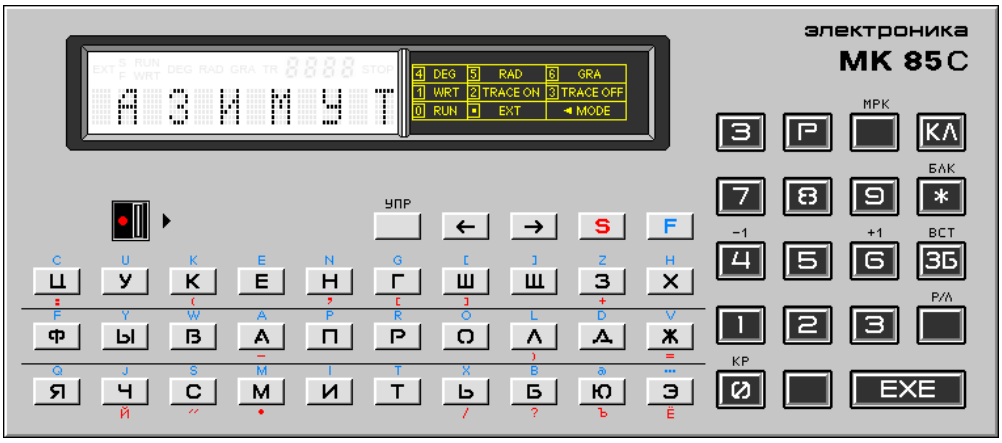
Неофициальное руководство

Электроника МК-85С

Персональный шифратор «АНКРИПТ»



Версия документа — **1.2**

Содержание

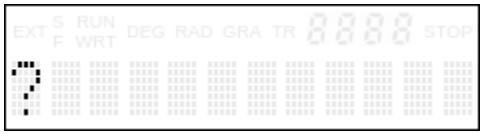
Ссылки:

- **https://b3mk.ru/2024/09/20/mk85c_details/**
- **https://habr.com/ru/users/MaFrance351/publications/articles/**
- **https://web.archive.org/web/20080612123243/http://www.taswegian.com/MOSCOW/mk-85c.html**
- **http://www.leningrad.su/museum/show_calc.php?n=698**
- **https://coollib.cc/b/292195/read**
- **https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B0_%D0%9C%D0%9A-85**
- **https://web.archive.org/web/20080103055330/http://www.ancort.ru/fea_ancript.htm**
- **https://www.electronics.ru/files/article_pdf/0/article_617_924.pdf**
- **https://mk.bs0dd.net/piotr433/index.htm**
- **https://github.com/kaseiiro/mk85**
- **https://retro-computer.ru/home.aspx#/item/MK-85C**

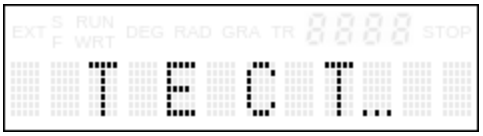
Снимки экрана сделаны с помощью эмулятора **JS85cEMU** — **mk.bs0dd.net**

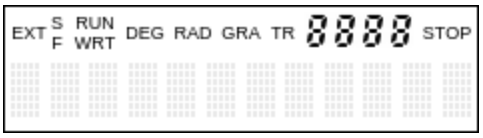
Начало работы

1. Включить МК. «?» сигнализирует о необходимости инициализации ОЗУ.



2. Нажать тонким (не проводящим ток) предметом кнопку «начальная установка». Будет произведено тестирование ЦПУ, ПЗУ, ОЗУ и дисплея.



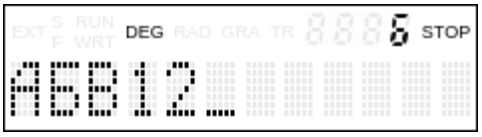


3. Далее система предложит проверить клавиатуру. Можно нажимать на различные клавиши для проверки их работоспособности. Для окончания теста нужно нажать (последовательно) клавиши **УПР** + **EXE**.

