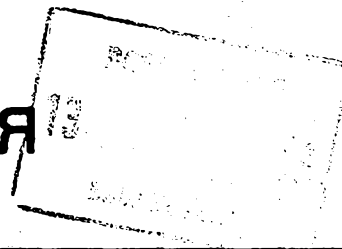




4(51) G 06 F 3/02

ГОСУДАРСТВЕННЫЙ КОМИТЕТ СССР
ПО ДЕЛАМ ИЗОБРЕТЕНИЙ И ОТКРЫТИЙ

ОПИСАНИЕ ИЗОБРЕТЕНИЯ К АВТОРСКОМУ СВИДЕТЕЛЬСТВУ



(21) 3643105/24-24

(22) 19.09.83

(46) 23.01.85. Бюл. № 3

(72) Г.А.Семавин и С.П.Клокоцкий

(53) 681.327.11(088.8)

(56) 1. Авторское свидетельство СССР
№ 960784, кл. G 06 F 3/02, 1981.

2. Авторское свидетельство СССР
по заявке № 3508263/24,
кл. G 06 F 3/02, 26.05.83 (прототип).
(54)(57) УСТРОЙСТВО ДЛЯ ВВОДА ИНФОР-
МАЦИИ, содержащее первый блок памяти,
первый блок сравнения, первый и вто-
рой регистры, шифратор, формирова-
тель импульсов сдвига, клавиатуру,
блок индикации, элемент 1 НЕ-И, счет-
чик, таймер, первый элемент И, эле-
мент ИЛИ, группу элементов И, выходы
первого блока памяти подключены
к входам первой группы первого блока
сравнения, вход которого и вторые
выходы элементов И группы подключены
к первому выходу счетчика, первый
вход которого подключен к выходу эле-
мента 1 НЕ-И, первые входы которого,
таймера и первого элемента И подклю-
чены к выходу первого блока сравне-
ния, первый выход таймера подключен
к первым входам элементов И группы,
третьи входы которых подключены
к выходам первой группы клавиатуры,
выходы второй группы которой подклю-
чены к входам шифратора и формирова-
теля импульсов сдвига, выход которо-
го подключен к третьему входу перво-
го регистра, входы группы которого
подключены к выходам шифратора, вы-
ходы элементов И группы подключены
к входам группы второго регистра,
выходы группы которого являются выхо-

дами второй группы устройства и под-
ключены к входам элемента ИЛИ, вы-
ход которого является вторым выходом
устройства, вторые входы первого
и второго регистров объединены и яв-
ляются вторым входом устройства, пер-
вые входы регистров и вторые входы
таймера и счетчика объединены и яв-
ляются первым входом устройства,
четвертый вход счетчика подключен
к выходу первого элемента И, второй
выход таймера подключен к входу
блока индикации, выходы первой
группы первого регистра являются
выходами первой группы устройства,
отличающееся тем, что,
с целью повышения надежности уст-
ройства путем повышения эффектив-
ности защиты от несанкционирован-
ного доступа, в него введены вто-
рой блок памяти, второй блок срав-
нения, элемент задержки, второй эле-
мент И, выходы второго блока памяти
подключены к входам первой группы
второго блока сравнения, входы второй
группы которого и второй группы пер-
вого блока сравнения подключены к вы-
ходам второй группы первого регистра,
выход второго блока сравнения подклю-
чен к второму входу второго элемен-
та И, первый вход которого, второй
вход первого элемента И, третий вход
таймера, второй вход элемента 1 НЕ-И
подключены к выходу клавиатуры, вход
второго блока сравнения подключен
к выходу элемента задержки, вход кото-
рого подключен к выходу блока индика-
ции и второму выходу счетчика, кото-
рые являются первым выходом устройст-
ва.

(19) **SU** (11) **1136142** **A**

Изобретение относится к вычислительной технике и предназначено для ввода информации в ЭВМ.

Известно устройство для ввода информации, содержащее блок памяти, блок индикации, блок сравнения, таймер, два регистра, два элемента ИЛИ, шифратор, блок элементов И, элемент задержки, клавиатуру [1].

К недостаткам устройства относится значительная вероятность несанкционированного его использования, определяемая вероятностью подбора пароля за фиксированный интервал времени.

