

**авто**  
*шпаргалка*

Н. Г. Еремич

# КАК ИЗБЕЖАТЬ **УГОНА**



**СИСТЕМЫ  
БЕЗОПАСНОСТИ  
АВТОМОБИЛЯ**

 **ПИТЕР®**

Наталья Еремич

**Как избежать угона. Системы  
безопасности автомобиля**

«Питер»

2011

**Еремич Н. Г.**

Как избежать угона. Системы безопасности автомобиля /  
Н. Г. Еремич — «Питер», 2011

Прочитав книгу, вы удивитесь тому, что дверь автомобиля открывается обыкновенной проволокой, сирена и иммобилайзер «убиваются» практически голыми руками, зажигание включается без ключа... и поймете, как с этим бороться. Вы узнаете, зачем угоняют машины, какова их дальнейшая судьба, как их ищут и почему не находят. Читайте, что делать, если страшное все-таки случилось, как вести себя с представителями власти, страховой компании и даже с самими угонщиками, требующими выкуп за то, что и так вам принадлежит. Защищайте себя и свою собственность!

© Еремич Н. Г., 2011

© Питер, 2011

# Содержание

Введение	5
Глава 1. Вашу машину угнали? Алгоритм действий	6
Глава 2. Возможные сценарии и способы угона	9
Кража	10
Кодграбберы	13
Конец ознакомительного фрагмента.	17

# **Н. Г. Еремич**

## **Как избежать угона. Системы безопасности автомобиля**

### **Введение**

В редких случаях, став обладателем долгожданного автомобиля, человек в первую очередь задумывается о безопасности и сохранности своего драгоценного приобретения. Как правило, новоиспеченного автовладельца сначала переполняют эмоции (мечта сбылась), вслед за ними возникает непреодолимое желание кататься, кататься и кататься, затем понемногу голова остывает от вылезших наружу проблем и неисправностей, в результате человек погружается в заботы об их устранении...

И только потом, спустя несколько недель, когда утихают эйфория и страсти бесконечного ремонта, автовладелец вспоминает, что машина-то закрывается только центральным замком (в лучшем случае). И даже если установлена сигнализация, она постоянно глючит, не срабатывает и орет на всю округу... Но на это человек обращает мало внимания, потому как есть другие, более важные неисправности, которые, в отличие от полуробочей системы безопасности, влияют на скорость. Именно поэтому нередко люди лишаются автомобилей в первые неделю-две после покупки.

Справедливости ради отмечу, что столь невнимательны к сохранности авто далеко не все новоиспеченные владельцы. Есть и другая категория, к которой принадлежат товарищи, которые немедленно после покупки машины отправляются в гараж к дяде Ване – мегаэлектрику, который, как умеет, ставит «самопальную сигналку» за умеренную плату, после чего хозяин машины обретает твердую уверенность, что построил китайскую стену на пути воров к автомобилю... Да каких там воров! Как раз водители данной категории ставят сигнализацию на машину не в целях безопасности, а просто потому, что она должна быть априори, как руль или колеса. Об угоне никто и не задумывается, ведь «ЭТО может случиться с кем угодно – только не со мной!». Немалую роль здесь играет и суеверие: чем больше боишься чего-то, тем больше вероятность, что это случится. И к литературе, подобной этой книге, люди обращаются зачастую уже после того, как ЭТО случилось, когда «Боржоми» пить поздно. Хотя... будет еще машина, и не одна...

Ведь никто не говорит о том, что каждый автовладелец должен ждать угона. Речь как раз о бдительности и осведомленности. Необходимо знать, как могут угнать вашу машину и что может этому помешать, чему и посвящена данная книга. Прочитав ее, вы узнаете, как «уводят» автомобили в течение 1–3 минут среди бела дня и под покровом ночи, как мошенники «разводят» беспечных автовладельцев и отнимают машины почти без усилий, а также о других способах автоворовства. А главное – вы узнаете, как с этим бороться и какие слабые места есть у той или иной марки автомобиля на предмет хищения. Читайте также о том, зачем угоняют машины, какова их дальнейшая судьба, как их ищут и почему не находят. Что делать, если страшное все-таки случилось, как себя вести с представителями власти, страховой компании и даже с самими угонщиками, требующими выкуп за то, что и так вам принадлежит. Как вновь не потерять то, что нашли и вернули вам по закону. Чем живут, руководствуются, промышляют воры-обидчики и какое наказание за это несут – об этом также написано в книге. И еще много полезной, интересной и познавательной информации.

