

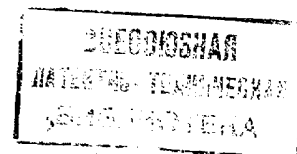


СОЮЗ СОВЕТСКИХ
СОЦИАЛИСТИЧЕСКИХ
РЕСПУБЛИК

(19) SU (11) 1663165 A1

(51)5 E 05 B 47/00

ГОСУДАРСТВЕННЫЙ КОМИТЕТ
ПО ИЗОБРЕТЕНИЯМ И ОТКРЫТИЯМ
ПРИ ГКНТ СССР



ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ

1

(21) 4630076/12
(22) 03.01.89
(46) 15.07.91. Бюл. № 26
(72) С.П.Клокоцкий и М.Н.Бобов
(53) 683.338 (088.8)
(56) Авторское свидетельство СССР
№ 1414959, кл. E 05 B 47/00, 1987.

(54) УСТРОЙСТВО УПРАВЛЕНИЯ КОДОВЫМ ЗАМКОМ

(57) Изобретение относится к устройствам защиты различных объектов от доступа посторонних лиц. Цель — повышение секретности устройства. В блоке 1 памяти ключа хранятся тестовые коды ключа и соответствия (ТКК, ТКС1, ТКС2) и коды идентификации ключа соответствия (КК, КС1, КС2), в блоке 3 памяти замка хранятся коды идентификации (КС1, КС2). В состыкованном состоянии вначале осуществляется в ключе автономное тестирование. Из блока 1 считываются коды ТКК, ТКС1, ТКС2 и в преобразователе 2 кодов ключа формируется результат тестирования, который записывается в регистр 9.

2

При неисправном ключе по окончании тестирования запрещающим сигналом с выхода дешифратора 10 блокируется выдача кодов в ответную часть через элемент И 14, иначе обеспечивается разрешение задачи. Затем осуществляется процесс идентификации. Генератор 5 случайных чисел формирует случайную последовательность ГСЧ. С выхода преобразователя 4 кодов замка через разъем 8, элемент И 12 на вход преобразователя 2 выдается результирующая последовательность кодов КС1, ГСЧ. При положительном результате тестирования (т.е. исправном ключе) с выхода преобразователя 2 в ответную часть выдается результирующая последовательность кодов идентификации ключа КС1, КС2, КК и принятого кода. В преобразователе 4 формируется результирующая последовательность из принятой из ключа и кодов КС2 и ГСЧ. Если коды КС1 и КС2 ключа и ответной части соответственно равны, то в выходной блок 7 поступает код КК, который затем выдается на выход устройства. 7 з.п. ф-лы, 8 ил.

(19) SU (11) 1663165 A1

Изобретение относится к средствам защиты различных объектов от доступа посторонних лиц.

Целью изобретения является повышение секретности.

На фиг. 1 приведена функциональная схема устройства; на фиг. 2 — то же, блока памяти ключа; на фиг. 3 — то же, преобразователя кодов ключа; на фиг. 4 — то же, блока памяти замка; на фиг. 5 — то же, преобразователя кодов замка; на фиг. 6 — то же, гене-

ратора случайных чисел; на фиг. 7 — то же, блока синхронизации; на фиг. 8 — то же, исполнительного блока.

Устройство содержит блок 1 памяти ключа, преобразователь 2 кодов ключа, блок 3 памяти замка, преобразователь 4 кодов замка, генератор 5 случайных чисел, блок 6 синхронизации, исполнительный блок 7, электрический разъем 8, регистр 9, дешифратор 10, триггер 11, первый элемент И 12, второй элемент И 13, третий элемент И 14.

Блоки 1, 2, 9, 10, 11, 12, 13, 14 составляют ключ, блоки 3, 4, 5, 6, 7 — ответную часть.

Блок 1 памяти ключа предназначен для хранения кодов идентификации ключа и тестовых последовательностей и содержит счетчик 15 и блоки 16, 17, 18 памяти, предназначенные для хранения кодов идентификации соответственно кода ключа (КК), первого кода соответствия (КС1), второго кода соответствия (КС2), а также тестовых последовательностей ТКК, ТКС1, ТКС2, приведенных в таблице. В таблице приведен также результат тестирования исправного ключа (РТ).

В качестве блоков памяти могут быть использованы РПЗУ.