4. Шифратор отобразит приветственный экран. Для начала настройки необходимо ввести (не отображается на экране) кодовое слово **«АЗИМУТ».**

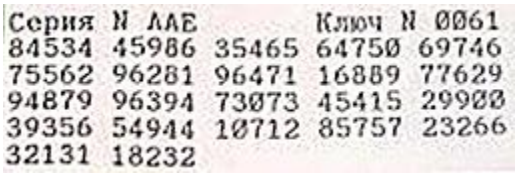
5. Система произведет краткий тест и отобразит контрольную сумму ПЗУ. Для всех известных (на момент составления руководства) устройств она равна **04367402034** (код микросхемы ПЗУ — **061**). Клавиша **Н** запустит повторный тест, клавиша **Д** начнет процедуру настройки.

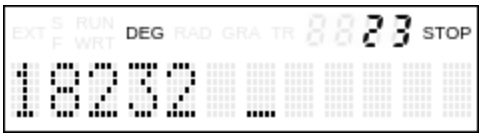
6. Система попросит задать пароль длиной 5 символов. Запомните его, чтобы в дальнейшем иметь возможность разблокировать шифратор! Пароль подтверждается комбинацией клавиш **УПР** + **EXE**.



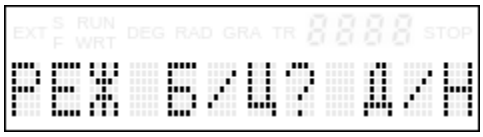
7. Теперь в систему требуется ввести ДКЛ (долговременный ключ), представляющий из себя последовательность 110 цифр (разбитых на 22 блока по 5 цифр). Два последних блока (10 символов) являются контрольной суммой ключа (защита от ошибок при вводе). Такие ключи поставлялись в комплекте с устройством, либо же генерировались (утерянной) программой на IBM PC. На данный момент ключ можно сгенерировать в эмуляторе **JS85cEMU**, используя программу **DKLKM85C** или **утилиту** для Python от kaseiiro. Подтверждение ввода — **УПР** + **EXE**. В качестве примера приведен вот такой ключ:

84534 45986 35465 64750 69746 75562 96281 96471 16889 77629 94879
96394 73073 45415 29900 39356 54944 10712 85757 23266 32131 18232

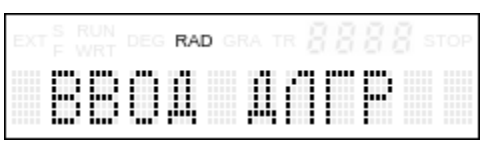


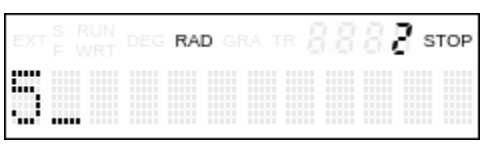


8. Система предложит выбрать тип данных, которые в дальнейшем будут шифроваться (можно поменять только при вводе нового ключа). Это может быть как Буквенно-цифровая информация, так и исключительно Цифровая (цифры будут отображаться с разделением по блокам).



9. Теперь нужно указать длину групп, на которые будут делиться числа. Это могут быть группы от 2 до 5 цифр в каждой (на экране всегда показываются только 2 группы). Подтверждение ввода — **УПР** + **EXE**.

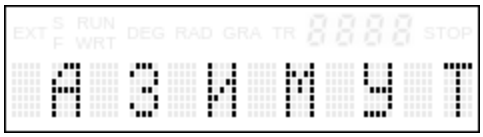




10. Конфигурация шифратора закончена! Теперь можно использовать его для шифровки и расшифровки данных.