Читайте с удовольствием, вооружайтесь и защищайте себя и свою собственность!

## Глава 1. Вашу машину угнали? Алгоритм действий

Что бы ни случилось в жизни, в том числе и угон машины, не стоит впадать в истерику – прежде всего соберитесь с мыслями. И помните: если вы вышли из офиса (из дома или магазина) и не нашли машину там, где оставили, это вовсе не значит, что ее угнали. В ваше отсутствие ее мог утащить эвакуатор на штрафстоянку из-за парковки в неположенном месте, дорожные службы вместе с работниками ГИБДД могли передвинуть ее на другое место, потому как она мешала, к примеру, убирать улицу от снега или листвы. Поэтому первым делом окиньте взглядом прилегающую территорию, одновременно набирая 02 на мобильном телефоне.



Если все-таки выяснится, что автомобиль не утащил эвакуатор, а, скорее всего, его украли, незамедлительно принимайте меры по поиску. В этом деле дорога каждая минута, потому что воры постараются как можно быстрее покинуть место преступления и спрятать машину. Хуже того – отправить на авторазборку или сбыть покупателям. Поэтому действуйте оперативно.

► Когда дозвонитесь по номеру 02, сразу же сообщите дежурному, что вашей машины нет там, где вы ее оставили час назад. В случае угона это вдвойне необходимо сделать в первые же минуты, так как на вашей машине могут совершить наезд на человека или скрыться после ограбления банка. Кроме того, чем раньше органы внутренних дел узнают о пропаже, тем больше шансов найти автомобиль.

► Пока будете ждать полицию<sup>1</sup>, осмотрите ближайшие окрестности в районе того места, где находилась машина. Нередко бывает и так, что угонщики бросают добычу где-нибудь неподалеку до тех пор, пока в районе не утихнут оперативноразыскные мероприятия, связанные с угоном. Кроме того, не исключено, что воры – вовсе не матерые автоугонщики, а какая-нибудь шпана, которая покаталась и бросила автомобиль в соседнем дворе.

---

<sup>1</sup> Слово «полиция» в книге употребляется вместо «милиция» в соответствии со вступлением в силу с 1 марта 2011 года Федерального закона от 7 февраля 2011 года № 3-ФЗ «О полиции». – Примеч. ред.

► Если вблизи от того места, где до исчезновения находился ваш автомобиль, расположены дорогие кафе, рестораны, бутики, банки и другие подобные заведения, поинтересуйтесь, нет ли у них систем видеонаблюдения и не захватывают ли камеры нужную территорию. Естественно, при этом будьте готовы к тому, что видеозапись вам в руки не отдадут, но вы сможете подсказать приехавшим полицейским, что она в принципе есть.

► Поговорите с персоналом этих же заведений. Вдруг кто-то стал невольным свидетелем угона вашего авто и помалкивает просто из страха. По возможности запишите номера их телефонов. Не забывайте: чем больше информации вы соберете, тем больше вероятность вернуть автомобиль.

► Если машина оборудована системой спутниковой сигнализации, свяжитесь с диспетчером и сообщите об угоне авто.

► Если ваш автомобиль застрахован (а иначе и быть не может), позвоните в страховую компанию и также заявите об угоне машины. Конечно, об этом вас спросят по телефону, но все же не забудьте указать свои данные как страхователя, по возможности номер страхового полиса (если документы не остались в бардачке), а также контактный телефон и расскажите вкратце об обстоятельствах происшествия. Оператор должен разъяснить, как вам действовать дальше и какие собирать документы, чтобы получить страховку в случае, если автомобиль не найдется.

► Когда приедет полиция, опишите ситуацию.