Преобразователь 2 кодов ключа предназначен для преобразования кодов идентификации и выдачи их в замаскированном виде. Преобразователь 2 содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ 19, 20, сумматор 21 (одноразрядный накапливающий сумматор).

Блок 3 памяти замка предназначен для хранения кодов идентификации замка. Блок 3 содержит счетчик 22 и блоки 23, 24 памяти, предназначенные для хранения кодов идентификации соответственно первого кода соответствия (КС1) и второго кода соответствия (КС2). В качестве блоков памяти могут быть использованы РПЗУ.

Преобразователь 4 кодов замка предназначен для выдачи в замаскированном виде кода соответствия КС1 и выделения из принимаемой из ключа последовательности кода ключа КК, обеспечивающего доступ на охраняемый объект. Преобразователь 4 содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ 25, 27, сумматор 26 (одноразрядный накапливающий сумматор).

Генератор 5 случайных чисел предназначен для формирования хаотической последовательности двоичных импульсов. Генератор 5 содержит диод 27, усилитель 28, элемент И 29, элемент НЕ 30, счетчик 31, элемент ИСКЛЮЧАЮЩЕЕ ИЛИ 32, D-триггер 33. Сигнал с шумового диода 28 поступает через усилитель 29 на элемент И 30.

При отсутствии тактового сигнала элемент И 30 открыт и импульсы шума подсчитываются в счетчике 32, а затем складываются по модулю два на элементе ИСКЛЮЧАЮЩЕЕ ИЛИ 33. При поступлении тактового импульса элемент И 30 закрывается и в триггер 34 записывается состояние элемента ИСКЛЮЧАЮЩЕЕ ИЛИ 33.

Блок 6 синхронизации предназначен для обеспечения обмена кодами между ключом и ответной частью. Блок 6 синхронизи-

ции содержит генератор 36, делитель частоты 37, регистр сдвига 38, концевой переключатель 39, счетчики 40, 41, триггер 42, элементы И 43, 44, 45. При отсоединении от ответной части ключа концевой переключатель 39 разомкнут и с его выхода на вход регистра 38 поступает сигнал, который устанавливает его в нулевое состояние. По сигналу логического нуля с выхода регистра 38 запрещается прохождение импульсов через элемент И 43, триггер 42 и счетчики 40, 41 устанавливаются в нулевое состояние. На прямых выходах счетчиков 40, 41 устанавливаются запрещающие сигналы, а на инверсном выходе счетчика 40 — разрешающий. Сигналом с выхода регистра 38 устанавливаются в нулевое состояние счетчик адреса, блоки 3 памяти замка, и триггеры сумматора преобразователя 4 кодов замка. При подключении ключа к ответной части срабатывает концевой переключатель 39 и сигнал сброса с его выхода снимается. По импульсам с выхода генератора 36 в регистре 38 продвигается "1" и через некоторое время, большее времени переходного процесса при состыковке ключа с ответной частью, на выходе регистра 38 появляется сигнал 1. По этому сигналу разрешается прохождение импульсов через элемент И 43, счетчики 40, 41 и триггер 42 разблокируется. На выходе триггера 42 формируются сдвинутые на полпериода импульсы. Но на выход блока 6 поступают только импульсы Т1.1. После подсчета необходимого количества импульсов Т1.1 для тестирования ключа на выходе счетчика 39 устанавливается разрешающий сигнал и на выход блока 6 синхронизации через элементы И 45, 44 выдаются импульсы соответственно Т1.2, Т2. Затем после подсчета необходимого количества импульсов для приема кода ключа на прямом выходе счетчика 40 появляется сигнал Т3, разрешающий считывание кода ключа на защищаемый объект.

Исполнительный блок 7 предназначен для приема кода ключа и выдачи его на защищаемый объект. Блок 7 содержит регистр 46 и блок элементов И 47.

Регистр 9 предназначен для приема результата тестирования.

Дешифратор 10 предназначен для формирования разрешающего сигнала при исправном блоке 1 памяти ключа и преобразователе 2 кодов ключа, т.е. если в результате выдачи теста из блока 1 памяти ключа будет выявлено, что в регистре 9 сформирован требуемый код. Дешифратор 10 представляет собой преобразователь двоичного кода в код "1" из "n". В данном случае дешифратор имеет один выход, т.е.

является не полным, так как он в данном случае предназначен для выявления единственного кода, формируемого в регистре 9, соответствующего правильной работе ключа. В соответствии с примером, приведенном в таблице 1, данным кодом будет код 10000110.