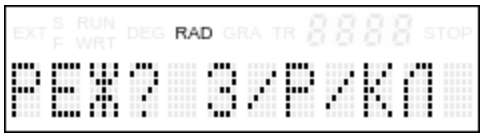
Включение шифратора

1. Включить МК. На экране отобразится приветствие. Для разблокировки шифратора необходимо ввести пароль (ввод не отображается). **ВНИМАНИЕ!** После ввода 25 неправильных символов (счетчик сбрасывается при выключении шифратора) сработает защита от перебора пароля и шифратор уничтожит пользовательские данные в ОЗУ, затем отобразит приветственный экран настройки. В таком случае необходима повторная настройка устройства, начиная с пункта 4.



2. Система произведет краткий тест и отобразит контрольную сумму ПЗУ. Клавиша **Н** запустит повторный тест, клавиша **Д** откроет главное меню.

3. Теперь устройство можно использовать!



Обозначение специальных клавиш

— клавиша включения режима шифровки («Зашифровать»).

— клавиша включения режима расшифровки («Расшифровать»).

— клавиша включения режима смены ДКЛ («Ключ»).

— клавиша стирания текущего символа (аналог Delete).

— клавиша блокировки ввода (только просмотр с прокруткой).

— клавиша смены раскладки (Русский и Латиница).

— клавиша выработки разового ключа (маркант).

— клавиша прокрутки на 12 символов (или два блока) назад.

— клавиша прокрутки на 12 символов (или два блока) вперед.

— клавиша-модификатор для дополнительных функций (управляющая).

Функции клавиш с модификатором УПР


— переход в начало строки.


— переход в конец строки.

— разблокировка ввода.

— вероятно, режим вставки, в прошивке не реализован.

— коррекция расшифровки: возврат к вводу шифротекста для правки.

— коррекция расшифровки: сдвиг гаммы на 1 разряд назад.

— коррекция расшифровки: пропуск 1 разряда шифротекста.

— подтверждение ввода данных.

Цветные подписи к клавишам

- Подписи **СИНЕГО** цвета вводятся при использовании Латинской раскладки.
- Подписи **КРАСНОГО** цвета вводятся при использовании клавиши **УПР**.

Обозначение сегментов на дисплее

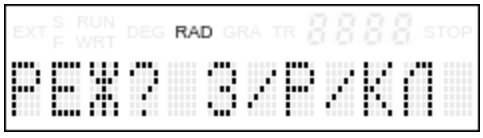
- **EXT** — активна Латинская раскладка.
- **S** — нажат модификатор УПР.
- **F** — не используется.
- **RUN** — режим расшифровки текста.
- **WRT** — режим шифровки текста.
- **DEG** — режим ввода долговременного ключа.
- **RAD** — шифрование в буквенно-цифровом режиме.
- **GRA** — шифрование в цифровом режиме.
- **TR** — активна блокировка ввода.
- **STOP** — достигнут лимит ввода символов.

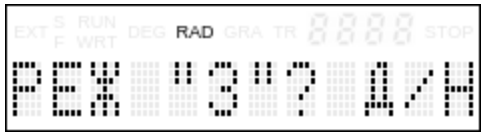
- **Семисегментные индикаторы** обычно показывают номер текущего символа или блока.

(альтернативный вариант сегментов, согласно их назначению)

Режим шифрования данных

1. Для активации режима в главном меню используем клавишу [3]. Соглашаемся активировать его клавишей **Д**.



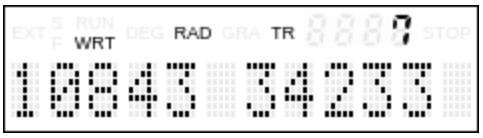


2. Перед началом процесса шифрования необходимо выработать случайный разовый ключ — маркант. Для этого нужно 10 раз нажать клавишу **МРК**.

3. Теперь необходимо ввести шифруемый текст (или цифры, если используется цифровой режим шифрования). В качестве примера приведена строка «ШИФРАТОР ANCRIPT». Подтверждаем комбинацией **УПР** + **EXE.**

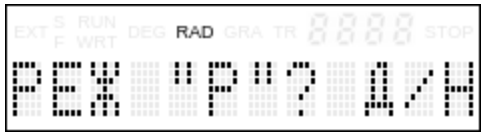
4. Строка шифруется в набор цифр, которые поделены на блоки заданной при настройке длины (вне зависимости от длины блоков на экране всегда отображается только 2 блока). Полученный шифротекст готов к передаче. Нажатие **УПР** + **EXE** возвращает в главное меню.