► После первичных оперативно-следственных мероприятий вас, скорее всего, направят в ближайшее отделение полиции, на территории которого был совершен угон, где вы напишете официальное заявление. Кстати, возьмите у принявшего заявление сотрудника контрольный талон и выясните, кто будет заниматься расследованием этого дела и куда его передадут. Официальное заявление об угоне машины послужит своего рода гарантией того, что страховая компания признает ваш случай страховым и не откажет в выплате страхового возмещения.

► В заявлении вас попросят указать контактные данные (фамилию, имя, отчество, адрес) и, естественно, регистрационный номер, марку и цвет угнанной машины. Потребуется вспомнить и некоторые подробности минувших дней, а также особые приметы автомобиля:

- ◆ когда, где и у кого вы купили машину;
- ◆ кто, кроме вас, имел право управления машиной, то есть была ли оформлена доверенность на другого человека; у кого находились дубликаты ключей;
- ◆ пробег автомобиля и количество топлива в баке на момент исчезновения;
- ◆ теряли ли вы когда-либо документы на машину;
- ◆ какая сигнализация установлена;
- ◆ метки (если таковые имеются) на основных деталях и агрегатах: где и когда они наносились.

Также к особым приметам относятся марка и модель автомагнитолы (колонок, усилителей и т. д.), аэрография, царапины и другие повреждения кузова, его ремонт (покраска, удаление вмятин и т. п.). Кроме того, важно вспомнить, какие вещи или предметы находились в салоне или багажнике (документы, журналы, сувениры, брелоки, инструменты, часы, одежда). Кстати, неплохим подспорьем для поисков послужат фотографии вашего автомобиля.

Затем со справкой о факте обращения в полицию (о возбуждении уголовного дела) по поводу угона автомобиля отправляйтесь в страховую компанию, где застрахована ваша машина: необходимо правильно (в письменной форме) сообщить страховщику о факте угона. Кстати, на это дается **всего 2 дня**. После этого вы проведете 2–3 месяца в ожидании – или страхового возмещения, или найденного автомобиля. Как правило, столько времени полиция ищет похищенное авто. А затем, если поиски безрезультатны, выносится решение о приостановлении уголовного дела (согласно Уголовно-процессуальному кодексу РФ). И только после

этого на основании соответствующей справки из полиции (о приостановлении дела) выплачивается страховка.

### **КСТАТИ**

Существует негласная закономерность: если в течение 2 месяцев вашу машину не отыскали, шансы найти пропажу резко снижаются: скорее всего, она переделана, перепродана и легализована в другом регионе.

**Что делать, если автомобиль угоняют у вас на глазах?** Хотя и нечасто, но подобное случается. Поэтому, если вы заметили открывающего ваш автомобиль или, того хуже, сидящего в ее салоне совершенно незнакомого субъекта, не подходите слишком близко (жизнь и здоровье дороже) и немедленно принимайте меры: позвоните по номеру 02, наблюдая за происходящим. Постарайтесь привлечь внимание прохожих, чтобы были свидетели преступления. Ведь из-за особенностей Уголовного кодекса иногда очень сложно в суде обвинить преступника в краже: многие подобные дела разваливаются из-за недостатка улик, поскольку преступление квалифицируется как неправомерное завладение транспортом без цели хищения, что влечет за собой гораздо меньшую ответственность, чем кража (подробнее об этом будет написано в одной из следующих глав).



Если машина уже тронулась с места, не стойте на пути движения. Кричите, привлекайте внимание окружающих. Можно даже бросить в сторону авто какой-нибудь предмет (камень, например), чтобы разбить фару или стекло своей же машины. Это потом можно поправить, а вот если у угонщика что-то пойдет не так, есть вероятность, что он оставит машину и убежит.



