УСТОЙЧИВОСТЬ ОХРАННЫХ УСТРОЙСТВ К «ЭЛЕКТРОННОМУ ВЗЛОМУ»

Приобретая сигнализацию покупатель задает себе естественный вопрос – легко ли подобрать «ключ» к этому электронному замку? Для того чтобы исключить возможность выключения сигнализации нежелательными лицами применяется кодирование передатчиков. Уровень секретности кодов различных сигнализаций значительно отличается. В устаревших сигнализациях применялись коды с числом комбинаций до 512, Подбор такого кода занимает менее 1 минуты. Количество комбинаций кодов в современных сигнализациях может достигать нескольких тысяч миллиардов. Для кодирования сигнала передатчика и последующего его декодирования используются комплекты специализированных микросхем, некоторые из которых представлены в таблице ниже или универсальные микроконтроллера с соответствующим программным обеспечением. Для того чтобы оценить секретность кодировки необходимо обратить внимание на следующие особенности, указываемые в рекламной информации:

Антисканирование

Этот термин обозначает то, что злоумышленник не сможет снять сигнализацию с охраны с помощью сканера. Сканер – это относительно несложное устройство, которое последовательно воспроизводит коды в формате взламываемой сигнализации. Систему с антисканированием нельзя выключить перебором кодов брелока, так как при приеме неверного кода она, на некоторое время блокируется, увеличивая время, необходимое для сканирования. Блокировка снимается многократной передачей правильного кода. При достаточно большом числе возможных кодов перебор займет нереально много времени. Технология антисканирования применяется уже несколько лет и не является новинкой. Системы с антисканированием не защищены от перехвата кодов из эфира с помощью специальных устройств (грабберов или перехватчиков кодов). Антисканирующая пауза является необходимым атрибутом и в системах с динамическим кодом.

Динамический, прыгающий, плавающий код (jumping, hopping, floating и т.д.)

Технология плавающих кодов делает невозможным, как перехват кодов из эфира, так и их подбор. Действительный код шифруется таким образом, что при каждой передаче излучается внешне совершенно другая кодовая посылка. В приемнике действительный код восстанавливается путем математической обработки. Перехват кодов становится бессмысленным, так как невозможно предсказать какая следующая кодовая комбинация снимет сигнализацию с охраны. Простое повторение предыдущей посылки не приведет к выключению сигнализации, так как бывшие в прошлом посылки считаются недействительными. Предсказать же будущую посылку теоретически можно, только зная алгоритм шифрования кода, который держится фирмой-изготовителем в секрете и достаточное количество выборок кода для анализа. Кодовые комбинации повторяются с очень большим интервалом. Исследования модели MICROCAR 052.1 показали, что для данной модели этот период составляет более 65000 нажатий. Можно сказать что, в процессе эксплуатации, передаваемые кодовые комбинации не разу не повторяются – машина не служит 20 лет. Коды-идентификаторы брелоков автосигнализаций с плавающими кодами записываются в заводских условиях и являются уникальными не подлежащими замене в процессе эксплуатации. Технология плавающих кодов очень эффективно защищает сигнализацию от взлома с помощью электронных средств.