Наиболее близким к предлагаемому является устройство, содержащее первый блок памяти, первый блок сравнения, первый и второй регистры, шифратор, формирователь импульсов сдвига, клавиатуру, блок индикации, элемент 1 НЕ-И, счетчик, таймер, первый элемент И, элемент ИЛИ, группу элементов И, выходы первого блока памяти подключены к входам первой группы первого блока сравнения, вход которого и второй вход группы элементов И подключены к первому выходу счетчика, первый вход которого подключен к выходу элемента 1 НЕ-И, первые входы которого, таймера и первого элемента И подключены к выходу первого блока сравнения, первый выход таймера подключен к первому входу группы элементов И, входы группы которой подключены к выходам первой группы клавиатуры, выходы второй группы которой подключены к входам шифратора и формирователя импульсов сдвига, выход которого подключен к третьему входу первого регистра, входы группы которого подключены к выходам шифратора, выходы группы элементов И подключены к входам группы второго регистра, выходы группы которого являются выходами второй группы устройства и подключены к входам элемента ИЛИ, выход которого является вторым выходом устройства, вторые входы первого и второго регистров объединены и являются вторым входом устройства, первые входы регистров и вторые входы таймера и счетчика объединены и являются первым входом устройства, четвертый вход счетчика подключен к выходу первого элемента И, второй выход тай-

мера подключен к входу блока индикации, выходы первой группы первого регистра являются выходами первой группы устройства [2].

Недостатком известного устройства является невысокая надежность защиты от несанкционированного доступа, т.е. блокировка ввода пароля осуществляется на фиксированный интервал времени, который не должен быть очень большим для обеспечения высокой оперативности готовности устройства по вводу паролей и сообщений. Но при малом времени блокировки (при отключении, выходе из строя системы сигнализации или ее отсутствии) обеспечивается большая скорость подбора пароля, что определяет недостаточную надежность защиты от несанкционированного доступа.

Цель изобретения - повышение надежности устройства путем повышения эффективности защиты от несанкционированного доступа.

Поставленная цель достигается тем, что в устройство для ввода информации, содержащее первый блок памяти, первый блок сравнения, первый и второй регистры, шифратор, формирователь импульсов сдвига, клавиатуру, блок индикации, элемент 1 НЕ-И, счетчик, таймер, первый элемент И, элемент ИЛИ, группу элементов И, выходы первого блока памяти подключены к входам первой группы первого блока сравнения, вход которого и вторые входы элементов И группы подключены к первому выходу счетчика, первый вход которого подключен к выходу элемента 1 НЕ-И, первые входы которого, таймера и первого элемента И подключены к выходу первого блока сравнения, первый выход таймера подключен к первым входам элементов И группы, третьи входы которых подключены к выходам первой группы клавиатуры, выходы второй группы которой подключены к входам шифратора и формирователя импульсов сдвига, выход которого подключен к третьему входу первого регистра, входы группы которого подключены к выходам шифратора, выходы элементов И группы подключены к входам группы второго регистра, выходы группы которого являются выходами второй группы устройства и подключены к входам элемента ИЛИ, выход которого является вторым выходом устройства, вторые

входы первого и второго регистров объединены и являются вторым входом устройства, первые входы регистров и вторые входы таймера и счетчика объединены и являются первым входом устройства, четвертый вход счетчика подключен к выходу первого элемента И, второй выход таймера подключен к входу блока индикации, выходы первой группы первого регистра являются выходами первой группы устройства, введены второй блок памяти, второй блок сравнения, элемент задержки, второй элемент И, выходы второго блока памяти подключены к входам первой группы второго блока сравнения, входы второй группы которого и второй группы первого блока сравнения подключены к выходам второй группы первого регистра, выход второго блока сравнения подключен к второму входу второго элемента И, первый вход которого, второй вход первого элемента И, третий вход таймера, второй вход элемента 1 НЕ-И подключены к выходу клавиатуры, вход второго блока сравнения подключен к выходу элемента задержки, вход которого подключен к выходу блока индикации и второму выходу счетчика, которые являются первым выходом устройства.

На фиг. 1 представлена блок-схема устройства для ввода информации; на фиг. 2 - блок-схема первого блока сравнения; на фиг. 3 - блок-схема таймера.