Триггер 11 предназначен для блокировки подачи на вход преобразователя 2 кода ключа кодовой последовательности из ответной части (или любого другого устройства) на время тестирования ключа с целью исключения возможности формирования в регистре 9 кода, соответствующему исправному состоянию ключа, в то время как ключ будет находиться в неисправном состоянии. Формирование в регистре 9 требуемого кода при неисправном ключе в конечном счете может привести к компрометации кодов идентификации. По окончании процесса тестирования триггер 11 обеспечивает блокировку поступления продвигающих импульсов в регистр 9.

Первый элемент И 12 предназначен для запрещения приема кода в ключ во время тестирования.

Второй элемент И 13 предназначен для разрешения поступления тактовых импульсов в регистр 9 только во время тестирования ключа.

Третий элемент И 14 предназначен для разрешения выдачи кода из ключа при поступлении разрешающего сигнала с выхода дешифратора 10, т.е. при исправном ключе.

Устройство работает следующим образом.

В исходном состоянии сигналом с выхода блока 6 синхронизации выходной блок 7 закрыт и информация из ответной части на запрашиваемый объект не выдается.

При состыковке ключа с ответной частью срабатывает концевой переключатель блока 6 синхронизации и последний с некоторой задержкой начинает вырабатывать тактовые импульсы Т1.1, которые поступают через электрический разъем 8 в ключ.

Счетчик блока 3 памяти замка устанавливается в исходное состояние, а триггер 11 — в нулевое состояние (не показано).

Импульсы Т1.1 поступают на входы блока 2 памяти кодов ключа, преобразователя 2 кодов ключа и через открытый элемент И 13 (так как с инверсного выхода триггера 11 поступает разрешающий сигнал) на вход регистра 9.

Вначале по импульсам Т1.1 из блока 1 памяти кодов побитно считываются тестовые последовательности первого кода соответствия (ТКС1), второго кода соответствия (ТКС2), кода ключа (ТКК), которые одновременно

поступают на преобразователь 2 кодов ключа. На выходе преобразователя 2 формируется последовательность (результат тестирования РТ), которая по импульсам Т1.1 записывается в сдвигающий регистр 9. По окончании тестирования по сигналу с выхода блока 2 памяти ключа поступает сигнал, который устанавливает триггер 11 в "1", что обеспечивает разрешение прохождения последовательности из ответной части через открытый элемент И 12 на вход преобразователя 2 кодов ключа и запрещение поступления импульсов Т1.1 на вход регистра 9 через элемент И 13. Если результат тестирования равен эталонному, что соответствует исправному ключу, то на выходе дешифратора 10 формируется разрешающий сигнал, который обеспечивает последующую выдачу через элемент И 14 в ответную часть последовательности с выхода преобразователя 2, иначе (результат тестирования не равен эталонному) по запрещающему сигналу с выхода дешифратора 10 осуществляется блокировка последующей выдачи результирующей последовательности с выхода преобразователя 2. По окончании тестирования в дополнение к импульсам Т1.1 блок синхронизации начинает вырабатывать импульсы Т1.2, совпадающие по времени с Т1.1, и импульсы Т2, сдвинутые на полпериода относительно импульсов Т1.1, Т1.2.

По импульсам Т1.1 из блока 1 памяти ключа считываются коды соответствия КС1 и КС2 и код ключа КК, которые одновременно побитно поступают на преобразователь 2 кодов ключа. Одновременно в ответной части по импульсам Т1.2 из блока 3 памяти замка считываются коды соответствия КС1 и КС2 и генератором 5 случайных чисел формируется случайная последовательность (ГСЧ), которая поступает на преобразователь 4 кодов замка. С выхода преобразователя 4 через разъем 8, элемент И 12 на вход преобразователя 4 через разъем 8, элемент И 12 на вход преобразователя 2 кодов ключа поступает результирующая последовательность кода соответствия КС1 и случайной последовательности ГСЧ.