## **Глава 2. Возможные сценарии и способы угона**

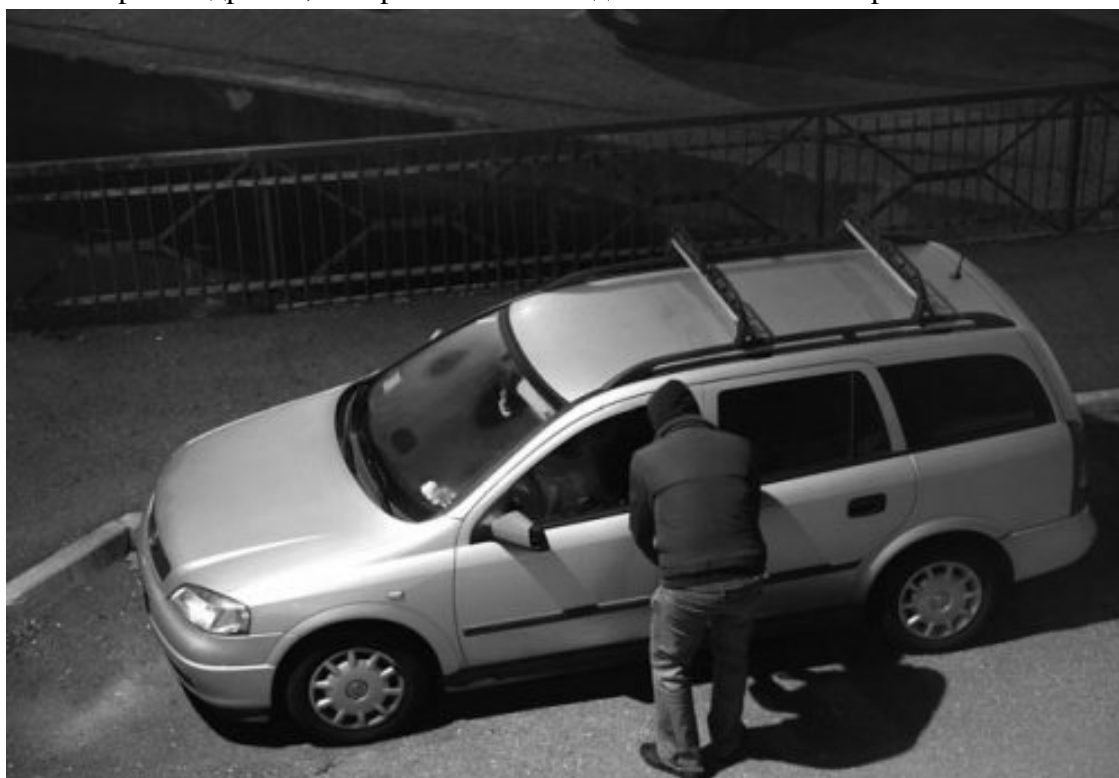
Способы угона автомобилей можно разделить на три большие группы.

- ▶ Тайное хищение (кража): вы вышли из дома, офиса, магазина, а машины нет; как это произошло, вы не видели.
- ▶ Явное хищение (разбой): происходит прямо в присутствии владельца авто, как правило, с применением насилия.
- ▶ Мошенничество: вы сдаете машину в аренду или даете другу покататься, а ее продают на запчасти. Вам говорят, что автомобиль угнали.

## Кража

Чтобы украсть (то есть тайно похитить) чужую машину, угонщики чаще всего пользуются следующими методами: крадут ключи у беспечных водителей, нередко прибегая при этом к помощи карманников; вскрывают замки отмычками; если машина оборудована сигнализацией или спутниковой охранной системой, используют «глушилки» и код грабберы; гораздо реже разбивают стекла (как правило, в недорогих отечественных машинах).

Ключи воруют в магазинах, кафе, ресторанах и в других местах, где бывает большое скопление людей. Поэтому будьте осторожны! Кстати, преступники нередко используют и более изощренный способ открыть машину вашим же ключом – делают его дубликат следующим образом. Хозяин оставляет машину в сомнительном автосервисе, пусть даже на очень короткое время, а на следующий день ее угоняют из двора его дома. Поэтому и к выбору автосервиса нужно подходить крайне ответственно. Хотя для самих угонщиков такой способ достаточно рискован, а соответственно, и не популярен, потому что в случае угона сомнительный автосервис станет первым адресом, который посетит следователь в поисках пропажи.