Устройство содержит первый блок 1 памяти, первый блок 2 сравнения, второй блок 3 памяти, второй блок 4 сравнения, первый регистр 5, шифратор 6, формирователь 7 импульсов сдвига, клавиатуру 8, элемент 9 задержки, блок 10 индикации, элемент 1 НЕ-И 11, счетчик 12, таймер 13, первый элемент И 14, второй элемент И 15, второй регистр 16, элемент ИЛИ 17, группу 18 элементов И, второй вход 19 устройства, первый вход 20 устройства, информационные выходы 21 устройства, командные выходы 22 устройства, первый выход 23 устройства, второй выход 24 устройства.

Первый блок 2 сравнения содержит элементы "Равнозначность" 25.1-25.к, элемент ИЛИ 26.

Таймер 13 содержит генератор 27 постоянной частоты, элемент И 28, счетчик 29, элемент И 30.

Блок 1 памяти предназначен для хранения эталонного пароля (П1), по которому разрешается доступ к выполнению команд, и может быть выполнен, например, на тумблерах.

Блок 2 сравнения предназначен для сравнения эталонного пароля П1, хранимого в блоке 1 памяти, и пароля, набираемого на клавиатуре 8, и может быть выполнен по схеме, представленной на фиг. 2.

Второй блок 3 памяти предназначен для хранения пароля П2, предназначенного для разблокировки устройства, которая происходит после предельно допустимого числа наборов паролей, не равных паролю П1, и может быть выполнен аналогично блоку 1 памяти.

Второй блок 4 сравнения предназначен для сравнения эталонного пароля П2, хранимого в блоке 3 памяти, и пароля, набираемого на клавиатуре 8, и может быть выполнен аналогично блоку 2 сравнения.

Первый регистр 5 предназначен для хранения набираемых паролей (П1 и П2) или для хранения информационных частей сообщений, набираемых на клавиатуре 8.

Шифратор 6 предназначен для преобразования десятичного числа в двоично-десятичный код.

Формирователь 7 импульсов сдвига предназначен для формирования импульсов сдвига и может содержать элемент ИЛИ, подключенный к входу элемента задержки. Входы элемента ИЛИ являются входами формирователя 7, а выход элемента задержки - выходом формирователя. Он эквивалентен первому элементу ИЛИ и элементу задержки известного устройства.

Клавиатура 8 предназначена для набора информационной и командной частей сообщений, а также для набора паролей П1 и П2 и содержит переключатели для набора информационной части сообщений, которые одновременно служат для набора паролей П1 и П2, переключатель для ввода паролей и переключатели для набора команд.

Элемент 9 задержки предназначен для устранения добавления ложных

логических "1" в счетчик 12 с выхода элемента 11 при наборе пароля, равного П2. При отсутствии элемента 9 задержки после набора пароля, равного П2, возможно после сброса счетчика 12 сигналом с выхода элемента И 15 добавление ложной "1" в счетчик 12 с выхода элемента 1НЕ-И 11.

Блок 10 индикации предназначен для отображения состояния устройства, при котором необходимо произвести повторный ввод пароля П1, и состояния, при котором осуществлена блокировка ввода пароля П2. Блок индикации состоит из двух элементов индикации, каждый из которых может содержать транзистор с лампой в цепи коллектора и резистор в цепи базы. Первый элемент блока подключен к выходу счетчика 12, а второй - к выходу таймера 13.

Элемент 1НЕ-И 11 предназначен для запрещения прохождения сигнала от переключателя ввода пароля блока 8 коммутационных элементов в счетчик 12 при наличии сигнала логической "1" с выхода блока 2 сравнения.

Счетчик 12 предназначен для подсчета числа вводов паролей, не равных П1, и может представлять собой сдвигающий регистр, в котором вход сигнала сдвига подключен к выходу элемента 1НЕ-И 11. На информационный вход регистра подается логическая "1" (не показано). Прямой выход счетчика 12 (шина 24) является выходом устройства, подключаемым к системе сигнализации (не показана).

Таймер 13 предназначен для выработки интервалов времени, по истечении которых необходимо производить повторный ввод пароля П1, обеспечивающих выполнение команд, и может быть выполнен по схеме, представленной на фиг. 3.

Таймер 13 работает следующим образом.