В преобразователе 2 кодов ключа при равенстве кодов соответствия КС1 отделяется случайная последовательность и из последовательностей кода соответствия КС2, кода ключа КК и случайной последовательности ГСЧ формируется результирующая последовательность, которая с выхода преобразователя 2 выдается через открытый элемент И 14 (если результат тестирования равен эталонному), разъем 8 в преобразователь 4 кодов замка. В преобразователе 4

при равенстве кодов соответствия КС2 (при условии, что были равны коды соответствия КС1) ключа и ответной части из результирующей последовательности выделяется код ключа КК в его регистр по импульсам Т2. Если коды соответствия КС1 и КС2 ключа и ответной части не совпадают, то поступающий в выходной блок 7 код ключа будет искажаться и, следовательно, доступа к защищаемому объекту не произойдет. По окончании процесса идентификации блок 6 синхронизации прекращает вырабатывать импульсы Т1.1 и Т1.2, Т2, а формирует сигнал Т3, по которому осуществляется выдача принятого в выходной блок 7 кода на защищаемый объект.

После отсоединения ключа от ответной части сигнал разрешения с выхода блока 6 синхронизации снимается и выдача кода ключа на защищаемый объект прекращается.

Таким образом, в данном устройстве обеспечивается повышение секретности устройства.

В прототипе в результате неисправностей, а именно: при обрыве связи между выходом блока сложения ключа и входом элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, или короткого замыкания на выходе блока сложения, или короткого замыкания на входе элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, соединенного с выходом блока сложения, или других неисправностей, приводящих к аналогичным последствиям, будет происходить выдача кода ключа (или его инверсии), обеспечивающего доступ на охраняемый объект, при подаче на вход ключа любого кода.

В предлагаемом устройстве перед режимом идентификации в ключе осуществляется проверка исправности ключа. Эта проверка заключается в том, что в ключе по тем же шинам, по которым выдаются коды идентификации КС1, КС2, КК, осуществляется выдача тестовых кодов К ТКС1, ТКС2, ТКС3 и формируется результирующая последовательность, которая записывается в регистр. Если результат тестирования представляет собой код, соответствующий неисправной работе ключа, т.е. полученный код отличается от кода, который должен был бы получиться при исправной работе ключа, то на выходе дешифратора будет формироваться запрещающий сигнал и будет производиться блокировка выдачи кодов идентификации из ключа. Следовательно, исключается возможность их компрометации, что и определяет повышение секретности устройства.

Ф о р м у л а и з о б р е т е н и я

1. Устройство управления кодовым замком, содержащее блок синхронизации, первый выход которого соединен с входами блока памяти замка и генератора случайных чисел, электрический разъем, первая пара контактов которого подключена к первому входу блока памяти ключа, элемент И, отличающееся тем, что, с целью повышения секретности, в устройство введены элементы И, преобразователи кодов ключа и замка, триггер, регистр, дешифратор и исполнительный блок, причем первый выход блока синхронизации дополнительно подключен к первому входу преобразователя кода замка, второй и третий входы которого подсоединены к выходам генератора случайных чисел и блока памяти замка, а первый выход через вторую пару контактов электрического разъема соединен с первым входом первого элемента И, вторым входом подключенного к выходу триггера, а выходом – к первому входу преобразователя кодов ключа, второй вход которого подсоединен к первой паре контактов электрического разъема, подключенной к первому входу второго элемента И, при этом первый выход блока памяти ключа подключен к входу триггера, а второй выход – к третьему входу преобразователя кодов ключа, выход которого подключен к первым входам регистра и третьего элемента И, причем выходы регистра соединены с входами дешифратора, выход которого подключен к второму входу третьего элемента И, выходом подсоединенного через третью пару контактов электрического разъема – к четвертому входу преобразователя кодов замка, вторым выходом подключенному к первому входу исполнительного блока, второй вход которого соединен с вторым выходом блока синхронизации, третий выход которого подключен к первой паре контактов электрического разъема, а второй выход триггера соединен с вторым входом второго элемента И выходом соединенного с вторым входом регистра.

2. Устройство по п. 1, отличающееся тем, что блок памяти ключа содержит счетчик и блоки памяти, причем вход счетчика является входом блока памяти ключа, первый выход которого является первым выходом счетчика, N выходов которого являются входами первого, второго и третьего блоков памяти, выходы которых являются вторым выходом блока памяти ключа.

3. Устройство по п. 1, отличающееся тем, что преобразователь кода ключа содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ и сумматор, причем первые входы первого

и второго элементов ИСКЛЮЧАЮЩЕЕ ИЛИ и сумматора являются третьим входом преобразователя кода ключа, выход второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ через сумматор подсоединен к второму входу первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, выход которого является выходом преобразователя кода ключа, а третьи входы сумматора и второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ являются вторым и первым входами преобразователя кода ключа.