87809 90512 93160 35334 13316 10843 34233 22345 40949

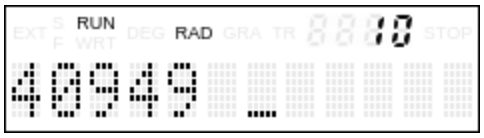


Режим расшифровки данных

1. Для активации режима в главном меню используем клавишу [P]. Соглашаемся активировать его клавишей **Д**.



2. Теперь вводим блоки шифротекста, полученные при шифровке. Подтверждаем ввод по **УПР** + **EXE**.

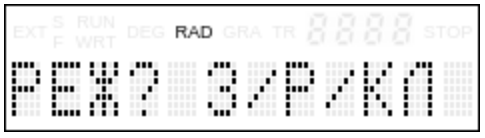


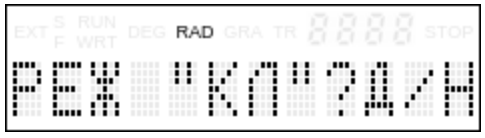
3. На экране видна расшифрованная строка. Если при вводе блоков была допущена ошибка и строка расшифровалась некорректно, можно вернуться к вводу шифротекста комбинацией **УПР** + **КР**. Также, можно устранять искажения в шифротексте с помощью комбинаций **УПР** + **-1** и **УПР** + **+1**, см. Коррекция искажений при расшифровке.

4. При нажатии на **УПР** + **EXE**, перед возвратом в главное меню программа предлагает добавить дополнительные блоки шифротекста. Основное назначение данной функции — расшифровка большого объема данных. Шифратор за раз может расшифровать меньше информации, чем зашифровать. Это вызвано необходимостью хранить шифротекст в ОЗУ, чтобы можно было вернуться к его редактированию по **УПР** + **КР**, поэтому свободного места для расшифровки меньше. В случае если шифротекст не умещается в допустимый лимит, нужно расшифровать и сохранить текущие данные, а затем ввести оставшиеся блоки шифротекста, используя функцию добавки.

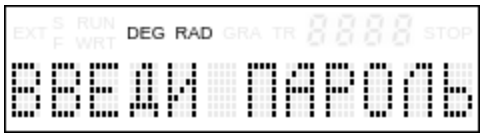
Режим замены долговременного ключа

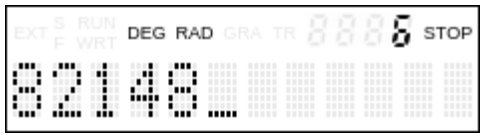
1. Для активации режима в главном меню используем клавишу КЛ. Соглашаемся активировать его клавишей **Д**.



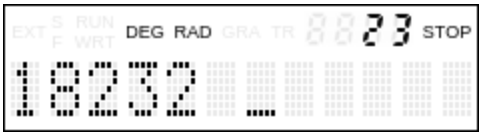


2. Система попросит задать новый пароль. Вводим и подтверждаем клавишами **УПР** + **EXE**.

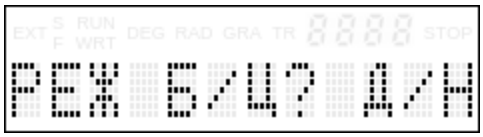




3. Теперь нужно ввести новый ДКЛ. Вводим 110 цифр и подтверждаем клавишами **УПР** + **EXE**.

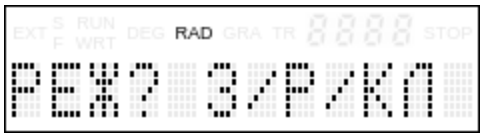


4. Задаем режим шифрования (Буквенно-цифровой или Цифровой).



