# Введение

Один из вопросов, который будет волновать любого человека или компанию, который подписывается на наши услуги – вопрос безопасности. В связи с этим предлагаю осуществить подробный разбор того какие данные и как фигурируют у нас в системе, для того чтобы сделать ряд выводов об обеспечении безопасности в системе.

Начнем с анализа модуля устанавливаемого в автомобиль.

# Модуль автомобиля:

Данный модуль в законченном исполнении будет иметь вид небольшой коробочки, устанавливаемой в диагностический разъем автомобиля и фиксирующийся там при помощи пломбы. Корпус имеет разъём: разъем антенны.

Важно отметить что система никаким образом не сможет оказывать влияния на ЛЮБЫЕ параметры автомобиля. Диагностический разъем конечно позволяет оказывать влияние на работу машины, чем пользуются при угонах, перепрашивая авто, однако Наш МК не запрограммирован осуществлять такие манипуляции, а так как обновление прошивки невозможно, то наличие нашего устройства в разъеме как раз является лучшей защитой автомобиля, так как не санкционированное изъятие устройства из разъёма приведет к срабатыванию сигнализации.

Рассмотрим данные которые передаются с вашего авто на наши базовые станции и как они защищены.

# Канал связи по протоколу LoraWan

Из автомобиля на БС передаются:

1. Уникальный ключ код автомобиля
2. Местоположение авто
3. Код ошибки

Данная информация подвергается первичному шифрованию при помощи специально разработанного алфавита.

Далее используется протокол защиты реализуемый в LoraWan. Абсолютно безопасных способов передачи данных, как известно, не существует, но концепции безопасности, заложенные разработчиками [протокола LoRaWAN](http://lorawan.lace.io/lorawan-networks/), делают взлом практически невозможным, вычислительные мощности способные подобрать комплект из двух [AES-128](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) ключей за разумное время появятся еще очень не скоро. Если учесть, что ключи разные для каждого устройства, то вероятность подбора ключей становится ничтожно малой величиной на данном этапе развития вычислительной техники.

Отметим отдельно, факт:

В июне 2003 года [Агентство национальной безопасности](https://ru.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8) США постановило, что шифр AES является достаточно надёжным, чтобы использовать его для защиты сведений, составляющих государственную тайну ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *classified information*). Вплоть до уровня SECRET было разрешено использовать ключи длиной 128 бит (AES-128).

Как мы видим, данные передаваемые по каналу, не имеют особой ценности для злоумышленников, так как даже в случае взлома не позволят предпринять никаких противозаконных действий.

# Базовая станция (БС)

Базовая станция Базовая станция представляет из себя мини компьютер к которому подключен приемник Lora и который имеет доступ в сеть интернет.

Так как миниПК является всего лишь ретранслятором данных, его