ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМОБИЛЯХ ДЛЯ ПРОТИВОДЕЙСТВИЯ УГОНУ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Козлов К. С.

Таболич Т. Г. – канд. техн. наук, доцент

Рассматриваются организационно-технические способы защиты информации в автомобилях для противодействия угону авто. В качестве таких мер предлагаются маскировка в автомобиле всех противоугонных средств, аутентификация при входе в ремонтные помещения станции техобслуживания, простейшее повышение общей грамотности персонала станции техобслуживания авто в области информационной безопасности.

В настоящее время существует множество программно-технических средств защиты от угона автомобилей (автоугона). Наиболее популярными из них являются контура противоугонной защиты с применением электромеханических и электронных устройств. Большое число производителей предлагает автовладельцам комплекты [1] своих противоугонных изделий этого вида. Такие комплекты не являются дешёвыми – стоимость их колеблется от 600 до 1400 $. В комплектах использованы стойкая криптография, автосигнализация с диалоговой авторизацией системы доступа, противоразбойные радиометки, биометрическое распознавание и обязательно сирена. Однако данные противоугонные изделия подвержены интеллектуальному взлому (синонимы: математический взлом, цифровой взлом), под которым понимается возможность обхода электромеханических и электронных контуров защиты от угона посредством алгоритмов, использующих электронную уязвимость средств защиты, без непосредственного воздействия на их элементы [2].

Наиболее яркими устройствами интеллектуального взлома на сегодня являются кодграбберы и ретрансляторы. В основе алгоритма работы грабберов лежит возможность вычисления посылок управления блоком сигнализации после анализа всего лишь одной перехваченной посылки управления [2]. Цена программно-аппаратных устройства интеллектуального взлома примерно соизмерима со стоимостью комплектов защиты авто от угона.

В этих условиях в докладе обсуждается комплекс организационно-технических мер по защите от угона. В отличие от программно-технических средств защиты организационные меры намного дешевле. Первой из таких мер предлагается маскировка в автомобиле всех противоугонных средств. При построении правильной защиты от угона нужно следовать одному простому правилу: охранный комплекс не должен иметь ни одного визуального элемента. Ничто не должно выдавать наличие хоть какой-нибудь защиты. Ни светодиодов, ни биперов, ни сканеров, ни матриц, открыто расположенных тумблеров и кнопок. Такая маскировка выполняется на станции техобслуживания и её цель – предотвратить использование для угона кодграбберов и ретрансляторов (а для чего их использовать, если противоугонных средств якобы нет?). А при обычном взломе в действие вступает сирена, и автовладелец предупреждается ею о наличии попытки угона.

Второй мерой из предлагаемого комплекса может быть выбор безопасной в плане утечки информации станции технического обслуживания. Действительно, попав на станцию под видом работника, злоумышленник может:

- определить наличие в авто дополнительного иммобилайзера;
- узнать месторасположение и название сигнализации;
- дописать в сигнализацию дополнительный пульт управления;
- дописать в память дополнительный чип-ключ для запуска двигателя;
- найти месторасположение аварийных тросов электромеханических замков капота;
- вывести тросы аварийного отпирания в нужное место.
- найти места возможного расположения блокировок двигателя, в том числе и подкапотных.

В докладе рассматриваются способы исключения ситуаций, когда на станцию техобслуживания попадают злоумышленники. К таким способам относится аутентификация при входе в ремонтные помещения станции и ряд других мероприятий, обсуждаемых в докладе.

Третьей мерой из предлагаемого комплекса может быть простейшее повышение общей грамотности персонала станции техобслуживания авто в области информационной безопасности [3], что намного дешевле, чем заводить на станции техобслуживания собственную службу безопасности.

Список использованных источников:

1. Комплекты для защиты от угона [Электронный ресурс]. – Режим доступа www.ugona.net/catalog25.html. – Дата доступа 27.12.2013.

2. Лаборатория Андрея Кондрашова. Интеллектуальный взлом [Электронный ресурс]. – Режим доступа www.kondrashov-lab.ru/v.../intellektualnyiy-vzlom/?. – Дата доступа 27.09.2013.

3. Джейкобсон Даг, Рурш Джулия. Информационная безопасность: научите персонал уважать её // Безопасность ИТ-инфраструктуры. – 2013. – № 10 (76). – С. 1-2.