# Руководство по эксплуатации
# изделия “409”



31.10.2000

## 1.ИСТОРИЧЕСКАЯ СПРАВКА

Радиосигнализации (РС) первого поколения имели длину кода 8 – 16 разрядов, что давало несколько тысяч возможных кодовых комбинаций. Не представляло большого труда перебрать все возможные комбинации, что бы найти нужную.

Второе поколение РС имело длину кода несколько десятков разрядов, то есть сотни миллионов возможных комбинаций. Против таких систем были созданы устройства, позволяющие перехватывать и записывать кодовые комбинации, с последующим их воспроизведением.

И, наконец, третье поколение РС обладающее, так называемым динамическим кодом, суть которого состоит в том, что кодовая комбинация меняется при каждом нажатии кнопки пульта, использованная комбинация сразу становится недействительной и больше не используется (новых комбинаций хватит на десятки лет). Следующая годная комбинация рассчитывается одновременно в пульте и приемном блоке по очень сложному закону с использованием индивидуальных ключей шифрования. Перехват даже большого числа комбинаций не позволяет за приемлемое время вычислить следующую годную комбинацию.

Но всегда есть слабые места.

Если сделать так, что бы при излучении комбинации пультом она была записана некоторым устройством, но не принята сигнализацией (путем постановки специфической помехи), то при посылке следующей комбинации, которая, естественно, будет послана клиентом почти сразу после первой несработавшей и точно так же будет подавлена, записана и самое главное ПОДМЕНЕНА первой комбинацией в автоматическом режиме, то система нормально сработает, не считая первого “сбоя”. Даже если клиент почует неладное и несколько раз выключит – включит систему, это уже не имеет значения, так как каждый раз система будет исправно срабатывать на очередную подменяемую комбинацию. Процесс подмены занимает 0,02 секунды и совершенно не заметен глазу. В результате в памяти устройства остается самая свежая неиспользованная (годная) комбинация, которую можно использовать в любой момент и по своему усмотрению.

Подавляющее большинство современных РС работают с описанным выше динамическим кодом. Дело в том, что фирма MICROCHIP выпускает набор микросхем (типа HCS200, HCS300, HCS301 и т. д.) очень хороших, дешевых и огромными тиражами. Такими микросхемами оснащены системы от Пантеры и Аллигатора до Клиффорда. Разница в том, что в большинстве систем с гордостью пишут, что используют динамический код системы KEELOQ фирмы MICROCHIP. В других же, в тех что претендуют на исключительность (например Клиффорд) пишут собственные названия динамического кода, а на самом деле тот же KEELOQ и стертые надписи с микросхем HCS200.

Вместе с тем, периодически появляются микросхемы со своим собственным кодом, но они не могут конкурировать с MICROCHIP.

## 2. ВОЗМОЖНОСТИ И СОСТАВ УСТРОЙСТВА.

Устройство состоит из трех основных частей:

1. Передатчик с частотой 433,92 МГц, мощностью 3 Вт. Для сравнения, мощность обычного пульта 0,001 – 0,01 Вт, автопейджера 0,01 – 0,1 Вт.

2. Высокочувствительный, широкополосный приемник диапазона 433 – 438 МГц, позволяет одновременно контролировать всю эту полосу без перестройки, с учетом того что разброс частот некварцованных пультов может достигать +/- 2 МГц.

3. Центральный микроконтроллер с блоком памяти.

Устройство позволяет:

Перехватывать годную кодовую комбинацию, использование которой полностью аналогично применению пульта. Дальность действия – до 50-70 м.

Скрытно контролировать радиоэфир в диапазоне работы РС, обнаруживать и анализировать работу РС, информация о работе которых отображается на 32-знаковом индикаторе. Дальность действия – до 70-100 м.

При необходимости, делать невозможным (подавлять) работу РС в радиусе до 50-70 м.

Обнаруживать работу автопейджеров, в зависимости от их мощности на расстояниях до 1000 м и более.

Подавлять работу автопейджеров на любом расстоянии при нахождении от пейджера в радиусе 50-70 м.

Размеры устройства: 195 * 190 * 65 мм.