4. Устройство по п. 1, отличающееся тем, что генератор случайных чисел содержит шумовой диод, элементы И-НЕ, ИСКЛЮЧАЮЩЕЕ ИЛИ, счетчик, триггер, причем катод шумового диода через усилитель подключен к первому входу элемента И, выходом через счетчик подключенный к входам элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, выход которого подсоединен к первому входу триггера, выход которого является выходом генератора случайных чисел, а второй вход триггера соединен со входом элемента НЕ и является входом генератора случайных чисел, при этом выход элемента НЕ подключен к второму входу элемента И.

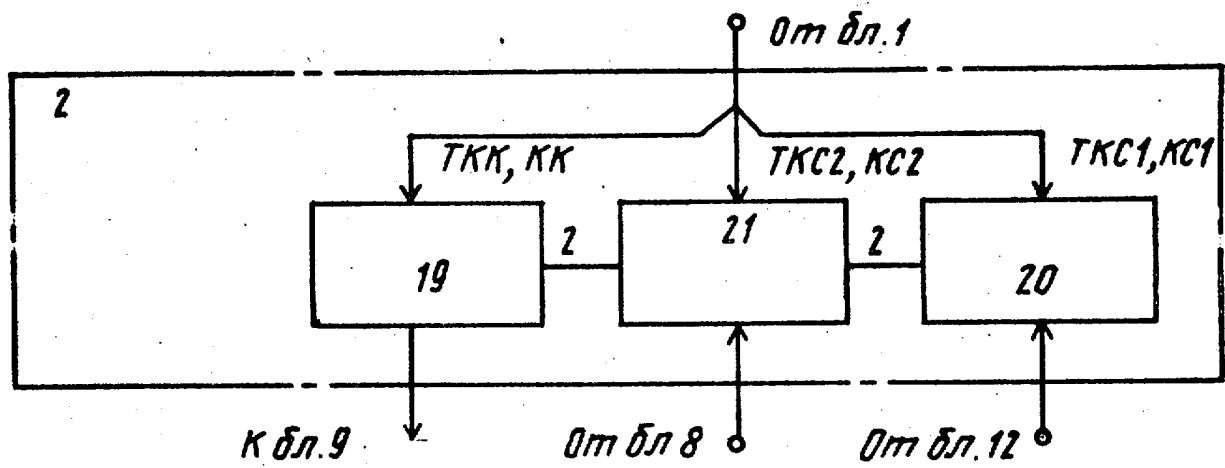
5. Устройство по п. 1, отличающееся тем, что блок синхронизации содержит счетчики, элементы И, триггер, регистр сдвига, генератор, делитель частоты, концевой переключатель, причем выход генератора через делитель частоты подключен к первому входу регистра сдвига, к второму входу которого подключен концевой переключатель, выход регистра сдвига подсоединен к первым входам первого счетчика, первого элемента И, второго счетчика и триггера, выход первого счетчика является вторым выходом блока синхронизации соединенным с выходом второго элемента И и вторым входом первого счетчика, причем второй выход первого счетчика через первый элемент И и триггер подключены к первому входу второго элемента И, второй выход триггера соединен с вторым входом второго счетчика, первым входом третьего элемента И и является третьим выходом блока синхронизации, при этом выход вто-

рого счетчика подключен к вторым входам второго и третьего элементов И, а выход последнего является первым выходом блока синхронизации, при этом второй вход первого элемента И соединен с выходом генератора.