5. При надобности можно сменить длину блоков.

6. Переконфигурация шифратора закончена!



Коррекция искажений при расшифровке

Примененная здесь система шифрует данные, используя метод гаммирования, когда специально выработанная последовательность (гамма) объединяется с данными. Такой способ удобен тем, что позволяет производить шифрование и расшифрование одной операцией, объединяя с гаммой исходный текст или шифротекст.

Гамма									
1	2	3	4	5	6	7	8	9	...
Данные									
1	2	3	4	5	6	7	8	9	...

Однако, при передаче шифротекста возможно искажение, утрата части данных, либо их дублирование. Если искажение при расшифровке дает, соответственно, искаженные, но читаемые данные, то при потере/дублировании всего одного разряда шифротекста происходит разрыв между данными и гаммой, что приводит к невозможности расшифровать оставшиеся данные. В шифраторе присутствует возможность исправления таких ситуаций. Важно понимать, что первые 10 разрядов (цифр) шифротекста содержат разовый ключ (маркант), искажение которого сразу приводит к невозможности расшифровки всего шифротекста, коррекция здесь ничем не поможет.

Гамма									
1	2	3	4	5	6	7	8	9	...
Данные									
1	2	3	4	8	9	10	11	12	...

Гамма									
1	2	3	4	5	6	7	8	9	...
Данные									
1	2	3	4	5	4	5	6	7	...

Возьмем ранее полученный шифротекст из примера по шифровке:

87809 90512 93160 35334 13316 10843 34233 22345 40949

Как известно, здесь зашифрована строка «ШИФРАТОР ANCRIPT». Теперь представим, что при передаче были утеряны три цифры шифротекста:

87809 90512 93160 35334 13316 10843 34233 22345 40949

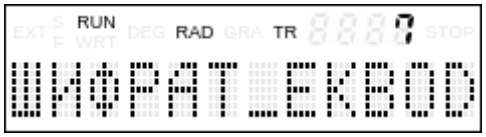
Попробуем ввести имеющийся шифротекст в шифратор:

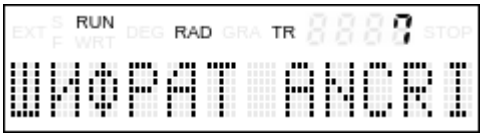
В связи с потерей, текст после 6 буквы оказался полностью нечитаем. Для коррекции предназначены комбинации клавиш **УПР + -1** либо **+1**. Клавиша **-1** сдвигает гамму на 1 разряд назад, клавиша **+1** пропускает один разряд данных. В данном случае, поскольку утеряны 3 цифры, гамму нужно подвинуть на столько же цифр назад.

Гамма									
10	11	12	13	14	15	16	17	18	...
Данные									
10	11	12	13	16	17	18	19	20	...

Гамма									
10	11	12	13	16	17	18	19	20	...
Данные									
10	11	12	13	16	17	18	19	20	...

Переместим курсор на позицию, где началось искажение (в цифровом режиме курсор почему-то перемещается только по блокам, впрочем сама по себе коррекция здесь особо не имеет смысла). Нажимаем комбинацию **УПР + -1** три раза. И действительно, получилась вполне читаемая строка «ШИФРАТ ANCRIPT», в тексте утратились только 2 буквы (каждый символ в буквенно-цифровом режиме кодируется 2 цифрами).





Теперь представим, что при передаче произошло дублирование 4 цифр:

87809 90512 93160 3530 35334 13316 10843 34233 22345 40949

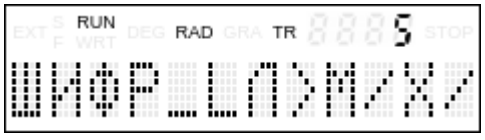
Уже после 4 буквы расшифровка нарушилась.

Для нормализации требуется пропустить 4 дублированных разряда:

Гамма									
5	6	7	8	9	10	11	12	13	...
Данные									
5	6	7	8	5	6	7	8	9	...