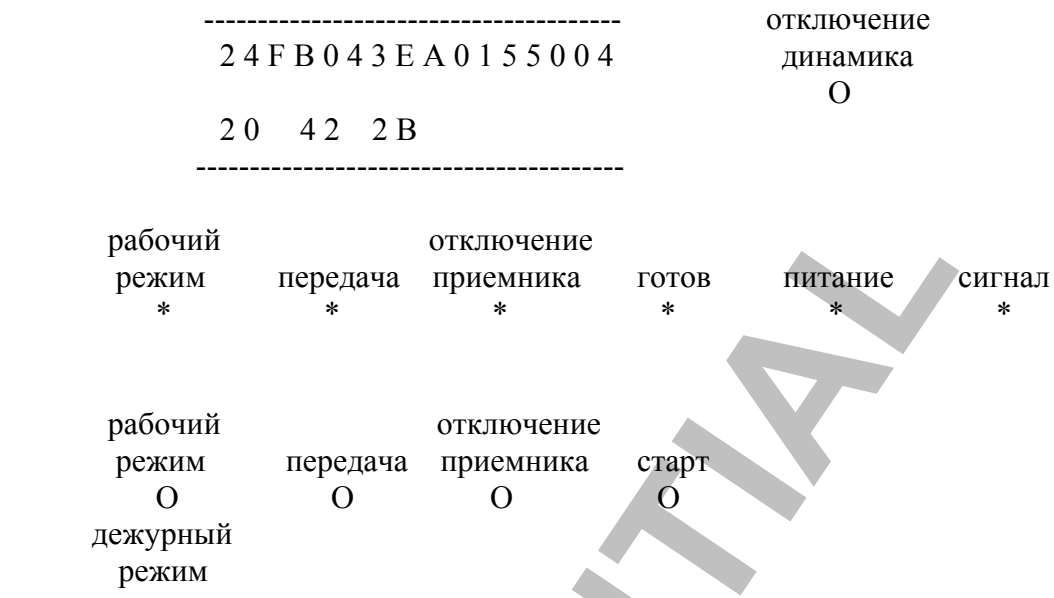


РИС. 1 РАСПОЛОЖЕНИЕ ОРГАНОВ УПРАВЛЕНИЯ

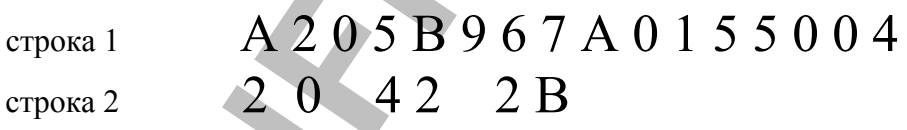


РИС. 2 ПРИМЕР ДИСПЛЕЯ В ДЕЖУРНОМ РЕЖИМЕ

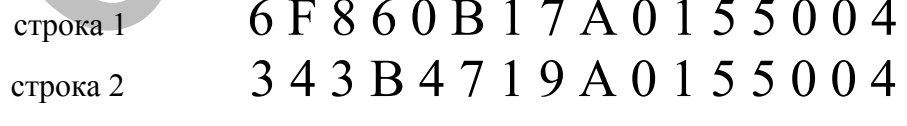


РИС. 3 ПРИМЕР ДИСПЛЕЯ В РАБОЧЕМ РЕЖИМЕ

## 3. ВКЛЮЧЕНИЕ

Сбросить все переключатели (смотрят вниз).

Подключить антенну (разъем на задней панели – вставить и защелкнуть!). Без антенны напряжение не подавать! Штыревая антенна нормально работает при наличии металлической подстилающей поверхности, поэтому крайне желательно устанавливать антенну на металлической крыше автомобиля. При размещении антенны внутри салона дальность работы не гарантируется.

Подключить к бортовой сети автомобиля, либо к источнику +12.6в…+ 15в. Должна загореться лампочка “питание”. Если лампочка не горит, то неконтачит прикуриватель, или перепутана полярность (плюс – центральный контакт, корпус – минус). Важно убедиться, что питание не пропадает (лампочка не мигает) при включении/выключении зажигания, пуске стартера и т. д.

## 4. ДЕЖУРНЫЙ РЕЖИМ

Все переключатели сброшены, из лампочек горит только “питание”. Курсор мигает в левой верхней позиции. При нажатии кнопки пульта, загорается “сигнал”, звучит динамик, на дисплее появляется код и служебная информация. Первые восемь разрядов – динамическая часть кода, следующие семь – постоянная (для данного пульта) часть кода. Последний шестнадцатый разряд в первой строке – номер кнопки (обычно 2, 4, 6 но может быть от 0 до F).

Динамическая часть меняется с каждым нажатием почти случайным образом. Постоянная часть всегда одинакова для данного пульта и позволяет узнавать своего клиента.

Во второй строке расположена служебная информация, не имеющая особого значения. Первые два разряда – признак конца кода (20, реже 00), если загорелось 30 (реже 10) – значит у клиента в пульте села батарейка. Можно предложить купить ему новую. Следующие два разряда - число битов в коде (обычно 42, но может быть 43, 45, FF). Последние два – длина одного бита, обычно от 2A до 32.

