УДК 62–519:629.053

Алефиренко Виктор Михайлович, Андрушкевич Виталий Сергеевич
Белорусский государственный университет
информатики и радиоэлектроники
(Минск, Беларусь)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМОБИЛЕЙ ОТ НЕСАНЦИОНИРОВАННОГО ДОСТУПА

Аннотация. *Рассмотрены современные способы защиты автомобилей от несанкционированного доступа и проанализированы основные уязвимости охранных систем автомобилей. Предложены решения, затрудняющие несанкционированный доступ при использовании штатных систем охраны автомобиля.*

Ключевые слова: *автомобиль, безопасность, охранная сигнализация, несанкционированный доступ, защита.*

Alefirenko Viktor Mihajlovich, Andrushkevich Vitaly Sergeevich
Belarus State University of Informatics and Radioelectronics
(Minsk, Belarus)

ENSURING THE CARS SAFETY FROM UNAUTHORIZED ACCESS

Abstract. *The modern methods of protecting cars from unauthorized access are considered and the main vulnerabilities of car security systems are analyzed. The solutions making hardening the unauthorized access when using regular car security systems are suggested.*

Keywords: *car, security, security alarm, unauthorized access, protection.*

В современном мире автомобили являются неотъемлемой частью повседневной жизни нашего общества и каждого человека. Сейчас практически для любого человека можно подобрать автомобиль, соответствующий его финансовым возможностям и желаниям. Современные автомобили сочетают в себе большое количество различных опций, делающих их максимально удобными в использовании. Кроме того, автомобиль для некоторой категории людей является не только предметом, выполняющим функции согласно потребностям его владельца, но и предметом роскоши. Однако автомобиль может использоваться не только по своему прямому назначению, но и как средство для осуществления террористических актов (как таранное средство для проникновения на объект, как взрывное устройство, как средство физического уничтожения людей и т.п.). Поэтому проблема обеспечения безопасности автомобилей от угона с каждым годом становится все более актуальной, также как и развитие различных видов защиты от этой угрозы.

Рассмотрим основные технические решения, применяемые для защиты автомобилей от несанкционированного доступа (системы защиты), способы обхода этих систем и соответствующие им способы, затрудняющие взлом систем в порядке их развития.

1. Механический ключ.

Это традиционное техническое решение является самым простым и менее защищенным. Суть его заключается в том, что автомобиль оснащается механическими замками, для открытия которых используются соответствующие ключи. Точно также происходит и запуск двигателя.

Для данного способа открытия дверей и запуска двигателя автомобиля существует два основных направления взлома – это различные операции с ключом (копирование ключа, использование специальных устройств – декодеров и турбодекодеров) и вандальские действия, при которых наличие ключа не требуется. Копирование ключа можно осуществить несколькими способами. Одним из них является похищение ключа для изготовления копии с его последующим возвратом. Возможна также ситуация, когда на станциях технического обслуживания недобросовестный работник делает копию ключа и в будущем, получив адрес владельца, ему или его сообщникам не составит труда угнать автомобиль. Потеря ключа также может привести к угону автомобиля. Декодеры и турбодекодеры представляют собой ключ с плавающими дорожками, которые позволяют реализовывать огромное количество вариантов исполнения ключа [1]. К вандальским способам взлома относятся такие способы открытия, как сворачивание сердцевины замка путем забивки в отверстие замка предмета отверткоподобной формы с последующим его поворотом, а также механический взлом замка (отжим двери).

Первоначальными способами защиты для данного способа открытия дверей и запуска двигателя автомобиля, было усложнение канавок и форм ключей, наличие нескольких ключей, которые использовались для разных функций, например, один ключ открывал дверь, а второй запускал двигатель [1]. Использовались также различные механические средства защиты, например, замок с подвижной сердцевиной, что позволило исключить сворачивание замка. Дополнительным средством защиты в автомобилях является установка автомобильных сигнализаций, которые позволяют повысить уровень защищенности автомобиля.

