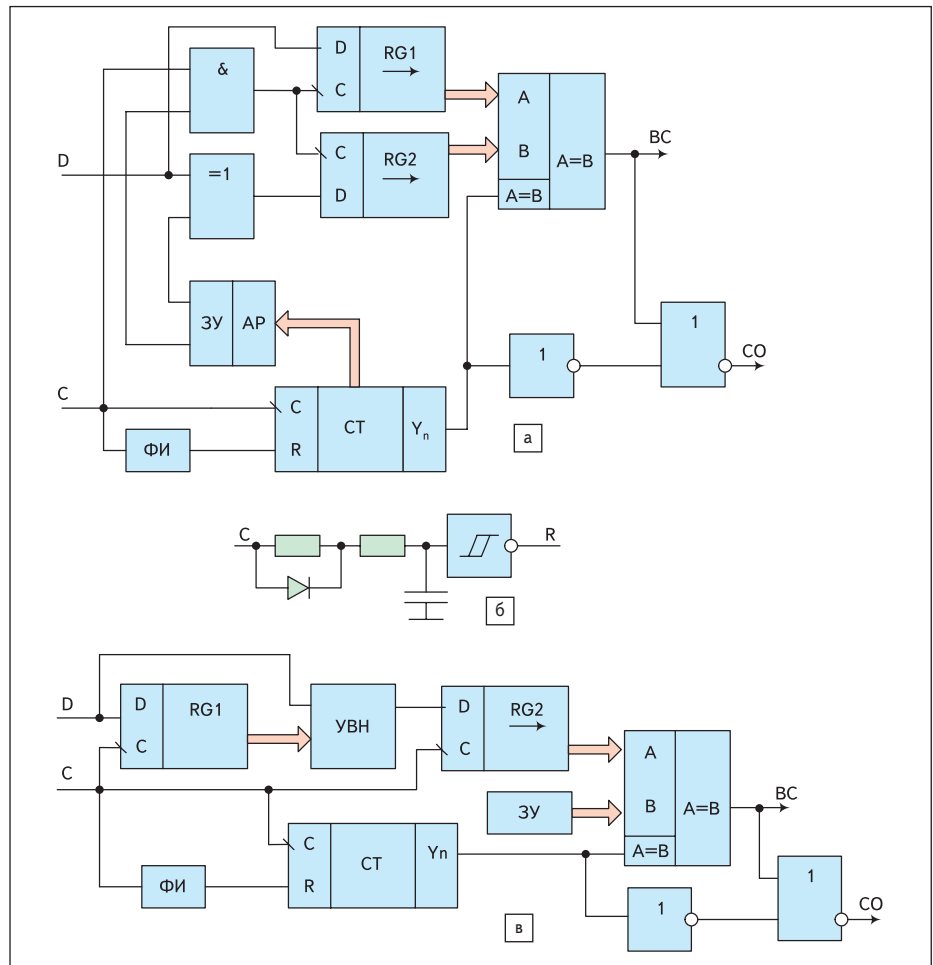


Рис. 2. СК с преобразованием последовательного кода в параллельный

ленника сделать перерыв для обнуления СТ и усложнит процесс подбора кода.

При необходимости с целью упрощения схемы регистр RG2 и элемент «исключающее ИЛИ» можно удалить с установкой дополнительного ЗУ по входу «В» цифрового компаратора аналогично показанному на рис. 1а или с введением УЗК между входами А и В цифрового компаратора в соответствии с рис. 1б. При этом одновременно упрощается схема основного ЗУ.

При проверке последовательного входного кода путем выбора для сравнения с эталоном определенной непрерывной части разрядов аналогично схеме, изображенной на рис. 1а, схема СК может быть трансформирована к виду, показанному на рис. 2в [4], где регистр преобразователя последовательного кода в параллельный разделен на две части. Контролируемая часть разрядов кода задается устройством выбора начального разряда (УВН) входного кода и количеством разрядов регистра RG2. При этом эталонное значение кода включения задается информацией ЗУ и схемой УВН.

В представленных на рис. 2 схемах СК производится одновременный контроль состояния групп разрядов входного кода с помощью цифрового компаратора после приема всех разрядов. При использовании последо-

вательного кода можно производить последовательный поразрядный контроль входной информации с фиксацией сигналов совпадения или сигналов ошибки.