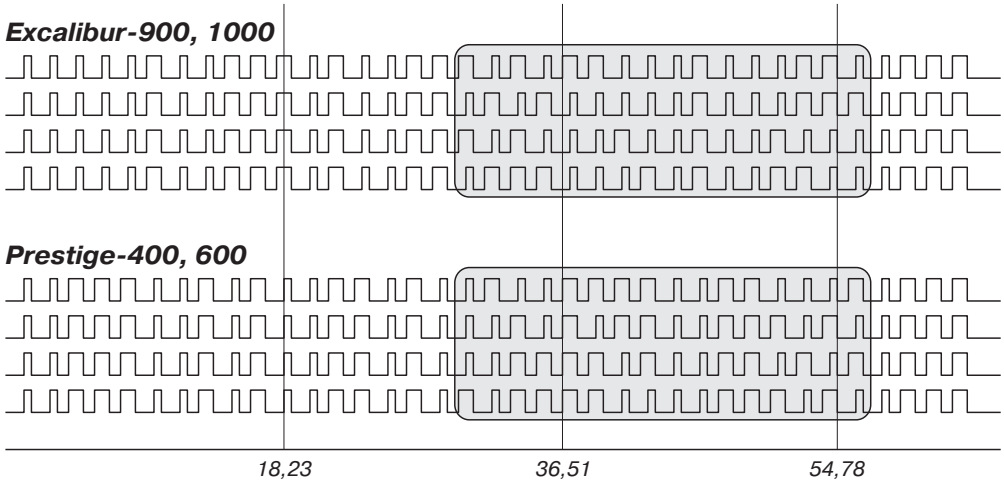

Рис. 1.

Степень защиты от расшифровки зависит от применяемого алгоритма кодирования. Приведенные ниже рис. 1 и 2 позволяют наглядно оценить, на сколько изменяются коды передатчика при четырех последовательных нажатиях кнопки брелока у различных распространенных систем сигнализации.

Двойной динамический код

С тех пор, как код – граббер перестал быть экзотикой и доступен угонщикам, все большое значение уделяется степени секретности кодовой посылки, передаваемой с брелока. Как результат этого процесса все большее число систем выпускается с динамическим кодом. Никто не оспаривает его преимуществ. Однако и он не может считаться панацеей на все случаи. Если алгоритм изменения становится известен, (а он известен, по крайней мере, разработчику), то внедриться в систему остается делом техники. Не даром система кодировки так тщательно засекречивается и скрывается производителями сигнализаций. Для исключения и этой возможности для электронного взлома разработан так называемый D2-код, сущность которого заключается в том, что каждому брелоку, помимо разрядного номера, присвоен еще и свой индивидуальный закон изменения кода. Это индивидуальное правило записывается в декодер один раз при вводе (программировании) брелока, в эфире больше не появляется и радиоперехвату недоступно. Таким образом, даже разработчик системы, обладая всей необходимой информацией о способах кодирования и соответствующей аппаратурой, не сможет расшифровать этот код. Специалисты считают, что динамический код с индивидуальным законом изменения для каждого брелока это тот уровень секретности, когда вопрос о дальнейшем совершенствовании отпадает, по крайней мере, на ближайшие 20...30 лет.

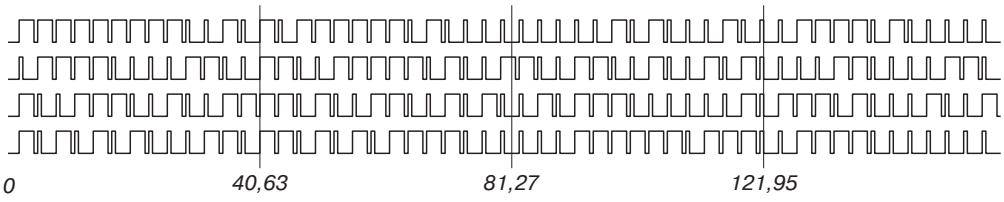

Рис. 2.

ФОРМИРОВАНИЕ ДИНАМИЧЕСКОГО КОДА

Прыгающий код фирмы Microchip

Основные термины

- ❒ Код Изготовителя (Manufacturer's Code) – 64-битовое слово, уникальное для каждого изготовителя, используется, для того чтобы произвести уникальный кодирующий ключ в каждом передатчике.
- ❒ Кодирующий ключ (Encoder Key) – 64-битовый ключ, уникальный для каждого передатчика.
- ❒ Ключ кодирующего устройства управляет алгоритмом дешифрования и хранится в EEPROM микросхемы декодера.
- ❒ Обучение – приемник в режиме обучения использует информацию, которая передана, чтобы получить передатчика, дешифровать диапазон дискриминации, и синхронизировать счетчик.
- ❒ Ключ кодирующего устройства – функция кода изготовителя и серийного номера устройства и-или величина начального смещения.