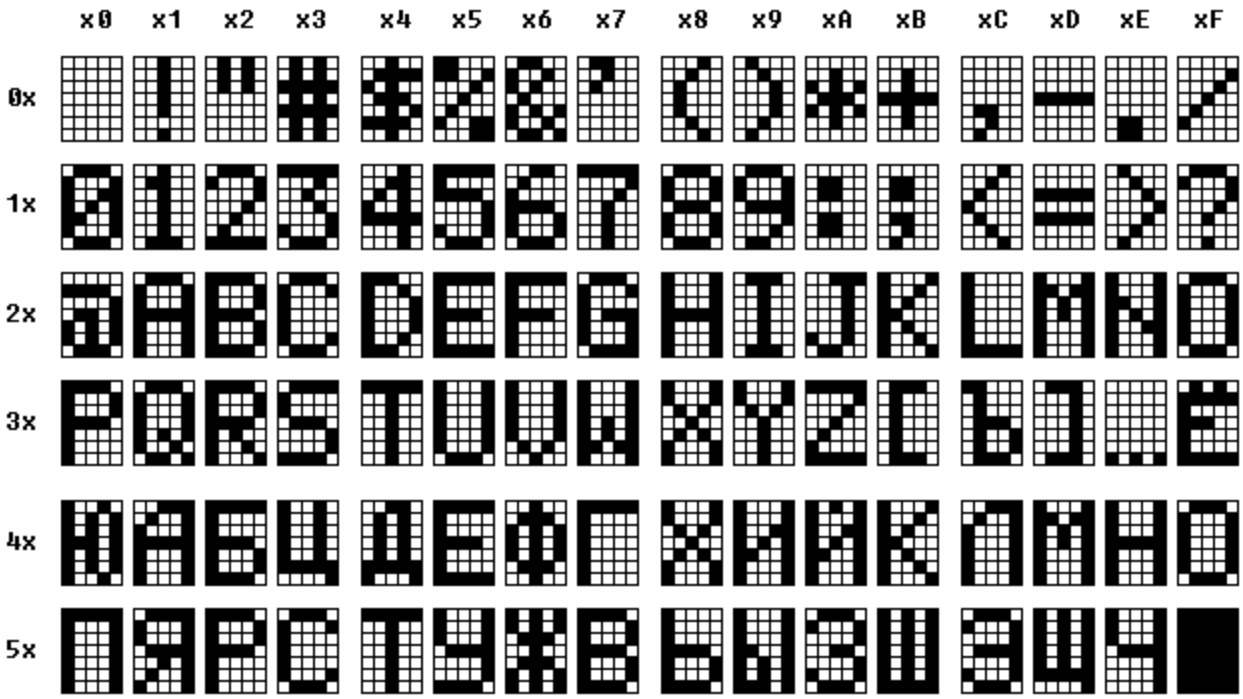
Гамма									
5	6	7	8	9	10	11	12	13	...
Данные									
5	6	7	8	9	10	11	12	13	...

Устанавливаем курсор на позицию и 4 раза нажимаем **УПР + +1.** Данные полностью расшифрованы.



Сведения о устройстве

- **Объем открытого текста:** 750 символов или 1500 цифровых знаков
- **Объем информации, расшифровываемой за один раз:**
  - **Буквенно-цифровой режим:** 535/536* символов
  - **Цифровой режим:** 800/802/803/804** цифры
- **Объем информации, зашифрованной на одном долговременном ключе:** до 3,000,000 символов
- **Долговременный ключ:** 10^{100} вариантов
- **Разовый ключ:** 10^{10} вариантов
- **Алгоритм шифрования:** нелинейный алгоритм высшей сложности «Ангстрем-3»
- **Кодировка:** подобна КОИ-7, со сдвигом на 32 позиции.



* Для блоков по 2 цифры можно расшифровать на 1 символ больше.

** Для блоков по 5/4/3/2 цифры.