2. Механический ключ с иммобилайзером.

В настоящее время практически все автомобили снабжаются штатной системой охраны, препятствующей запуску двигателя без ключа, – иммобилайзером. Иммобилайзер – это противоугонное средство, выключение и включение которого должно быть доступно только владельцу автомобиля. Обычно, для этой цели может использоваться бесконтактный электронный кодовый ключ, ключ с ручным набором кода или скрытая кнопка. Большинство современных автомобилей оснащены простыми встроенными иммобилайзерами производителя автомобиля [2]. В шляпке ключа замка зажигания находится электронный транспондер (чип) (рис.1). Вокруг замка зажигания намотана специальная считывающая рамка (катушка). При включении зажигания катушка создает электромагнитное поле, которое проходит через чип. Чип получает энергию этого поля и передает свой код. Если код верный, иммобилайзер дает команду на запуск двигателя. Процедура опроса чипа проходит за достаточно короткий промежуток времени 0,5 – 1 секунду [3].

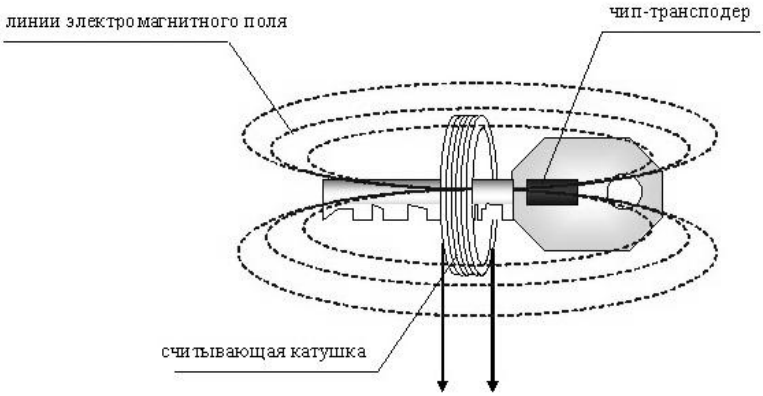

Рис. 1. Принцип работы иммобилайзера

Можно отметить следующие основные способы обхода штатного иммобилайзера с целью угона автомобиля:

– иммобилайзер, как и любая другая охранная система, имеет аварийный режим работы. При наличии необходимого аппаратного и программного обеспечения иммобилайзер вводится в аварийный режим через диагностический разъем. По цифровой шине в блок управления двигателем транслируются определенные исполнительные команды, разрешающие запуск двигателя без подтверждения положительного опроса чипа. Таким оборудованием завод-изготовитель снабжает только своих дилеров и в свободной продаже аппаратную, и тем более, программную часть простому обывателю достать невозможно;

– обход происходит путем подмены блока управления двигателем на блок с уже предустановленной новой конфигурацией оборудования (отключенным иммобилайзером, введенным в аварийный режим) такой же модели и такой же марки автомобиля. Способ используется в основном для «потокового» угона конкретной марки автомобиля;

– дублирование ключа на станции технического обслуживания. Недобросовестный мастер, работающий на станции, с помощью специального оборудования может «дописать» в память еще один чип-ключ и сделать «электронный слепок» с основного ключа [3].

К способам защиты от взлома ключей с иммобилайзером можно отнести следующие:

– установка дополнительной скрытой кнопки, о местоположении которой будет известно только владельцу автомобиля и без нажатия на которую завести машину невозможно;

– использование различных видов блокировок, препятствующих процессу подключения к автомобилю через диагностический разъем специального оборудования, позволяющего осуществлять перепрошивку электронного блока управления. Например, доступ осуществлять только через дилерское программное обеспечение или после ввода какого-либо пароля, использовать различного рода переходники для разъема или перенести

разъем в другое место, поиск которого усложнит злоумышленнику задачу;

– блокировка цифровой шины путем установки дополнительного электрического реле, что не позволит злоумышленнику записать информацию в блок сертификации ключей;

– осуществление ремонта автомобиля только на сертифицированных станциях технического обслуживания.

