http://support.microline.ru/index.php/%D0%94%D0%B8%D0%B0%D0%BB%D0%BE%D0%B3%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4_%D1%81_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%D0%BC_AES-128

Диалоговый код с шифрованием AES-128

Диалоговый код с шифрованием AES-128 — обмен данными по радиоканалу 2,4 GHz с индивидуальными ключами шифрования длиной 128 бит, используемый в автосигнализациях ZONT для защиты от электронного взлома.

Как это работает при снятии и постановке авто на охрану?

Автомобиль безошибочно узнает своего владельца по следующему алгоритму:

1. При нажатии на кнопку, сигнализация отправляет зашифрованный запрос идентификации радиометке/радиобрелоку.

2. Радиометка/радиобрелок получает его, зашифровывает повторно, соответственно своему алгоритму, и отправляет обратно сигнализации.

3. Если сообщение правильное, то сигнализация выполняет команду.

Такой мгновенный радиоконтакт в охранных системах ZONT обладает особой криптостойкостью, так как он защищен шифрованием по стандарту AES-128. Данная технология шифрования применяется в военной авиации, работе спецслужб и банковском оборудовании.

В каждой системе используется индивидуальный ключ шифрования, передаваемый единственный раз при регистрации радиометки/радиобрелока в системе. Длина ключа – 128 бит, что дает такое количество комбинаций, которое невозможно подобрать.