Схема СК с фиксацией сигналов совпадения показана на рис. 3а. Проверка разрядов входного кода производится путем использования элемента «исключающее ИЛИ», опрос состояния которого проводится с помощью элемента И-НЕ во время действия тактового импульса. На выходе элемента И-НЕ формируются сигналы совпадения отрицательной полярности, которые вызывают синхронное со счетчиком тактов переключение счетчика сигналов совпадения (ССС). После приема всех разрядов кода на выходе СТ формируется сигнал  $Y_n$ , который при отсутствии ошибок входного кода, когда состояние СССР совпадает с состоянием СТ, формирует BC, а при наличии ошибок, когда состояние СССР отстает от состояния СТ, формирует СО.

Схема СК с фиксацией ошибок в наборе входного кода показана на рис. 3б [5, 6]. Ошибка в наборе любого разряда входного кода выявляется элементом «исключающее ИЛИ» и во время действия тактового импульса вызывает переключение триггера Т в состояние логической «1». Сигнал переполнения счетчика тактов в зависимости от состояния

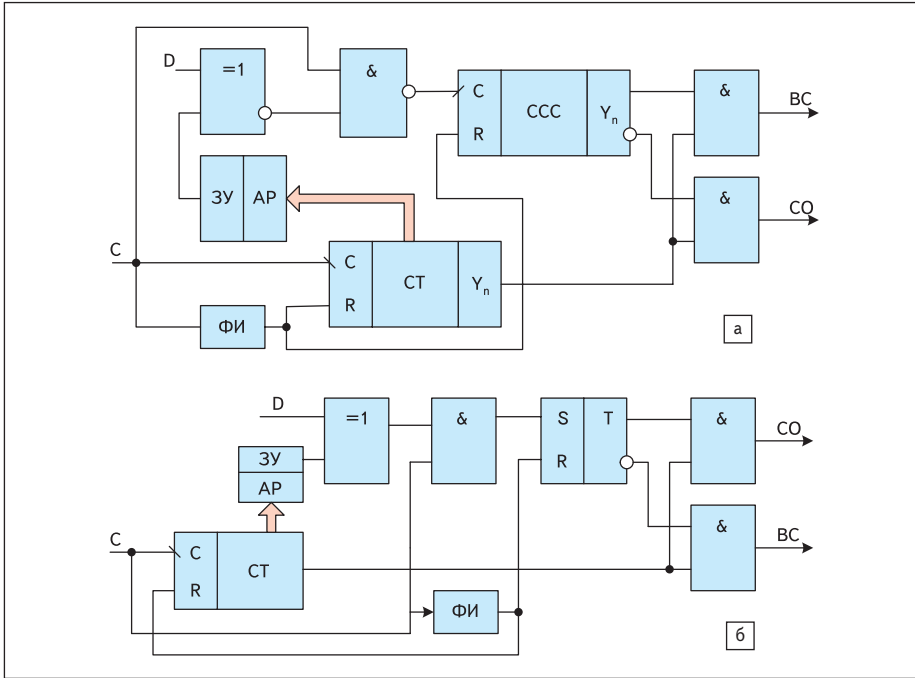


Рис. 3. СК с поразрядной проверкой последовательного кода

триггера Т вызывает формирование ВС или СО. В схеме рис. 3б формирование импульсного выходного сигнала  $Y_n$  не требуется, поскольку введение перерыва в подачу тактовых импульсов диктуется необходимостью сброса в исходное состояние триггера Т.

В схемах рис. 3 момент формирования ВС определяется счетчиком тактов. Ошибки входного кода не влияют на состояние СТ. Формирование ВС запрещается при наличии ошибок счетчиком ССС или триггером Т. На рис. 4 показаны схемы СК, в кото-

рых запрет формирования ВС при наличии ошибок набора кода производится путем воздействия на счетчик тактов. В схеме на рис. 4а [7] ошибка в наборе любого разряда входного кода вызывает установку СТ в исходное состояние логического «0» по заднему фронту тактового импульса выходным импульсом формирователя сброса (ФС). При этом после набора  $n$  разрядов входного кода ВС не формируется. После прекращения подачи тактовых импульсов на выходе ФИ формируется положительный перепад напряжения, вызы-

вающий формирование на выходе элемента совпадения формирователя опроса и сброса (ФОС) импульса опроса состояния ВС с выдчей СО. После окончания импульса опроса уровень логической «1» с выхода ФИ передается на R-вход СТ, устанавливая его в исходное состояние.

Для несанкционированного включения СК в режиме непрерывной подачи входной информации необходимо обеспечить формирование сигнала сброса на выходе ФС перед подачей кода включения, что предъявляет дополнительные требования к алгоритму подбора кода.