Теперь поговорим о незащитности сигнализаций и спутниковых систем. «Глушилки» – это специальные устройства, заглушающие сигнализацию. Данный прибор, как и любое другое радиоустройство, работает на определенной частоте вещания. В случае попытки угона автомобиля – на той же частоте, что и сигнализация, которой оборудована машина. Разница лишь в том, что мощность «глушилки» намного выше и сигнал сильнее. Поэтому сигнал тревоги, который подает на брелок система охраны, просто не приходит по назначению, а подавляется более мощным устройством. Таким образом, сигнализация не отключается, она срабатывает, но ее импульсы заглушаются.

Есть элементарное решение этой проблемы – брелок сигнализации, который будет постоянно обмениваться сигналом с автомобильной охранной системой. В случае прерывания сигнала на брелоке появится сообщение. Это будет означать, что что-то не так. Правда, есть одно «но» – велика вероятность ложных срабатываний.

Еще один вариант воровства машины с помощью «глушилки» – заставить самого хозяина отключить сигнализацию и закрыть автомобиль только на ключ. Это добавит миллион шансов вскрыть и увести «железного коня» тихо и быстро. У каждого автомобилиста хотя бы единожды не срабатывала сигнализация при попытке поставить авто на охрану. Вспомните свою реакцию или представьте, что бы вы подумали. Наверняка примерно следующее: «Что же делать? Наверное, села батарейка в пульте... Закрою пока на ключ – завтра разберемся». Дальше – дело техники. Злоумышленник спокойно вскрывает ваш автомобиль какой-нибудь нехитрой отмычкой и уезжает.

Но опять-таки есть решение и этой проблемы – иммобилайзеры с так называемой активной меткой. Если не срабатывает сигнализация, то есть иммобилайзер не может получить от нее метку (что вполне может случиться, если включена «глушилка»), автомобиль все равно самостоятельно закроется на охрану через какое-то время, которого будет достаточно, чтобы преступник не успел угнать машину. Но если вы закрыли авто именно таким образом, то снять его с охраны можно только с помощью дополнительной кнопки, установленной в секретном месте и предназначенной для отпирания автомобиля без ключа сигнализации. Единственное, место это должно быть уж очень секретным.

В ходу у автоугонщиков и такое оборудование, как подавитель GSM- и GPS-сигналов. Вообще это устройство имеет вполне мирное назначение: основная его функция – конференц-связь. Поэтому данное чудо техники находится в свободной продаже, запретить которую никто не может. Это как раз и на руку угонщикам: все спутниковые охранные устройства оснащены встроенным GSM-модемом, который передает информацию через GSM-тракт в виде СМС, голосовых звонков, GPRS. «Глушилка» нейтрализует передачу данных, в том числе сигналы тревоги и координаты автомобиля. Радиус действия такого устройства – до 15 метров, но этого вполне достаточно для того, чтобы нейтрализовать сигнал тревоги или сигнал выхода на связь спутниковой охранный системы для определения координат автомобиля.

Еще один наиболее популярный способ отключения сигнализации – сканирование путем подбора кода. Происходит все следующим образом. С помощью специального устройства – кодграббера – радиосигнал, который подает брелок, перехватывается и повторно используется для отключения сигнализации. Кодграббер перехватывает сигнал путем простого перебора.

Средством защиты от него является антисканер (функция сигнализации, дающая возможность обнаруживать попытку подбора кода и блокировать радиосигналы). Еще один способ защиты – динамический код брелока, который меняется при каждом нажатии на кнопку постановки/снятия с охраны. Здесь уж, как говорится, кто кого.

Есть и более хитрый, чем предыдущий, кодграббер с кодозамещением. Он позволяет обмануть автосигнализацию с динамическим кодом, в результате чего взломщику удастся заполучить не то что действующую, но даже еще и не использовавшуюся команду брелока. Однако, как известно, против лома нет приема, кроме второго лома. Так что и в этом случае есть средство защиты – просто закрепите команды включения-выключения сигнализации за разными кнопками!

Успокоились? Как бы не так! И на это у автомобильных воров есть ответ – алгоритмический кодграббер, который отключает сигнализации, распознавая, какие кнопки брелока нажимает хозяин машины... И вот вам средство защиты – принципиально новая система кодирования брелока и сигнализации «диалоговый код», основанная на принципе «свой – чужой».