3. Ключ с дистанционным открыванием дверей.

Такая автомобильная сигнализация состоит из блока управления, входных и исполнительных устройств. К входным устройствам относятся пульт дистанционного управления и входные датчики.

Пульт дистанционного управления выполнен в виде брелока. В штатной сигнализации он совмещен с физическим ключом зажигания. С помощью брелока осуществляется постановка и снятие сигнализации с охраны, а также контроль состояния автомобиля. Связь между брелоком и блоком управления осуществляется по радиоканалу. Для защиты информации от перехвата производится ее кодирование. Различают статическое и динамическое кодирование. Статическое кодирование в настоящее время не используется. Динамическое кодирование имеет высокую степень защиты от перехвата, т.к. передаваемые пакеты информации никогда не повторяются (алгоритм кодирования построен на генераторе случайных чисел). Разновидностью динамического кодирования является диалоговое кодирование, которое реализуется по двухстороннему каналу связи (приемо-передатчик находится в брелоке и блоке управления). Сигнализация, реализующая диалоговое кодирование, называется сигнализацией с двухсторонней связью.

Входные датчики обеспечивают выполнение охранных функций сигнализации. Они фиксируют изменение различных физических параметров и преобразуют их в электрические сигналы. В конструкции автомобильной сигнализации используются следующие основные датчики: датчик удара, контактный датчик, датчик наклона, датчик объема. В ряде конструкций можно встретить и другие датчики – датчик движения, датчик разбития стекла, датчик обрыва электропитания, датчик падения напряжения и др. [4].

К способам взлома такой сигнализации относятся:

– сканирование радиоканала с применением сканеров-кодграбберов. Сканирование радиоканала первоначально использовалось для взлома ранних моделей автосигнализаций, которые имели легко различающийся код. Часто его можно было установить путём разборки брелока и центрального блока сигнализации с помощью микропереключателей. Со временем код начал удлиняться, поэтому перебор комбинаций вручную стал слишком трудоёмким и для этого стали использовать сканеры-кодграбберы. В состав сканера-кодграббера входит высокочувствительный приёмник, портативный компьютер, а также настраиваемый передатчик с компоновщиком частоты. Дополнительным устройством к сканеру-кодграбберу может быть антенна, позволяющая считывать и посылать эфирные посылки на определенное расстояние. Сканер-кодграббер способен прочитать код любой сложности, сделать анализ его структуры и попытаться его опознать. Алгоритм динамических изменений либо вычисляется, либо уже известен программному обеспечению. Далее происходит проектирование следующей посылки и

последующая его выдача в эфир. Эти устройства могут также ставить заградительные помехи, чтобы иметь достаточно времени для анализа информации последовательно меняющихся кодов брелока [5];

– применение электрошоковых приборов. В то время, когда появились первые автосигнализации, для вывода их из строя использовали электрошокеры. Чтобы взломать автосигнализацию, достаточно было разбить плафон сигнализатора поворота, вынуть лампочку, подключиться к её клемме и с помощью портативного электрошокера вывести из строя систему безопасности под воздействием высокого напряжения. На сегодняшний день большинство автосигнализаций оснащены устройством высоковольтной гальванической разрядки [6].

Поскольку в большинстве своём, автомобильные сигнализации осуществляют обмен по радиоканалу, то основная часть защиты автомобильных сигнализаций сводится к защите радиоканала:

– необходимо использовать сигнализации, имеющие динамический код, что затруднит использование различного вида сканеров;

– снятие и постановка автомобиля на охрану должна осуществляться владельцем, находясь рядом с автомобилем, тем самым затруднив злоумышленнику возможность перехвата сигнала;

– использование сигнализаций с более сложными алгоритмами шифрования, а также с наличием опций обратной связи (с модулями GPRS и GPS), что позволит немедленно реагировать на различные ситуации, связанные с автомобилем (отслеживать местоположение автомобиля, получать уведомления о состоянии системы сигнализации и т.п.);

– оснащать автомобили высоковольтными разрядниками.