Аналогичная схема СК на основе реверсивного счетчика тактов показана на рис. 4б. Счетчик тактов при правильном наборе разрядов входного кода, когда на инверсном входе элемента «исключающее ИЛИ» присутствует уровень логической «1», работает в режиме сложения, а при наличии ошибки переходит в режим вычитания. Схема ФОС приведена на рис. 4а. Для исключения формирования ВС в режиме вычитания переключение счетчика тактовыми импульсами из состояния логического «0» разрешается только в режиме сложения при совпадении входной информации с эталонным значением.

Несанкционированное включение СК в режиме непрерывной подачи информации затруднено необходимостью для любого реального состояния СТ задавать соответствующую часть разрядов кода включения.

В схемах СК на рис. 3 и 4 введение УВР не имеет смысла, поскольку не приводит к уменьшению схемных затрат, использование УЗК невозможно, поскольку оно предполагает наличие параллельных кодов, реализация УПК возможна с помощью дополнительного элемента «исключающее ИЛИ», включаемого по

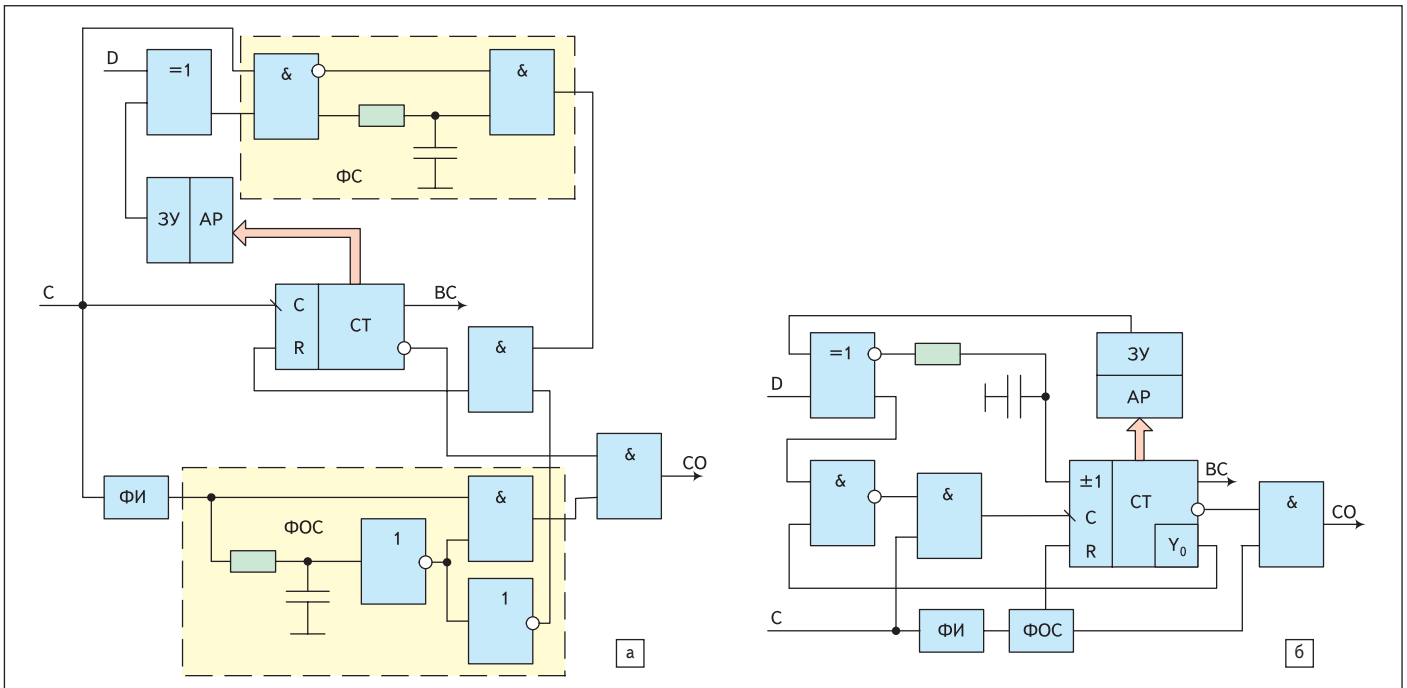


Рис. 4. СК с усложнением проверки сигналом ошибки

D-входу СК, и дополнительного ЗУ, управляемого счетчиком тактов, аналогично схеме, показанной на рис. 2а.