Кодеры и декодеры используют технологию прыгающего кода KeeLoq и алгоритм шифрования KeeLoq.

Прыгающий Код – метод, при которым код, переданный с передатчика на приемник является различным, при каждом нажатии кнопки. Этот метод, вместе с длиной передачи 66 битов, фактически делает невозможным перехват или подбор кода.

Принцип работы кодера

Кодирующие устройства серии HCS имеют небольшой массив EEPROM-памяти, который должен быть загружен несколькими параметрами перед использованием.

Наиболее важный из этих величин:

- ✓ кодирующий ключ, который генерируется.
- ✓ 16-битовое число в счетчике синхронизации
- ✓ 28-битовый серийный номер, который, как предполагается, является уникальным для каждого кодера.

Изготовитель программирует серийный номер для каждого кодера во время продукции, в то время как «Алгоритм генерирования ключа» генерирует кодирующий ключ (рис. 1а).

Исходные данные к алгоритму генерирования ключа включают в себя серийный номер кодера и 64-битного код изготовителя, который создается во время изготовления.

Обратите внимание: код изготовителя – самая важная часть секретности системы. Следовательно по отношению к этому коду должны приниматься все возможные предосторожности.

Счетчик синхронизации с 16-битным основанием служит для модификации передаваемого кода, при каждой передаче и обновляется каждый раз по нажатию кнопки.

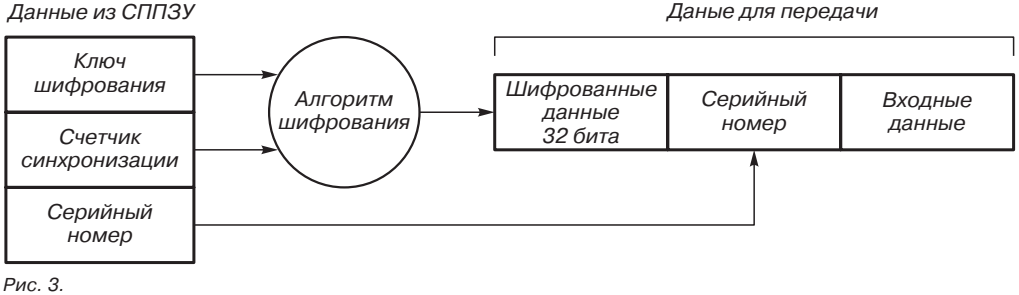

Рис. 3.

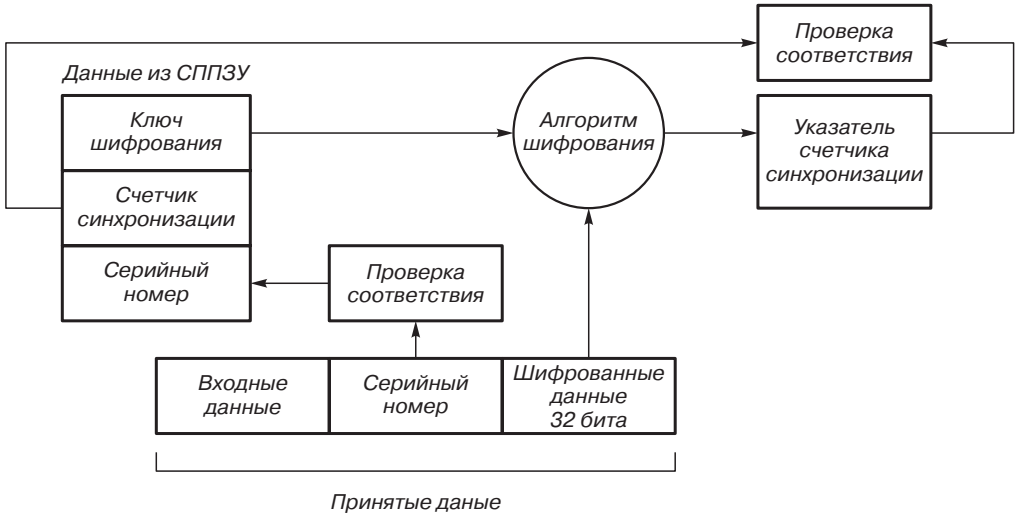

Рис. 4.