Итак, нажимаем разные кнопки пульта (и две вместе), наблюдаем появление кода на дисплее. Таким способом можно проверить дальность срабатывания (на прием) устройства.

## 5. РАБОЧИЙ РЕЖИМ

Основной режим, который позволяет автоматически перехватывать кодовые комбинации и переизлучать записанные из памяти.

Все переключатели сброшены, взведен только “рабочий режим”. Горят лампочки “питание” и “рабочий режим”. Дисплей можно предварительно очистить. Чистка дисплея производится автоматически, при переключении режима. Курсор мигает в левой верхней позиции.

После первого нажатия кнопки пульта, появляется код в первой строке, излучается помеха, система не срабатывает.

После второго нажатия кнопки пульта, появляется код во второй строке, излучается первая кодовая комбинация, система срабатывает, загорается лампочка “готов”.

Если теперь включить/выключить переключатель “старт”, то система сработает как будто от пульта.

Если несколько раз нажать на кнопку, уже после появления сигнала “готов”, то будет видно как предыдущая запись перемещается со второй строки в первую, а на свободное место записывается новая.

Теоретически, это можно продолжать до бесконечности, устройство в любой момент будет готово к применению, пока не произойдет сбой. Тогда придется начать сначала. Для этого достаточно очистить дисплей переключателем режима и не забыть поставить его в “рабочий режим”.

Последний разряд в первой строке показывает номер кнопки пульта (обычно 2, 4, 6). Почти во всех пультах одна и та же кнопка служит для включения и выключения системы. Либо со светом/звуком – одна кнопка, либо без – другая кнопка. Пока редко, но встречаются системы у которых одна кнопка – только для постановки, другая – только для снятия (один из Мангустов, один из Фараонов). С такими системами требуется более сложный алгоритм “принуждения к нажатию всех кнопок”, сортировки и излучения сигналов. Во избежание путаницы он пока не записан в устройство. Повторяю, подавляющее большинство систем имеет совмещенные кнопки и, если появляются в последнем разряде разные цифры, то это значит, что клиент ставит с подтверждением светом/звуком, а снимает без. Но это не помеха работе устройства.

## 6. ОТКЛЮЧЕНИЕ ПРИЕМНИКА

После того как приняты нужные кодовые последовательности и новых нажатий не ожидается, полезно отключить приемник переключателем “отключение приемника” (загорается лампочка “отключение приемника”) так как случайные сигналы других пультов могут вытеснить записанные коды.

## 7. ВКЛЮЧЕНИЕ ПЕРЕДАТЧИКА ПОМЕХ

Передатчик позволяет подавить работу систем на расстоянии до 50 –70 м. Переключатель “передача” работает независимо от других переключателей, включение подтверждается лампочкой “передача”. Чтобы убрать звук, можно отключить приемник, либо динамик. Не забыть потом включить!

## 8. ПЕРЕКЛЮЧАТЕЛЬ “СТАРТ”

Имитирует кнопку на пульте, после того как загорелась лампочка “готов”. Некоторые системы ждут окончания передачи сигнала, поэтому через 1- 3 секунды нужно отключать передачу.

## 9. ОТКЛЮЧЕНИЕ ДИНАМИКА

Отключает только динамик, когда нужна тишина. Лампочка “сигнал” продолжает работать. Не забыть включить обратно! Без звука момент прихода сигнала легко пропустить. Лампочка “сигнал” и динамик подключены к выходу приемника. Они сигнализируют о любых сигналах в диапазоне 430 – 438 МГц: систем с фиксированным кодом, случайных помех, а, главное, показывают работу автомобильных пейджеров. Повторяющиеся примерно каждые 5 секунд сигналы длительностью около 1 секунды – это сигналы тревоги типичного автопейджера. Если сигнал повторяется примерно раз в 60 – 90 секунд и имеет длительность около 5 секунд, то это автопейджер с проверкой радиоканала.

Изделие 409 предъявляет минимальные требования к квалификации оператора. Следующее поколение представлено изделием 502, которое позволяет:

- Обрабатывать системы с раздельным снятием-постановкой.
- Обнаруживать-подавлять-подменять сигналы автопейджеров с контролем радиоканала.
- Контролировать радиоэфир в диапазоне 40 – 960 МГц.

Изделие 502 предъявляет более высокие требования к квалификации оператора.

Подробную техническую информацию об изделиях 409, 502 можно получить по адресу: keeloq@narod.ru