При использовании параллельно-последовательного кода СК может быть построен в соответствии со схемой рис. 1 после преобразования параллельно-последовательного кода в параллельный код. Наименьшие затраты на преобразование требуются при использовании регистров сдвига, количество которых равно количеству параллельных разрядов в каждой группе входного кода, а количество разрядов — количеству параллельных групп. Суммарное количество разрядов регистров равно количеству разрядов входного кода. Однако в этом случае при подключении преобразователей к схемам рис. 1 необходимо учитывать сложившееся распределение номеров разрядов входного кода по разрядам регистров сдвига. Опрос состояния регистров должен производиться с помощью счетчика тактов после приема всех групп входного кода. Аналогичное преобразование входного кода требуется при использовании любой из схем рис. 2. При использовании параллельно-последовательного кода в схемах рис. 3 и 4 требуется замена элементов «исключающее ИЛИ» на цифровые компараторы [5, 6]. При этом уменьшается емкость счетчика тактов.

Для анализа входной информации, поступающей в числоимпульсном коде, необходимо предварительно преобразовать его в параллельный код и использовать одну из схем, представленных на рис. 1 [8, 9]. Соответствующий преобразователь кода может быть выполнен на основе счетчика, который в режиме ожидания удерживается в исходном состоянии логического «0». После начала первого счетного импульса разрешается переключение счетчика по заднему фронту счетных импульсов. После окончания последнего счетного импульса формируется сигнал опроса состояния счетчика и выдача информации на выход. Затем сигнал опроса состояния заканчивается, а счетчик сбрасывается в исходное состояние. Схема формирования сигналов опроса и сброса аналогична показанной на рис. 4а.

Одной из основных технических характеристик СК является степень защищенности от несанкционированного включения, которая оценивается вероятностью несанкционированного включения с первой попытки и объемом массива исчерпывающего перебора вариантов входных кодов, необходимого для гарантированного включения СК. Последовательность вариантов входного кода при исчерпывающем переборе формируется злоумышленником, исходя из знания схемной реализации конкретного селектора. В наихудшем случае злоумышленник знает все параметры схемы, включая количество двоичных разрядов входной команды, кроме эталонного значения кода включения, обнаруживает факт включения СК и обладает неограничен-

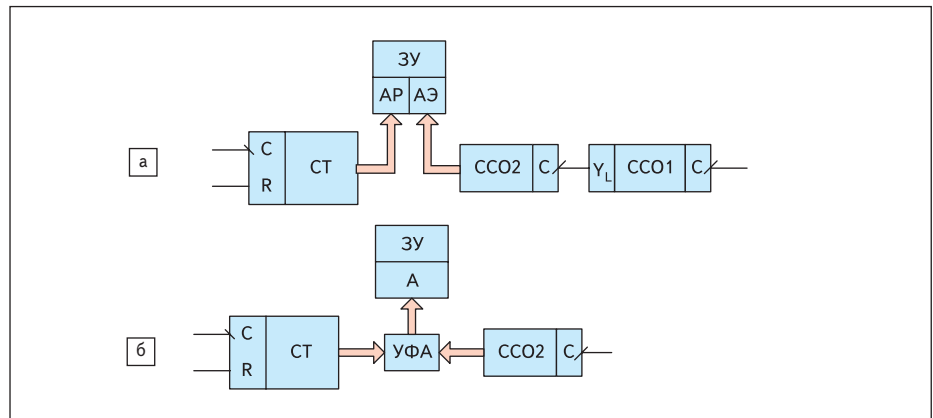


Рис. 5. Способы смены эталонного значения кода

ными возможностями синтеза алгоритмов подбора кода и их практической реализации.

Вероятность  $P_1$  несанкционированного включения СК с первой попытки подбора кода определяется количеством  $m$  контролируемых разрядов и не зависит от количества  $n$  разрядов входного кода. При этом  $P_1 = 1/2^m$ . При изменении  $m$  от  $n$  до 1  $P_1$  изменяется в широком диапазоне от  $1/2^n$  до  $1/2$ .

Объем массива исчерпывающего перебора кодов зависит не только от количества  $m$  контролируемых разрядов, но и от количества  $n$  разрядов входного кода. При этом количество вариантов входного кода, содержащих код включения СК,  $N_b = 2^{n-m}$ , а количество вариантов входного кода, не содержащих код включения,  $N = 2^{n-m} (2^m - 1)$ . Максимальный объем массива исчерпывающего перебора кодов реализуется в наихудшем для злоумышленника случае, когда сначала будут сформированы все варианты кода, не содержащие код включения. При этом  $M = N + 1 = 2^{n-m} (2^m - 1) + 1$ . При изменении  $m$  и  $n$  до 1  $M$  изменяется от  $2^n$  до  $2^{n-1} + 1$  всего лишь в два раза.

Указанные оценки получены с учетом возможности использования для включения СК входного кода, все разряды которого находятся в состоянии логического «0». Исключение данного кода из рассмотрения практически не влияет на полученные результаты.

Дальнейшее рассмотрение способов построения СК проведем для случая контроля всех разрядов входного кода ( $m = n$ ).