При наличии логического "0" на инверсном выходе счетчика 29 импульсы от генератора 27 постоянной частоты на счетный вход счетчика 29 не поступают. При поступлении сигнала с блока 2 сравнения и нажатии переключателя ввода пароля блока 8 происходит сброс счетчика 29 в "0", на инверсном выходе которого устанавливается сигнал "1", который открывает

элемент 28 И. Счетчик 29 подсчитывает импульсы от генератора 27. При установке логической "1" на прямом выходе счетчика 29 (на инверсном выходе - логический "0") поступление импульсов на вход счетчика 29 прекращается. Таким образом, таймер 13 выдает на блок 10 индикации команды "Повтор пароля П1" через фиксированные интервалы времени.

Элементы И 14 и 15 предназначены для формирования сигналов сброса счетчика 12, второй регистр 16 - для хранения командных частей сообщений, набираемых на блоке 8 коммутационных элементов, элемент ИЛИ 17 - для формирования сигнала "Готовность", передаваемого в ЭВМ.

Группа 18 элементов И предназначена для блокировки записи команд в регистр 16 по истечении времени действия пароля П1 и может содержать элементы И, первые входы которых соединены с выходами блока 8, вторые входы соединены и подключены к выходу счетчика 12, третьи входы соединены и подключены к выходу таймера 13, а выходы соединены с входами регистра 16.

Устройство работает следующим образом.

При включении питания сигналом с входа 20 сбрасываются в "0" регистры 5 и 16, а счетчик 12 и счетчик 29 таймера 13 устанавливаются в "1". Сигналом логического "0" с инверсного выхода счетчика 12 запрещается работа блока 2 сравнения и ввод команд в регистр 16 через группу 18 элементов И. Кроме того, запрет ввода команд в регистр 16 подтверждается сигналом логического "0" с инверсного выхода таймера 13.

По сигналам с прямых выходов счетчика 12 и таймера 13 включаются оба элемента индикации блока 10, сигнализирующие о необходимости ввода паролей П1 и П2. Сигналом с прямого выхода счетчика 12 через элемент 9 разрешается также сравнение паролей в блоке 4. Этот же сигнал поступает по шине 24 в систему сигнализации (не показана).

Лицо, ответственное за доступ к ресурсам ЭВМ, производит ввод пароля П2, обеспечивающего разрешение сравнения набираемого пароля с паролем П1. Ввод пароля П2 осуществляет-

ся следующим образом. При нажатии переключателей клавиатуры 8 преобразованная шифратором 6 в двоично-десятичный код информация по сигналам с выхода формирователя 7 импульсов сдвига заносится в регистр 5 сдвига. При совпадении введенного пароля с эталонным П2, хранимым в блоке 3 памяти, блок 4 сравнения выдает на элемент И 15 разрешающий сигнал (логическую "1"). После нажатия переключателя ввода пароля клавиатуры 8 сигналом с выхода элемента И 15 счетчик 12 устанавливается в нулевое состояние. При этом по сигналу логической "1", поступающему с инверсного выхода счетчика 12, разрешается работа блока 2 сравнения. Этим же сигналом подготавливается группа 18 элементов И к передаче команд. Сигнал логического "0", поступающий с прямого выхода счетчика 12, через элемент 9 задержки запрещает работу блока 4 сравнения, выключает элемент индикации блока 10 и, поступающая по шине 24, включает систему сигнализации.

После этого пользователь перед вводом команд набирает пароль П1, знаки которого, аналогично описанному выше, заносятся в регистр 5. При совпадении введенного пароля с паролем П1, хранимым в блоке 1 памяти, блок 2 сравнения выдает на вход таймера 13 разрешающий сигнал логической "1". После нажатия переключателя ввода паролей клавиатуры 8 таймер 13 выдает разрешающий сигнал на группу 18 элементов И, который разрешает прохождение команд с клавиатуры 8 на регистр 16. Одновременно гасится элемент индикации блока 10, который предназначен для отображения состояния устройства, при котором необходимо произвести ввод пароля П1. После этого оператор может набирать информационную и командную части сообщений на клавиатуре 8.