Благодаря сложности алгоритма шифрования KEELOQ, изменение в одном бите величины счетчика синхронизации приводит к большим изменениям в передаваемом коде.

Имеется связь (рис. 3) между величинами в СППЗУ и фактическим выходным кодовым словом.

Если только кодер обнаруживает, что кнопка была нажата, он считывает состояние входных сигналов и модифицирует счетчик синхронизации.Величина из счетчика синхронизации обрабатывается вместе с кодирующим ключом алгоритмом шифрования KEELOQ, в результате получаются 32 бита шифрованной информации.

Эти данные изменятся с каждым нажатием кнопки. Это и упоминается как прыгающая часть кодового слова.

32-битовая часть с прыгающим кодом объединена с информацией о нажатой кнопке и серийным номером, чтобы формировать кодовое слово, передаваемое на приемник.

Принцип работы декодера

Прежде, чем передатчик и приемник смогут работать вместе, приемник должен снача-

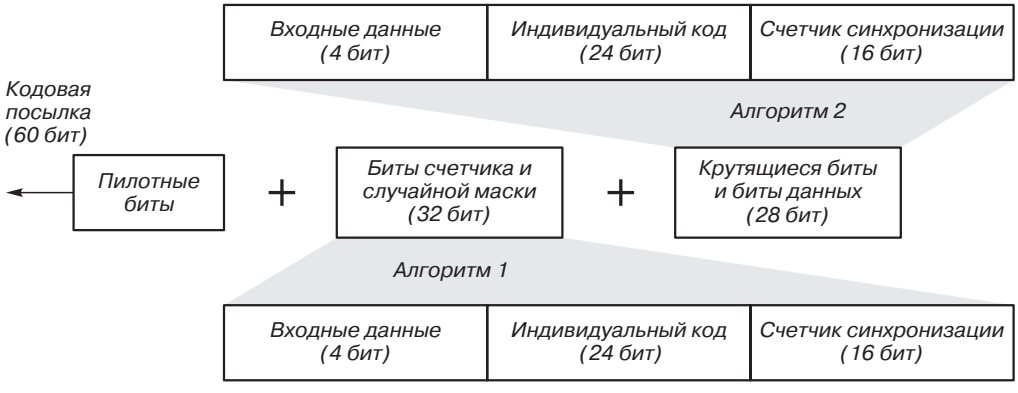

Рис. 5.

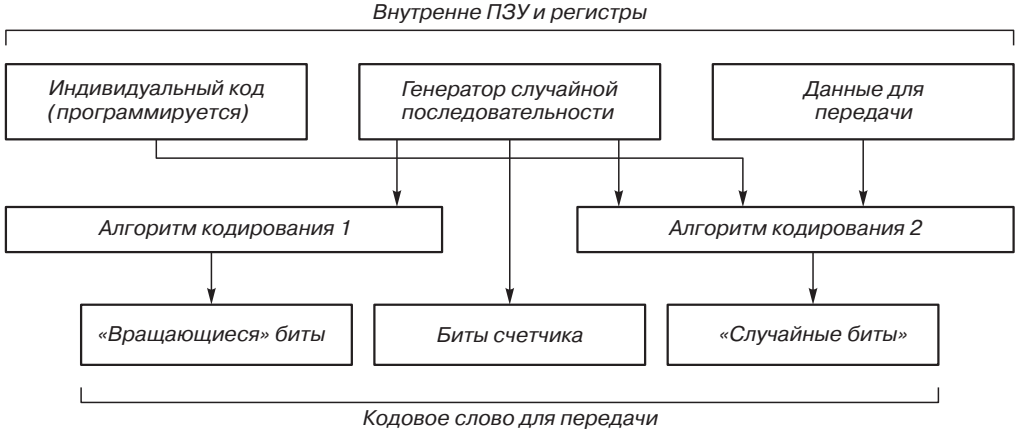

Рис. 6.