Для увеличения массива исчерпывающего перебора кодов в СК необходимо выявить факт подбора кода и усложнить его продолжение. Признаком подбора кода можно считать количество СО, превышающее пороговое значение  $L$ . Для выявления факта подбора вводится счетчик сигналов ошибок набора кода (ССО), который после фиксации допустимого количества ошибок производит смену эталонного значения кода включения или переключение СК в дополнительное состояние блокировки включения.

Смена эталонного значения кода включения может производиться различными способами. При записи в ЗУ нескольких вариан-

тов эталонного значения смена кода может производиться путем изменения адреса выбранного кода выходными сигналами ССО2 [3], как показано на рис. 5а для последовательного входного кода. При этом ССО1 задает пороговое значение количества ошибок. При использовании параллельного кода в схемах рис. 1 смену эталонного значения можно производить воздействием выходными сигналами ССО на УВР [1], УПК [2, 10], УВН [4] или УЗК. В этом случае при построении УПК и УЗК на основе элементов «исключающее ИЛИ» изменяется место включения инверторов. При построении УПК на основе мультиплексоров изменяется порядок подключения разрядов входного кода к входам ЦК. При этом в ЗУ содержится одно значение кода.

При использовании последовательного кода смену эталонного значения можно производить путем изменения последовательности вывода из ЗУ информации о состоянии разрядов одного кода в соответствии с рис. 5б, где УФА — устройство формирования адреса. УФА в данной схеме может быть построено на основе сумматора или отдельных элементов «исключающее ИЛИ». В первом случае в каждом последующем значении эталона по сравнению с предыдущим производится сдвиг номера начального разряда вправо, во втором случае производится перемещение номеров разрядов.

Наихудшая для злоумышленника ситуация при подбore кода будет реализована, когда все  $B$  вариантов кода включения уложатся на последние попытки подбора кода, а действующее значение кода включения будет сформировано последним. В этом случае злоумышленник вынужден проверить каждое из  $2^n$  значений входного кода группами по  $L$  значений на соответствие каждому из  $B$  эталонных значений кода и объем массива исчерпывающего перебора  $M = 2^n \times B$ .

Вероятность несанкционированного включения СК с первой попытки подбора кода  $P_1 = 1/2^n$ .

После неудачных попыток подбора кода ССО может находиться в любом состоянии. При этом для включения СК легальному опе-