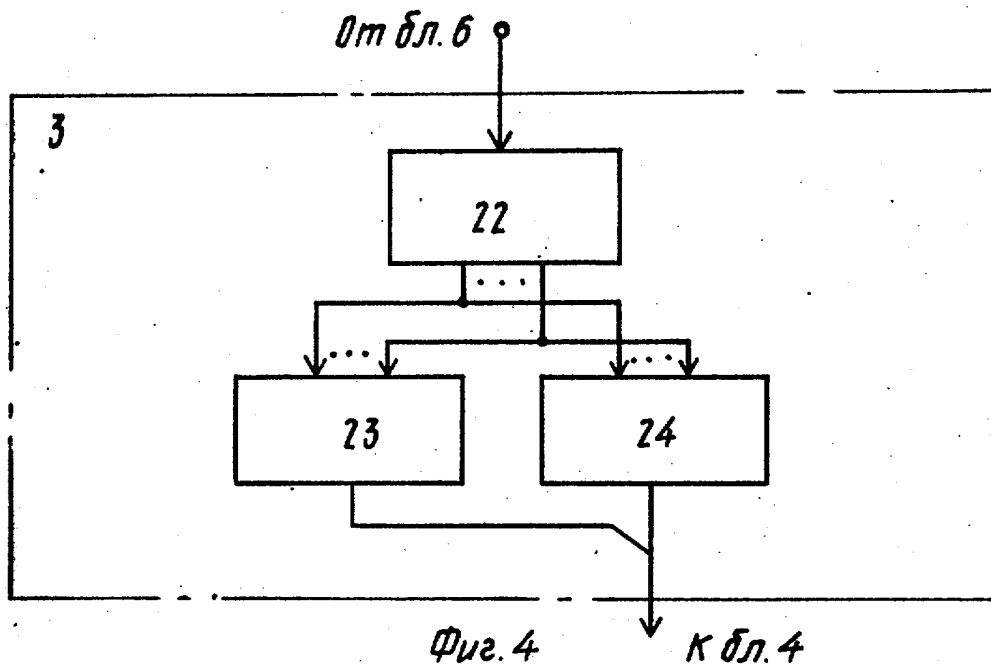
6. Устройство по п. 1, отличающееся тем, что блок памяти замка содержит счетчик и блоки памяти, причем вход счетчика является входом блока памяти замка, выходы счетчика подключены к входам первого и второго блоков памяти, выходы которых соединены и являются выходом блока памяти замка.

7. Устройство по п. 1, отличающееся тем, что преобразователь кода замка содержит элементы ИСКЛЮЧАЮЩЕЕ ИЛИ и сумматор, причем вход первого элемента ИСКЛЮЧАЮЩЕЕ ИЛИ является четвертым входом, а выход - вторым выходом преобразователя кодов замка, второй вход элемента ИСКЛЮЧАЮЩЕЕ ИЛИ через сумматор подключен к первому входу второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, который является вторым входом преобразователя кодов замка, выход второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ, который является вторым входом преобразователя кодов замка, выход второго элемента ИСКЛЮЧАЮЩЕЕ ИЛИ является первым выходом преобразователя кодов, причем второй вход элемента ИСКЛЮЧАЮЩЕЕ ИЛИ и второй вход сумматора соединены между собой и являются третьим входом преобразователя кода замка, при этом третий вход сумматора является первым входом преобразователя кодов замка.

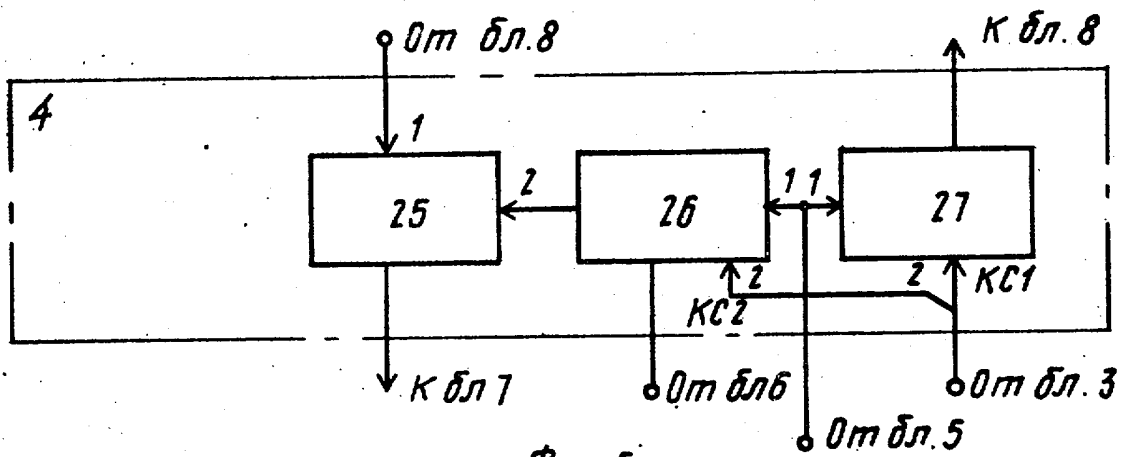
8. Устройство по п. 1, отличающееся тем, что исполнительный блок содержит регистр и блок элементов И, причем первый вход регистра является первым входом исполнительного блока, а второй вход регистра и первый вход блока элементов И соединены между собой являются вторым входом исполнительного блока, а выходы блока элементов И являются выходами исполнительного блока.



