

Все операции динамических преобразований и передачи кодов выполняются с большой скоростью в строгой временной последовательности и традиционные методы глушения или перехвата посылок являются совершенно неэффективными.

Сам по себе любой диалог не дает гарантий невзламываемости системы, если его коды при каждом сеансе связи одинаковые или меняются по простому алгоритму. Резко снижается криптостойкость процедуры диалога, если используются неизменяемые коды во всех моделях у конкретной серии автосигнализаций.

Сложный динамический диалог в автосигнализациях Pandora DeLuxe принципиально разный у всех экземпляров систем, т.к. каждая система имеет уникальный ключ шифрования равный 80 бит. Более того, пользователи могут самостоятельно сменить ключ шифрования, если не доверяют предприятию-изготовителю.

Индивидуальный ключ шифрования формируется контроллером базового блока во время процедуры записи брелоков с использованием алгоритма генерации случайных чисел. Значение этого ключа в процессе процедуры записи брелока передается с базового блока на все прописываемые брелоки в системе и хранятся в их энергонезависимой памяти (для исключения сбоев и ошибок используется несколько записей ключа).

Конечно, примененные в Pandora столь бескомпромиссные методы защиты во многом чрезмерны, но такая защита радиоканала связи принципиально не оставляет возможностей для электронного взлома.

Состояние проблемы. Существование способов и устройств электронного взлома идентификационного диалога (авторизации) неизвестно и представляется вообще весьма маловероятным.



Вывод.

Эффективные методы защиты от интеллектуального взлома существуют и они доступны установщикам и водителям.

Вопрос же в том, как долго будет существовать их превосходство?