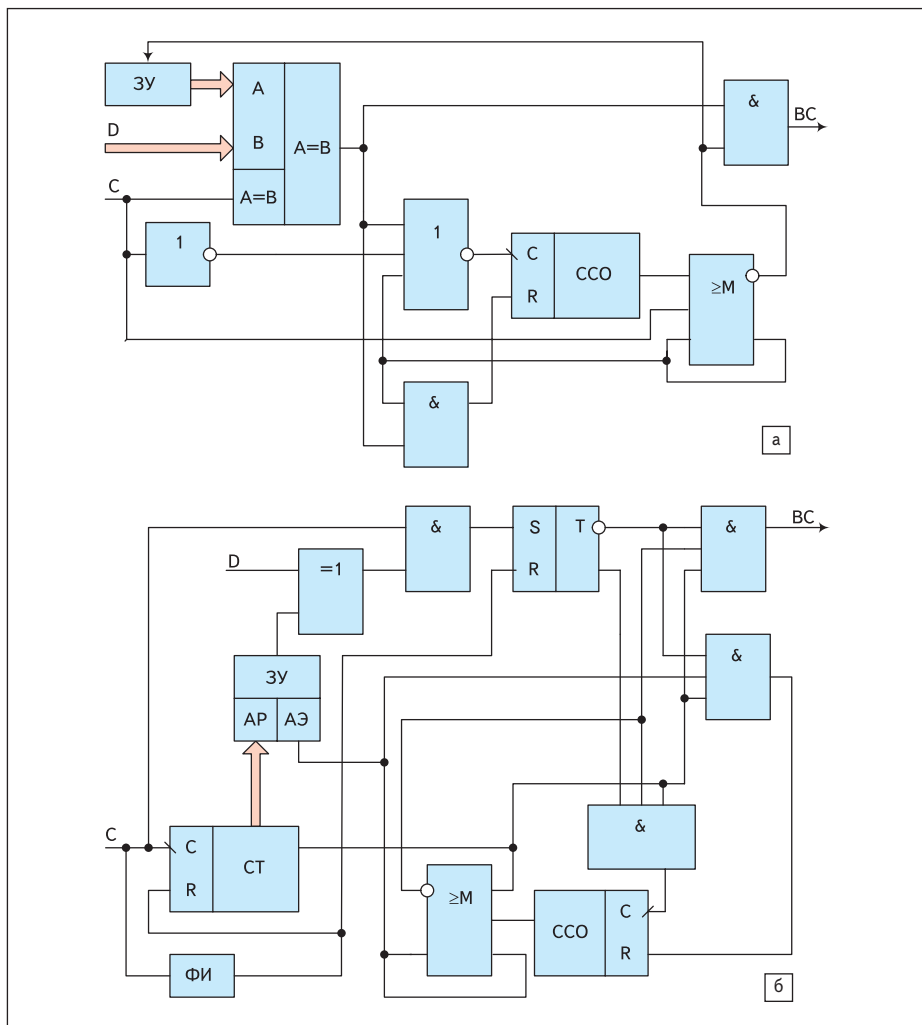


Рис. 6. СК с разрешением сброса счетчика ошибок после блокировки

ратуру, которому известно только одно значение кода включения, в наихудшем случае необходимо повторить его  $(2^L - 1) \times B + 1$  раз, что потребует больших затрат времени. Процесс включения СК упрощается при знании всех  $B$  значений кода включения. При  $B \leq L$  для включения СК в наихудшем случае необходимо последовательно задать один раз все варианты кода включения, начиная, например, с первого, и повторить подачу первого кода включения.

Способы построения СК с блокировкой включения после выявления факта подбора кода показаны на рис. 6 и 7. Разблокировка СК производится путем обнуления ССО.

На рис. 6а приведена схема с управлением параллельным кодом и с возможностью обнуления ССО только после блокировки СК. При этом до блокировки ЗУ выдает на вход ЦК эталонное значение кода включения, а после блокировки — эталонное значение кода разблокировки. Сигнал блокировки формируется с помощью мажоритарного элемента во время действия тактового импульса без задержки после переключения ССО сигналом ошибки и разрешает прохождение выходного сигнала ЦК через элемент

«И» на R-вход ССО. При поступлении кода разблокировки положительный импульс с выхода ЦК обеспечивает обнуление ССО. Мажоритарный элемент снимает блокировку после окончания положительного тактового импульса, запрещая формирование ВС кодом разблокировки и обеспечивая надежное обнуление ССО. При необходимости обнуление ССО можно обеспечивать также при формировании ВС.

Аналогичная изображенной на рис. 6а схема СК с управлением последовательным кодом в соответствии с рис. 3б приведена на рис. 6б.

На рис. 7а [11] приведена схема СК с управлением параллельным кодом и с возможностью обнуления ССО в любой момент времени, в том числе и до блокировки СК. В схеме реализована независимая проверка входного кода на соответствие эталонному значению кода включения с помощью цифрового компаратора ЦКВ и запоминающего устройства ЗУВ и на соответствие эталонному значению кода разблокировки с помощью ЦКР и ЗУР. После блокировки СК запрещены формирование ВС и дальнейшее переключение ССО сигналами ошибки. Для надежной установки

ССО в нулевое состояние необходимо, чтобы тактовый импульс заканчивался не позднее информационных.

Аналогичная приведенной на рис. 7а схема СК с управлением последовательным кодом в соответствии с рис. 3б приведена на рис. 7б. ЗУ формирует эталонные значения разрядов кодов включения и разблокировки. При несоответствии входного кода коду включения переключается в состояние логической «1» триггер Т1, а при несоответствии коду разблокировки — триггер Т2. При несоответствии входного кода ни одному из эталонных значений после приема всех разрядов переключается ССО до состояния блокировки.

В СК с блокировкой включения, соответствующих рис. 7, наиболее простой алгоритм подбора кода состоит из  $N$  циклов, а в каждом цикле с номером  $i$  производится последовательное формирование всех  $N$  возможных вариантов кода включения и перед каждым из них формируется код разблокировки с номером  $i$ . При этом объем массива исчерпывающего перебора  $M = 2N^2$ .

Уменьшение массива исчерпывающего перебора достигается при формировании после каждого значения кода разблокировки группы из  $L$  возможных вариантов кода включения. При этом объем массива исчерпывающего перебора уменьшается до значения  $M = N(N + C) = N^2 + CN$ , где  $C = N/L$  — количество групп кодов включения.

Для дальнейшего уменьшения массива исчерпывающего перебора кодов в рассматриваемых СК представляется целесообразным формирование непрерывной последовательности различных вариантов кодов разблокировки и включения с использованием теории размещений [12].