Набор информационной части сообщения осуществляется нажатием переключателей, предназначенных для ввода информационной части сообщения, которая записывается в регистр 5. Набор командной части сообщений осуществляется нажатием переключателей, предназначенных для ввода командной части сообщения. При этом команды через открытую группу 18

элементов И записываются в регистр 16. На выходе 23 устройства устанавливается сигнал "Готовность", по которому ЭВМ принимает сообщение по шинам 21 и 22. После приема сообщения ЭВМ обнуляет регистры 5 и 16 по входу 19.

По истечении фиксированного интервала времени на инверсном выходе таймера 13 устанавливается запрещающий сигнал (логический "0"), который блокирует ввод команд с клавиатуры 8. Одновременно сигналом логической "1" с прямого выхода таймера 13 включается элемент индикации блока 10. Для дальнейшей работы устройства необходимо произвести повторный ввод пароля П1.

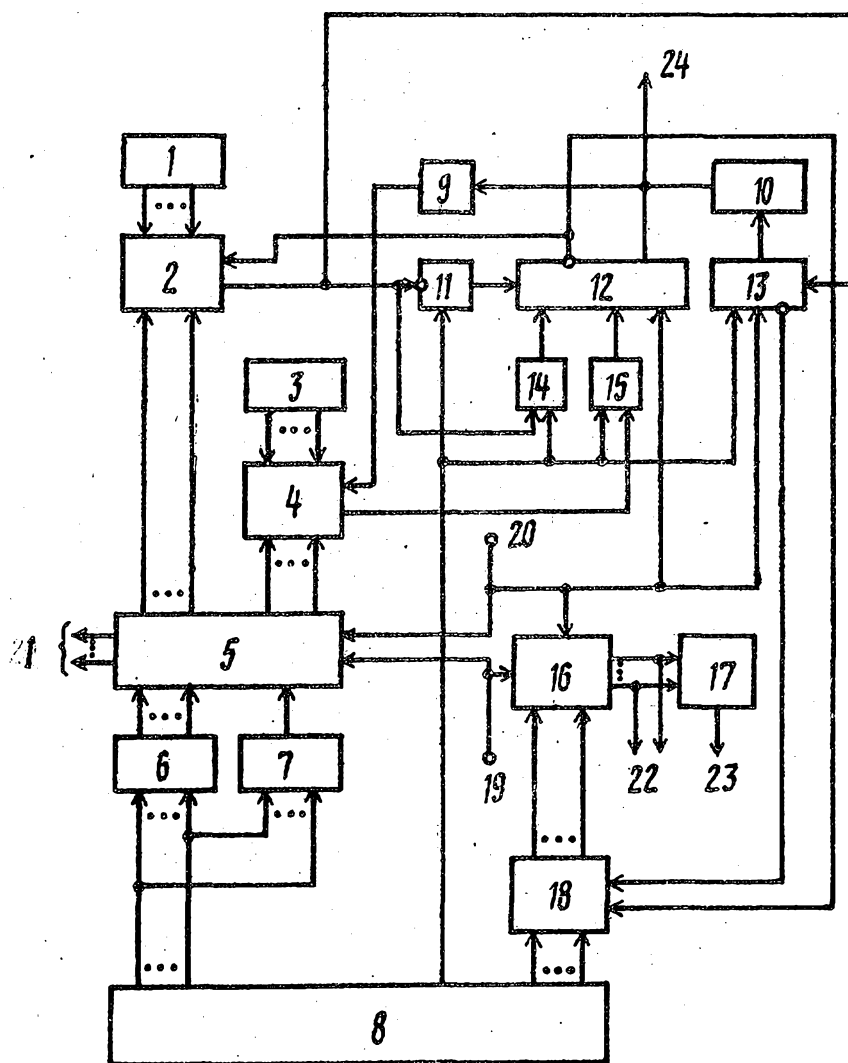
При правильном наборе пароля П1 подтверждается нулевое состояние счетчика 12 сигналом с выхода элемента И 14 и перезапуск таймера 13. Если произойдет набор кода, не равного паролю П1, то с выхода блока 2 сравнения на инверсный вход элемента 11 поступит разрешающий сигнал (логической "0") и при нажатии переключателя ввода паролей блока 8 через второй вход элемента ИЕ-И 11 на синхровход счетчика 12 поступит сигнал, который на единицу увеличит состояние счетчика 12. После нескольких вводов кодов, не равных паролю П1, на инверсном выходе счетчика 12 устанавливается сигнал логического "0", который запрещает работу блока 2 сравнения и блокирует группу 18 элементов И. Одновременно по сигналу логической "1", поступающему с прямого выхода счетчика 12, разрешается работа блока 4 сравнения и включается элемент индикации блока 10 индикации, сигнализирующий о необходимости ввода пароля П2.