ла обучиться и сохранять некоторую информацию из передатчика.

Эта информация включает контрольную сумму серийного номера, ключ кодирования, и текущую величину счетчика синхронизации.

Когда сообщение верного формата обнаружено, приемник сначала сравнивает серийный номер.

Если контрольная сумма серийного номера соответствует запомненному ранее передатчику, сообщение дешифруется.

Затем, приемник проверяет расшифрованную величину счетчика синхронизации сравнивая ее с тем, что сохранено в памяти. Если величина счетчика синхронизации удовлетворяет, то допустимое сообщение принимается. Рис. 4 показывает связь между некоторыми из величин, сохраняемых приемником и величинами, полученными от передатчика.

Кодеры и декодеры фирмы Holtec

Кодер HT6P26 обеспечивает передачу 4 битов данных к декодерам HT6P36.

HT6P26 имеет внутренний 16-битовый случайный счетчик синхронизации. При передаче очередного кода величина случайного счетчика изменится, и величина изменения передается декодеру.

Передаваемое кодовое слово разделено на нечетное и четное окно. И нечетное, и четное окно включает в себя 8 пилотных битов, 1/3 стартовых биты, 24 катящихся бита, 16 битов индекса, 16 случайных битов и 4 бита данных (рис. 5).

«Катящиеся» биты и «случайные» биты генерируются различными алгоритмами шифрования (рис. 6). Биты данных устанавливаются по состоянию выводов данных.

Синхронизация системы с динамическим кодом

Для того чтобы обеспечить невозможность вскрытия сигнализации уже переданными ранее комбинациями в системах с динамическим кодом в кодовой посылке присутствует информация о том, сколько раз нажималась кнопка брелока с момента программирования микросхемы кодера изготовителем. При запоминании брелока микросхемой декодера (процедура learning) состояния счетчиков в кодере и декодере уравниваются.

Каждый раз при получении кода счетчик декодера следит за тем чтобы счетчик кодера указывал на большее или равное значение. Только тогда принятый код считается вер-

Рис. 7.

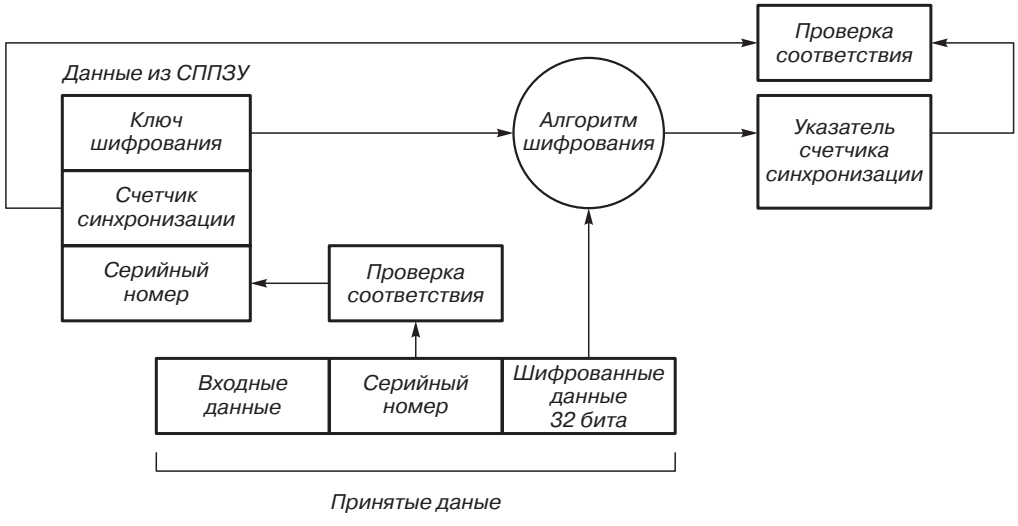

Рис. 8. ***Окно синхронизации прыгающего кода KeeLoq***

ным. Разница между счетчиком декодера и счетчиком кодера при которой код все еще считается верным различна для устройств разных изготовителей и может составлять величину от единиц до сотен.