4. Бесключевой доступ.

По отраслевой терминологии такие системы называются PKES (Passive Keyless Entry Start – пассивный бесключевой доступ и запуск двигателя). Такая система предназначена для открывания двери автомобиля и запуска двигателя без использования привычного отпирающего устройства.

Бесключевой доступ – это система доступа к автомобилю с использованием особой электронной карты (смарт-ключа). Компьютер автомобиля на небольшом расстоянии обменивается кодами со смарт-ключом, идентифицирует его и дает команду на открытие дверей. При удалении на некоторое расстояние компьютер теряет смарт-ключ из виду и запирает автомобиль [7].

Основными составляющими элементами бесключевой системы доступа являются: транспондер (представляет собой сочетание микросхем с антенной, расположенных внутри корпуса); антенна (обеспечивает связь транспондера с автомобилем); датчики касания (как правило, располагаются на дверных ручках и являются своеобразным ключом); кнопка запуска двигателя (переключатель); блок электронного управления**.**

Такая система доступа имеет установленный алгоритм работы. Он заключается в том, что водитель, касаясь ручки двери машины, запускает работу индуктивного датчика. Датчик, в свою очередь, передает сигнал и считанную информацию на блок управления. Блок управления при помощи антенны передает информацию на транспондер, который выполняет функцию распознавателя, поскольку по поступившему сигналу определяется

положение смарт-ключа (автовладельца) относительно транспортного средства. При наличии смарт-ключа в радиусе действия системы, транспондер получает определённый ответ на свое сообщение. На основании принятого транспондером решения сигнал передается на центральный замок (приемную антенну) и противоугонную сигнализацию. Таким образом, выключается охранная сигнализация, и центральный замок открывает дверь. Запуск двигателя производится путем нажатия специальной кнопки, после чего сигнал «Старт» передается на блок управления и через антенну на смарт-ключ, который обозначает свое расположение (расположение автовладельца) внутри автомобиля и передает информацию на центральный замок и противоугонную сигнализацию. После передачи сигнала происходит отключение противоугонной блокировки и передается запрос о готовности запуска. При получении положительного результата запуск двигателя происходит автоматически [8, 9].

Современные бесконтактные смарт-ключи, которые позволяют водителю автоматически открывать двери и без ключа запускать двигатель, уязвимы для взлома через радиоканал. Для этого может использоваться следующая схема устройства для перехвата сигнала (рис. 2) [10].