В базовом объекте производится блокировка ввода паролей на фиксированный интервал времени после вводов ложных паролей. Но если блокировка осуществляется на большой интервал времени (15-30 мин), что обеспечивает низкую скорость подбора паролей и, следовательно, высокую надежность защиты устройства от несанкционированного доступа, то базовый объект будет иметь низкую оперативность готовности устройства к вводу паролей и сообщений, так как при

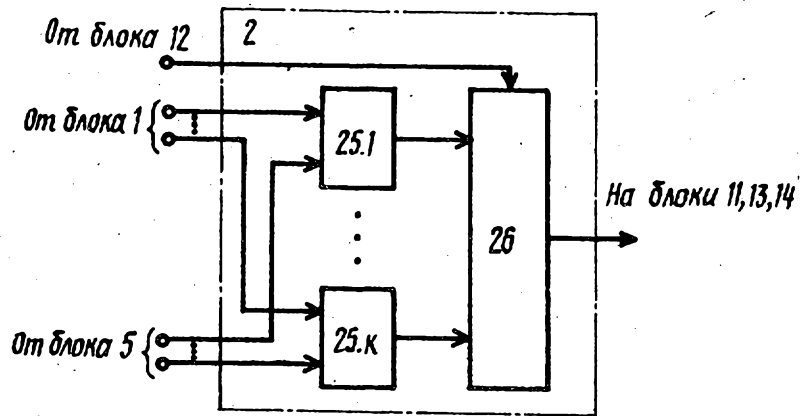
включении напряжения питания устройство блокируется. Если блокировка осуществляется на небольшой интервал времени (1-2 мин), то устройство будет иметь высокую оперативность готовности к вводу паролей и сообщений, но при этом обеспечивается также высокая скорость подбора паролей и, следовательно, низкая надежность защиты устройства от несанкционированного доступа.

В отличие от базового объекта в предлагаемом устройстве путем введения второго блока памяти, второго блока сравнения, второго элемента И и элемента задержки осуществляется блокировка ввода пароля П1, предназначенного для получения разрешения

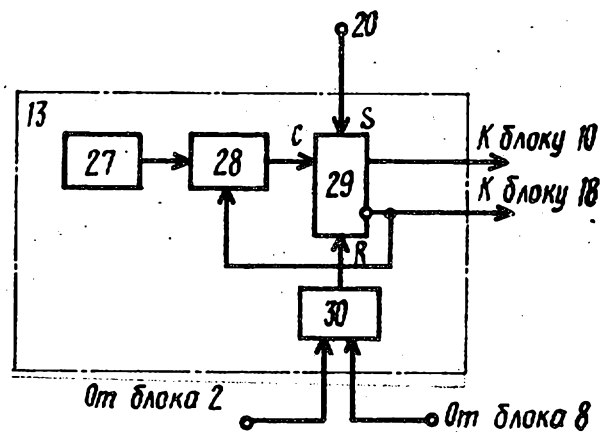
ввода сообщений, после К вводов ложных паролей на неограниченное время. Это уменьшает скорость подбора пароля, предназначенного для получения разрешения ввода сообщений, и, следовательно, повышает надежность защиты от несанкционированного доступа. Снятие блокировки ввода пароля П1 осуществляется набором пароля П2, который может иметь сколь угодно большую длину (например, 15 знаков), так как нет необходимости в оперативном вводе пароля П2, как это требуется для ввода пароля П1. Поэтому вероятность подбора пароля П2 можно считать практически равной нулю, что обеспечивает более высокую надежность защиты от несанкционированного доступа.



Фиг.1



Фиг. 2



Фиг. 3

Составитель В.Верховский

Редактор В.Петраш Техред Л.Мартьянова Корректор Е.Сирохман

Заказ 10286/36

Тираж 710

Подписное

ВНИИПИ Государственного комитета СССР

по делам изобретений и открытий

113035, Москва, Ж-35, Раушская наб., д. 4/5

Филиал ИПИ "Патент", г.Ужгород, ул.Проектная, 4