Способы формирования непрерывной последовательности рассмотрим на простом примере. Допустим, что количество возможных кодов включения равно количеству кодов разблокировки и равно 4, а их совпадение исключено. Обозначим возможные варианты кодов буквами  $a, b, c, d$ . Количество возможных размещений из четырех элементов по два:  $A_4^2 = 12$ :

$ab$	$ba$	$ca$	$da$
$ac$	$bc$	$cb$	$db$
$ad$	$bd$	$cd$	$dc$

Общее количество элементов в приведенных размещении равно  $2A_4^2 = 24$ .

Для наглядного представления способов формирования последовательности кодов использован направленный граф размещений, показанный на рис. 8; вершинами его являются элементы размещений, а ветви, количество которых равно 12, соответствуют размещениям, например, ветвь 1 соответствует размещению  $ab$ , а ветвь 2 — размещению  $ba$ .

При последовательном обходе всех ветвей графа получим последовательность размещений, в которой каждое размещение имеет

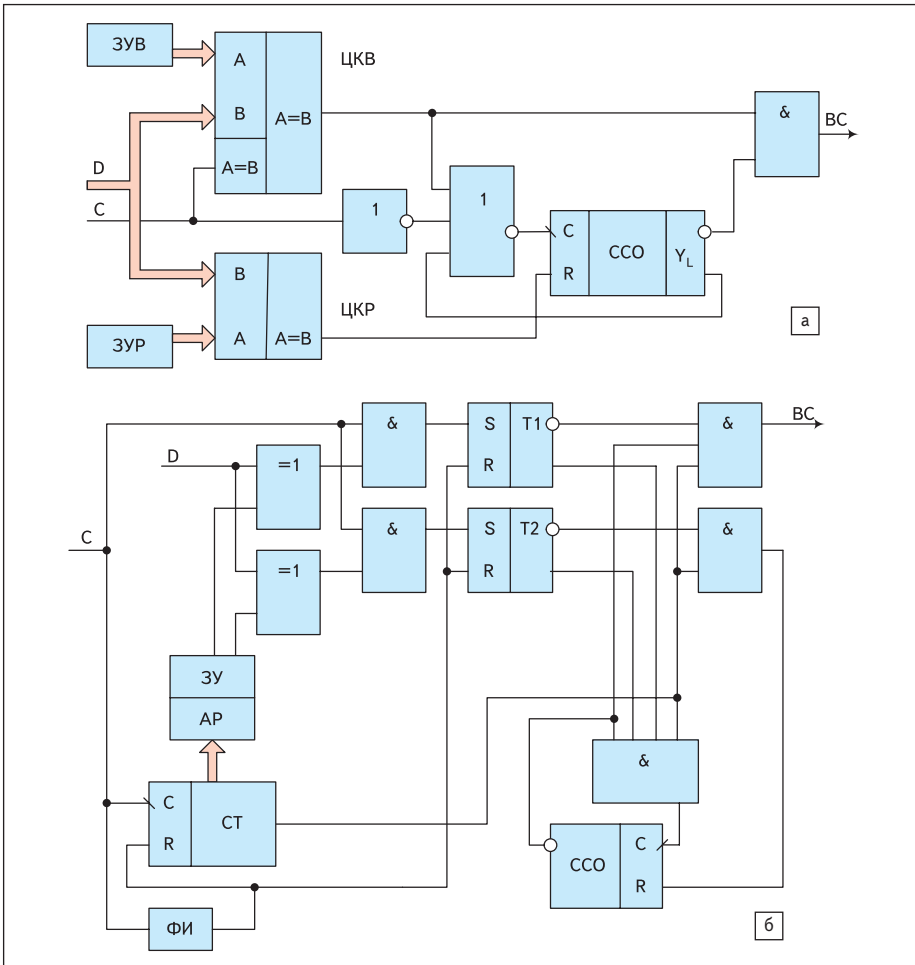


Рис. 7. СК с постоянным разрешением сброса счетчика ошибок

одинаковые соприкасающиеся элементы с размещением справа и слева. Исключив в каждом из размещений по одному из соприкасающихся с последующим размещением элементов, получим искомого последовательность из 13 элементов (кодов).

Количество возможных вариантов формируемой последовательности достаточно велико, но одним из наиболее оптимальных с точки зрения простоты схемной реализации представляется вариант, в котором произво-

дится обход всех вершин графа от *a* до *d* по внешнему контуру в прямом и обратном направлении. При этом на обратном пути до перехода в ближайшую вершину необходимо из каждой вершины сделать заход по очереди во все начальные вершины графа, начиная с *a*, кроме ближайшей вершины, с возвратом в исходную точку. При этом формируется следующая последовательность элементов:

$$a - b - c - d - a - d - b - d - c - a - c - b - a.$$

В этом случае объем массива исчерпывающего перебора  $M = A_N^2 + 1$ , где  $A_N^2 = N(N-1)$  — количество размещений из *N* по 2. Следовательно,  $M = N(N-1) + 1 = N^2 - N + 1$ .