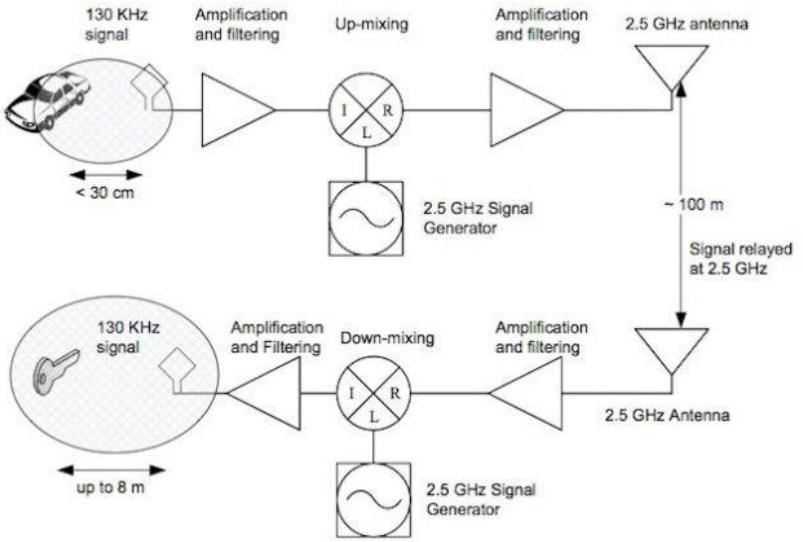

Рис. 2. Схема устройства для перехвата сигнала

Главной задачей для злоумышленника является перехват сигнала, который передает брелок на блок сигнализации автомобиля. Далее сигнал записывается специальным модулем в память, но сразу не передается на блок сигнализации автомобиля. Затем с помощью другого модуля (ретранслятора), записанный сигнал передается по специальному радиоканалу на устройство злоумышленника, находящегося около

автомобиля. Это устройство преобразовывает полученный аналоговый сигнал в цифровой и передает его на другое устройство с антенной, которое имитирует заводской ключ-брелок, передающий сигнал на автомобиль. Охранная сигнализация автомобиля воспринимает фальшивый дистанционный ключ за заводской и автоматически открывает двери автомобиля. Для передачи информации, перехваченной с брелока (смарт-ключа), используется ретранслятор (рис. 3) [11].

Возможность его использования заключается в том, что информация между блоками передается без цифровой обработки сигналов методом прямого переноса спектра, что позволяет уложиться в лимит времени, отведенный системой доступа автомобиля на диалог со смарт-ключом. Необходимо отметить, что все перечисленные ранее способы доступа с подключением к диагностическому разъему также актуальны и для систем бесключевого доступа.

Рис. 3. Типовая схема работы ретранслятора.

В качестве способов защиты бесключевой системы доступа от взлома можно рекомендовать следующие:

– уменьшение радиуса действия приемника и передатчика смарт-ключа, что затруднит приближение злоумышленника к автомобилю;

– использование различного рода фольгированных (экранированных) чехлов для смарт-ключа, основанных на принципе «клетки Фарадея», что позволит полностью подавить сигнал;

– оснащение модуля смарт-ключа кнопкой отключения питания;

– изъятие источника питания из модуля смарт-ключа после постановки автомобиля на сигнализацию, если кнопка отключения питания отсутствует;

– отключение штатного радиоканала и перевод управления модулем смарт-ключа на блок стороннего производителя, управляемого своей меткой;

– использование «интеллектуального» модуля защиты, позволяющего анализировать радиообстановку вокруг автомобиля, выявлять работу радиоудлиннителя и противостоять ему (создавать заградительную помеху в выявленном диапазоне частот его работы);

– использование «умного» программного обеспечения, которое может определять, насколько близко смарт-ключ находится от автомобиля;

– использование дополнительной радиометки, которая работает в другом диапазоне и по другому алгоритму, чем штатная система бесключевого доступа;

– блокировка доступа к диагностическому разъему и цифровой шине.

К способам взлома системы защиты можно отнести: доступ к диагностическому разъему и прошивка новых ключей, использование ретрансляторов, позволяющих увеличить радиус опроса сигнализации. К способам защиты – уменьшение радиуса действия системы сигнализации, использование фольгированных чехлов для брелока, ввод дополнительных радиометок, использование «интеллектуальных» модулей защиты, оснащение смарт-ключа кнопкой выключения питания, изъятие источника питания из брелока после постановки автомобиля на охрану, блокировка доступа к диагностическому разъему и цифровой шине.

Рассмотренные технические решения, применяемые для защиты автомобилей от несанкционированного доступа (системы защиты), способы обхода этих систем и соответствующие им способы, затрудняющие взлом систем, сведены в табл.1.