Синхронизация декодера HT6P36

В начале использования декодера, необходимо выполнить операцию «обучения», чтобы сохранить шифрованный код-идентификатор и значение счетчика синхронизации в СППЗУ.

16-разрядный счетчик синхронизации хранится в СППЗУ. Декодер автоматический создает «окно синхронизации». Ширина «окна синхронизации» – 256. Начало – «текущее состояние счетчика», конец – «текущее состояние счетчика + 255».

Если декодер получает надлежащий катящийся код, и полученное значение счетчика синхронизации будет находиться в пределах окна синхронизации, декодер активизирует выход декодера и обновит положение «окна синхронизации».

С другой стороны, если полученный код индекса вне «окно синхронизации», система дистанционного управления не будет работать и ее придется заново синхронизировать.

Синхронизации кодера HT6P60 и HT6P50 фирмы Holtec

В режиме дистанционного управления, если rolling-код правильно получен, и полученный rolling-адрес не большие чем на 6 указателя адреса СППЗУ, кодер и декодер считаются синхронизированными.

Указатель адреса декодера модифицируется для согласования с полученным rolling-адресом. С другой стороны, если разница между полученным rolling-адресом и внутренним указателем адреса декодера больше чем 6, кодер и декодер считаются рассинхронизированными, и декодер блокируется.

Успешное распознавание кода возможно только при условии синхронизации кодера и декодера. Для этого необходимо передать декодеру два последовательных rolling-адреса, и никакие ошибки не должны быть обнаружены декодером внутри 3-секундного интервала.

То есть вход данных кодера должен быть активирован дважды последовательно в течении 3 секунд, чтобы повторно синхронизировать декодер с кодером.

Кодовый брелок сигнализации – это миниатюрный передатчик (рис. 9), работающий в диапазоне волн 200...450 МГц. Реже встречаются модели, работающие на инфракрасных лучах, они отличаются малым радиусом действия. Рабочие частоты передатчиков постоянны и нормированы контрольными органами электросвязи стран в которые эти устройства ввозятся.

Поскольку в Украине ввоз автосигнализаций до последнего времени не контролировался ГИЭ можно сказать, что по факту здесь наиболее распространены сигнализации работающие на частотах 300 и 434 МГц.

Для передачи кода в эфир используется однотранзисторный генератор, работающий на одной из вышеуказанных частот. В современных сигнализациях, во избежание ухода частоты при изменении температуры и влажности, частота передачи стабилизируется с помощью фильтров на поверхностных акустических волнах (рис. 10). Для воспроизведения кода – идентификатора в брелоках используются специализированные микросхемы – кодеры, а также, запрограммированные соответствующим образом, микроконтроллеры.

Запоминание новых брелоков

Многие сигнализации и иммобилайзеры могут помнить несколько (4...8) брелоков-

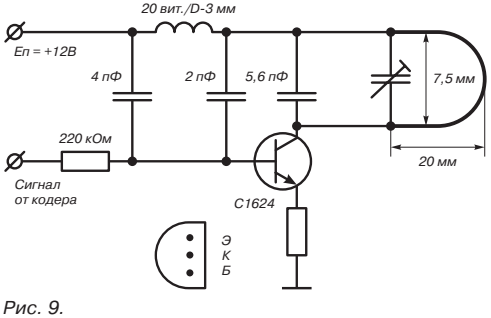

Рис. 9.

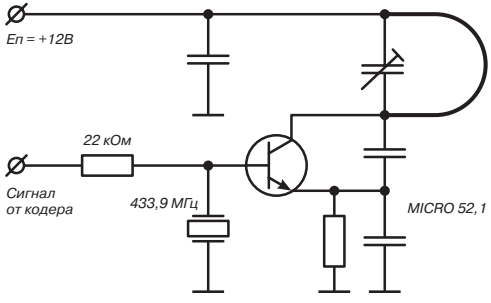

Рис. 10.