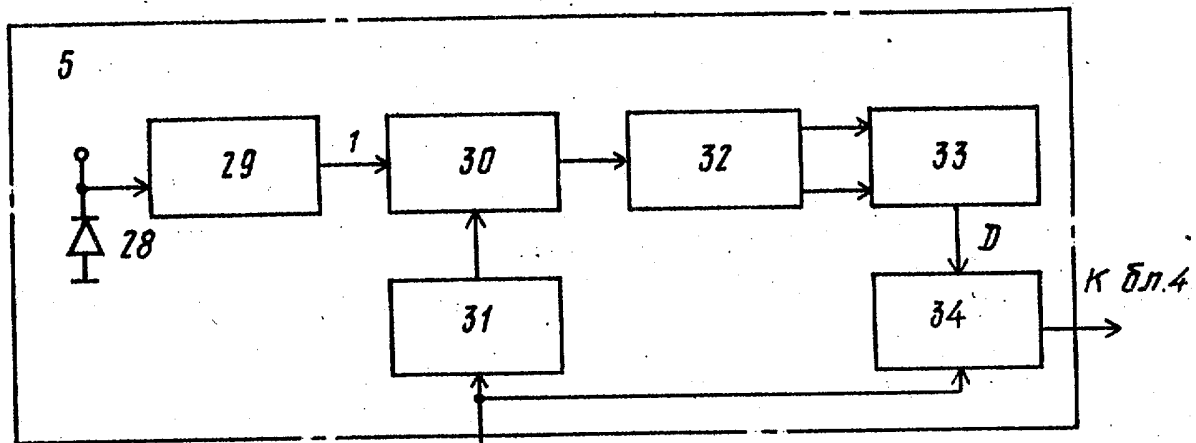
Фиг. 3



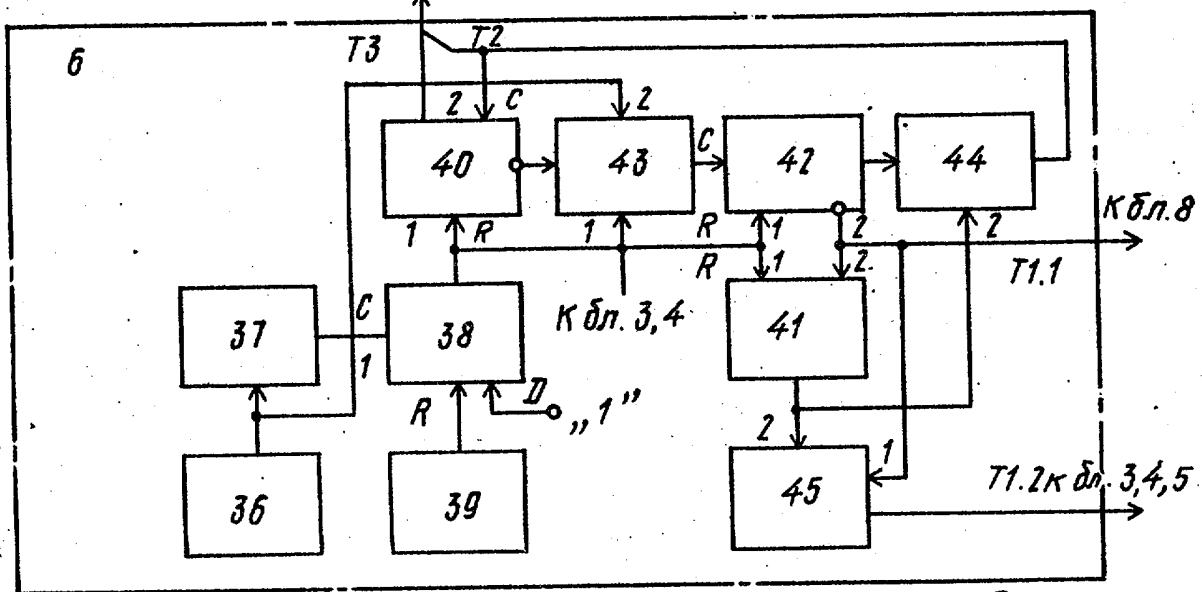
Фиг. 4



Фиг. 5



Фиг.6
К бл.7



Фиг.7
От бл.4