В заключение необходимо отметить, что методы взлома развиваются и совершенствуются злоумышленниками одновременно с развитием систем защиты, но с некоторым опозданием по времени. И, в конечном итоге, на любую систему защиты найдется способ ее взлома. Вопрос только времени и подготовленности злоумышленника. Однако, если вопрос подготовленности злоумышленника автовладельцы контролировать не могут, то вопрос затруднения взлома и усилий, затраченных злоумышленником, могут вполне. Использование соответствующих способов защиты позволит автовладельцу выиграть время у злоумышленника и, тем самым, повысить вероятность того, что автомобиль не будет угнан.

Таблица 1. Виды ключей, способы их взлома и защиты

Вид ключа	Способ взлома (доступа)	Способ защиты
Механический ключ	– Подбор ключа; – Копирование ключа; – Механический взлом замка.	– Не терять ключи из вида; – Использование замков с плавающими сердцевинами; – Ремонт на сертифицированных СТО; – Использование иммобилайзеров и автомобильных сигнализаций.
Механический ключ с иммобилайзером	– Подключение через диагностический разъем и перепрошивка электронного блока управления; – Копирование ключа.	– Ввод дополнительной скрытой кнопки включения; – Блокировка доступа к диагностическому разъему и цифровой шине; – Ремонт на сертифицированных СТО.

Ключ с дистанционным открыванием дверей	– Сканирование радиоканала с применением сканеров-кодграбберов; – Применение электрошоковых приборов.	– Использование сигнализаций с динамическим кодом; – Использование более сложных сигнализаций с наличием дополнительных модулей, позволяющих осуществлять контроль автомобиля в реальном режиме времени (GPS, GPRS и т.п.); – Оснащение автомобилей высоковольтными разрядниками.
Бесключевой доступ	– Использование ретрансляторов; – Подключение через диагностический разъем и перепрошивка электронного блока управления.	– Уменьшение радиуса действия систем сигнализации; – Использование фольгированных чехлов для смарт-ключа; – Оснащение смарт-ключа кнопкой отключения питания; – Изъятие источника питания из модуля смарт-ключа после постановки на охрану; – Отключение штатного радиоканала и перевод управления модулем смарт-ключа на блок стороннего производителя, управляемого своей меткой; – Использование «интеллектуальных» модулей защиты; – Использование «умного» программного обеспечения; – Ввод дополнительных радиометок; – Блокировка доступа к диагностическому разъему и цифровой шине.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Колёса [Электронный ресурс]. – Режим доступа: http://www.kolesa.ru/article/evolyutsiya-klyucha-zazhiganiya-1-2014-05-15.html/.
2. Infocar [Электронный ресурс]. – Режим доступа: http://www.infocar.ua/term_immobiliser.html/.
3. Лаборатория Андрея Кондрашова [Электронный ресурс]. – Режим доступа: http://www.kondrashov-lab.ru/v-tyilu-vraga/chto-takoe-immobilayzer-a-chast-1.html/.
4. Системы современного автомобиля [Электронный ресурс]. – Режим доступа: http://systemsauto.ru/another/car-alarm.html/.
5. 365cars [Электронный ресурс]. – Режим доступа: http://365cars.ru/soveti/vzlom-avtomobilnoy-signalizatsii.html/.
6. Alamtrade [Электронный ресурс]. – Режим доступа: http://www.alarmtrade.ru/articles/25.html/.
7. За рулем.рф [Электронный ресурс]. – Режим доступа: http://wiki.zr.ru/Бесключевой_доступ/.

8. CamaFon.ru [Электронный ресурс]. – Режим доступа: http://camafon.ru/skud/sistema-dostupa-bez-klyucha/.
9. Mashintop.ru [Электронный ресурс]. – Режим доступа: http://mashintop.ru/articles.php?id=2799/.
10. International Association for Cryptologic Research [Электронный ресурс].– Режим доступа: https://eprint.iacr.org/2010/332.pdf/.
11. Авторевью [Электронный ресурс]. – Режим доступа: https://autoreview.ru/articles/ugon-shou/klyuch-s-pravom-peredachi.html/.