передатчиков. Воспользовавшись этим свойством можно управлять одним брелоком несколькими однотипными сигнализациями, установленными на разных машинах или обеспечить нескольких человек брелоками для открывания одной машины. Все модели CLIFFORD, PRESTIGE, EXCALIBUR имеют возможность запоминания новых брелоков

Автосигнализации с брелоками-передатчиками на ИК-лучах

Для сигнализации оснащенных брелоками на ИК – лучах перехват кодов весьма затруднен из-за малого радиуса действия и направленности брелоков-передатчиков (при пользовании их приходится направлять в определенное место салона автомобиля с расстояния не более нескольких метров). Эта особенность может создавать неудобства при пользовании. Сигнализации с ИК-брелоками: BOSH Blocktronic IR-US, BOSH Blocktronic IM-US

Таблица 1.

Рабочие частоты охранных систем для некоторых стран	
Страна	Частота, МГц
Франция	224,5
Италия, США, Испания, Австралия, Греция	300,1
Великобритания	418
Германия, Бенилюкс, Скандинавия	433,92

Таблица 2.

Название таблицы			
Кодеры	Декодеры	Фирма-изготовитель	Характеристики
MC145026	MC145027B, MC145028B	Motorola	Фиксированный код, 512 комбинаций
HT6P20	HT6P11	Holtec	Фиксированный код, 2^{24} комбинаций
HT6P26	HT6P36	Holtec	Динамический код, 2^{24} комбинаций
HCS300	HCS512	Microchip	Динамический код
TRC1300, TRC1315	TRC1300, TRC1315	Texas Instruments	Динамический код, 40-битовый идентификатор, 1 триллион комбинаций

Таблица 3.

Название таблицы				
Кодер	Декодер	Количество комбинаций	Тип кода	Задание кода
16-023-381D	Центральный процессор		Плавающий	на заводе
NTK03S	NTK01A		Плавающий	на заводе
NTK03T	Центральный процессор AXC11A		Плавающий	на заводе
NTK03T	Центральный процессор		Плавающий	на заводе
NTK03S	Центральный процессор		Плавающий	на заводе
NTK03S	Центральный процессор		Плавающий	на заводе
NTK03S	Центральный процессор		Плавающий	на заводе
YC03/WN	YC03/N		Плавающий	на заводе
COPL311-RHH	Центральный процессор		Фиксированный	на заводе
PT2262	PT2272-L4	59049 исп. 19639	Фиксированный	Перемычками
TS-556	Центральный процессор		Фиксированный	на заводе
AX5326S-3	AX5227P-B	6561	Фиксированный	Перемычками
AX5326S-3	AX5227P-B	6561	Фиксированный	Перемычками
AX5326S-3	Центральный процессор	6561	Фиксированный	Перемычками
HT600	HT604L	177147		
Фиксированный	Перемычками			
HT600	HT604L	177147		
Фиксированный	Перемычками			
HT6207	HT604L	19638	Фиксированный	Перемычками
VD5012	VD5013	256	Фиксированный	Перемычками