Представленные способы подбора кода применимы в схемах рис. 7 при любом начальном состоянии ССО. При нулевом начальном состоянии ССО можно сначала задать *L* возможных вариантов кода включения. Затем необходимо задать  $(C-1)$  групп по *L* других вариантов кода включения и перед каждой из них задать все возможные варианты кода разблокировки. При этом  $M = L + N^2 + N(C-L-1)$ .

Аналогичный объем массива исчерпывающего перебора кодов при нулевом состоянии ССО требуется и в схемах, приведенных на рис. 6. При ненулевом начальном состоя-

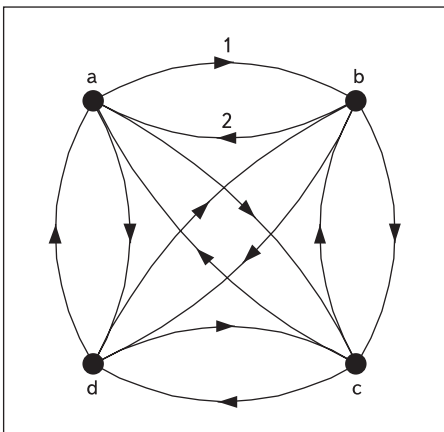


Рис. 8. Граф размещений

нии целесообразно сначала довести ССО до состояния блокировки путем задания *L* раз одного варианта входного кода, не совпадающего с кодом разблокировки, а затем сформировать *C* групп по *L* возможных вариантов кода включения и перед каждой из них задать все возможные варианты кода разблокировки. При этом  $M = L + N^2 + NC$ . Однако положительный результат подбора в этом случае не гарантируется, поскольку первый вариант входного кода может совпасть с кодом разблокировки, хотя вероятность такого совпадения мала.

Для санкционированного включения СК после попыток подбора кода необходимо в наихудшем случае последовательно задать код включения, а затем код разблокировки и код включения.

Продолжение следует

### Литература

1. Патент 2195541РФ, МКИ E05B47/00. Устройство управления электронным кодовым замком / Р. Ф. Зубаеров, В. Н. Фомченко, Г. И. Шишкин // Изобретения. Полезные модели. 2002. № 36.
2. Патент 2159315РФ, МКИ E05B47/00. Электронный кодовый замок / Д. Ю. Борнин, Г. И. Шишкин // Изобретения. Полезные модели. 2000. № 32.
3. Патент 2179224РФ, МКИ E05B49/00. Электронный кодовый замок / Д. Ю. Борнин, Г. И. Шишкин // Изобретения. Полезные модели. 2002. № 4.
4. Патент 2209909РФ, МКИ E05B47/00. Устройство управления электронным замком / Р. Ф. Зубаеров, Г. И. Шишкин // Изобретения. Полезные модели. 2003. № 22.
5. Патент 2154722РФ, МКИ E05B47/00, 49/00. Электронный кодовый замок / А. П. Мартынов, Д. Б. Николаев, Г. И. Шишкин // Изобретения. Полезные модели. 2000. № 23.
6. Патент 2215107РФ, МКИ E05B47/00. Электронный кодовый замок / О. А. Островский, Г. И. Шишкин // Изобретения. Полезные модели. 2003. № 30.
7. Патент 2213191РФ, МКИ E05B47/00. Электронный замок / Р. Ф. Зубаеров, Г. И. Шишкин // Изобретения. Полезные модели. 2003. № 27.
8. Патент 2179223РФ, МКИ E05B49/00. Электронное кодовое устройство / Д. Б. Николаев, В. Н. Фомченко, Г. И. Шишкин // Изобретения. Полезные модели. 2002. № 4.
9. Патент 2224075РФ, МКИ E05B47/00. Электронно-механический замок / А. П. Мартынов, Д. Б. Николаев, В. Т. Сычев, Г. И. Шишкин // Изобретения. Полезные модели. 2004. № 5.
10. Патент 2259455РФ, МКИ E05B49/00. Устройство управления электронного замка / Р. Ф. Зубаеров, Г. И. Шишкин // Изобретения. Полезные модели. 2005. № 24.
11. Патент 2239037РФ, МКИ E05B47/00. Устройство управления электронного замка / Р. Ф. Зубаеров, С. В. Панкратов, Г. И. Шишкин // Изобретения. Полезные модели. 2004. № 30.
12. М. Я. Выгодский. Справочник по элементарной математике. М.: Наука, 1976.