Устройство для проверки кодовых брелоков

Это приспособление при своей очевидной простоте позволяет не только проверять и настраивать кодовые брелоки автосигнализаций, но и оценить степень секретности кода. Устройство представляет собой обычный детекторный приемник на частоты 280...450 МГц (рис. 11). Устройство желательно расположить в плоском пластмассовом корпусе. Петлю из медного одножильного проводника следует поместить в корпус так, чтобы она располагалась параллельно верхней поверхности корпуса на минимальном расстоянии от нее. Переменный конденсатор припаивается непосредственно к петле, а ручка выводится наружу. Проверяемый брелок укладывают на верхнюю поверхность устройства. При нажатии кнопки на брелоке в телефоне слышится звуковой сигнал.. Ориентируя брелок, и вращая ручку переменного конденсатора добиваются максимальной громкости сигнала. По громкости сигнала можно оценить исправность брелока и степень разряда батареи. По положению ручки конденсатора можно определить рабочую частоту брелока, если предварительно наклеить бумажную шкалу и откалибровать ее по брелокам с известной рабочей частотой, поставив соответствующие метки. Настроить брелок со смещенной частотой передатчика можно, установив ручку переменного конденсатора, в положение соответствующее требуемой частоте и вращая шлиц подстроечного конденсатора внутри брелока до достижения максимума сигнала. Известно, что в сигнализациях со сложными длинными кодами передача ведется медленнее для повышения достоверности приема, а кодовые посылки длиннее, чем в простых системах. Частота и длина посылок кодовых брелоков прекрасно прослушивается в телефон приведенного устройства. Попробуйте проверить подряд брелоки от CLIFFORD и TOPP GUNN или SACA. Посылки от брелока CLIFFORD поступают редко и имеют низкий тон, они намного длиннее посылок брелока от TOPP GUNN, которые поступают очень часто и намного выше по тону. При желании кодовые последовательности брелоков легко посмотреть на осциллографе. Для этого потребуется изменить схему устройства в соответствии с рис. 12.

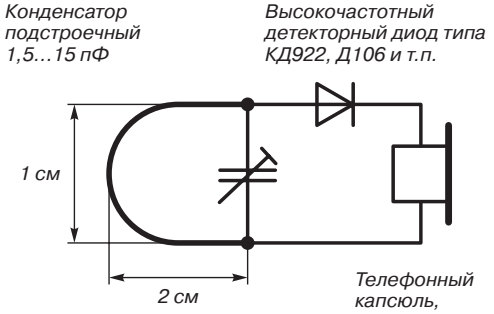

Рис. 11.

Устройство для проверки и настройки пейджеров

Иногда при установке пейджера возникают проблемы связанные с недостаточным радиусом действия. Настройка антенны пейджера в очень большей степени зависит от способа ее укладки в салоне автомобиля, поэтому заводскую настройку выходного контура передатчика нельзя считать оптималь-

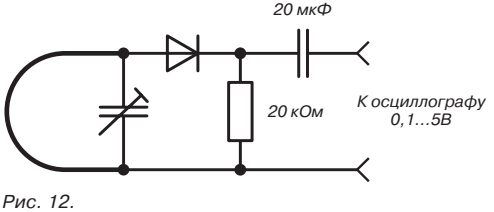

Рис. 12.

ной. Настройка выходного контура методом проб и ошибок с помощью приемника пейджера утомительна и занимает много времени. Для объективной оценки уровня мощности сигнала в антенне пейджера предназначено описываемое ниже устройство, схема которого приведена на рис. 13. Устройство представляет собой диполь с резонансной частотой 300...450 МГц, что соответствует рабочей частоте большинства распространенных пейджеров.

Диполь снабжен детектором и измерительной головкой, по которой осуществляется отсчет. Выполнять диполь следует из толстой медной проволоки или трубок. Устройство позволяет быстро настроить передатчик пейджера по максимуму сигнала. С потерей чувствительности схема работает и в диапазоне 27 МГц. При работе следует включить пейджер и, поднося устройство к антенне добиться того, чтобы стрелка прибора расположилась на середине шкалы. После чего устройство следует зафиксировать и, вращая элементы настройки выходного контура передатчика добиться максимальных показаний прибора.

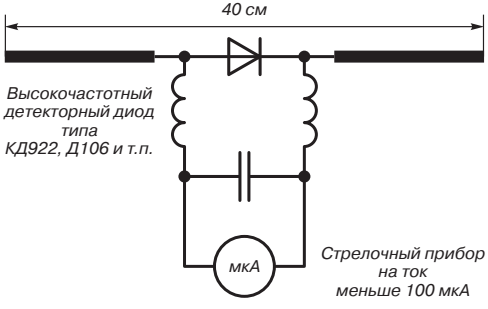

Рис. 13.