И помните, в отличие от 1990-х годов, сегодня кодграббер – это не ноутбук с «приблудой», а устройство, которое может выглядеть как сотовый телефон, всем знакомый «Тетрис» и даже как брелок автомобильной сигнализации.



Еще один относительно несложный метод угона – поиск GSM-и GPS-антенн трансляторов, установленных в автомобиле, и ликвидация передатчиков. При этом угонщик может элементарно вскрыть пластик в салоне, чтобы найти антенну, или использовать для этого специальное устройство – индикатор поля (или детектор поля). В результате такого вмешательства извне охранная система просто не в состоянии передавать координаты автомобиля или тревожные сигналы.

Наконец, наиболее сложный и требующий интеллекта способ угона автомобилей (преимущественно дорогих) – подмена базовой станции или ретранслятора. Замена подлежат как раз те вышки, которые мы привыкли видеть на крышах административных зданий. Установленное оборудование выдает себя за настоящую станцию, и модем в спутниковой охранной системе, естественно, принимает его за ретранслятор и поддерживает с ним обмен информацией. Таким образом, в случае появления различных сигналов тревоги реальной передачи данных между брелоком и непосредственно сигнализацией не происходит. Фактически система охраны информирует об опасности того, кто ее и создает, – подставной ретранслятор.

#### **КСТАТИ**

Это оборудование, выступающее в качестве фейковой базовой станции, называется EMSI-catcher и нередко применяется для прослушивания трафика GSM.

В этом случае оптимальный метод защиты – контроль канала связи, который применяется в ряде изделий некоторых производителей охранных систем автомобилей и спутниковых операторов.

Например, в качестве защиты можно применять клон SIM-карты. В случае необходимости ее может сделать оператор сотовой связи по запросу владельца номера. Таким образом, у одного телефонного номера могут быть две (а то и больше) SIM-карты. Зачем это нужно? Элементарно для проверки работоспособности спутниковой системы, установленной на автомобиль. Робот-оператор периодически звонит системе, и удачная попытка означает, что автомобиль под контролем. В случае опасности клон SIM-карты дает возможность получить верный сигнал, в то время как основная карта подавлена «глушилкой».

Не забывайте еще и о том, что автоугонщик может отключить охранный комплекс, помешать блоку управления (которые, как будто специально, ставятся на видные или предсказуемые места), с легкостью завести автомобиль и радостно уехать. Но его радость может быть недолгой, если, например, кроме множества охранных комплексов, у вас в авто стоит фотокамера, делающая снимки при посадке на сиденье...

Чем больше полезных, правильно установленных и настроенных противоугонных устройств в вашем автомобиле, тем сложнее работать автоугонщику.

Сейчас подробнее рассмотрим наиболее популярные устройства, которые применяются при угонах транспортных средств. Основная цель – показать различные методики взлома, чтобы у вас была возможность логически строить правильные охранные комплексы и применять при защите автомобиля стойкие к электронному или механическому взлому комплектующие.

Не зная современных способов, которые используют угонщики автомобилей, невозможно грамотно подходить к выбору защитных устройств. Необходимо регулярно исследовать эти факторы, чтобы максимально обезопасить свой автомобиль. То есть чтобы найти «противоядие», нужно изучить «болезнь». Ведь именно так поступают и преступники: как только на рынке появляется новое средство защиты, они тут же изобретают метод борьбы с ним. Поэтому, кстати, очень важно применять при защите автомобиля от угона несколько средств в комплексе. Согласитесь, чтобы справиться с целым набором препятствий, злоумышленнику понадобится немало времени, и высока вероятность, что он откажется от похищения именно вашей машины.

Итак, чем же пользуются автоворы?

## Кодграбберы

Разработчики средств взлома идут нога в ногу с коллегами, которые изобретают средства защиты, – об этом уже упоминалось выше. Так, на заре возникновения противоугонной сферы в России, в лихие 90-е, хитом номер один у автоугонщиков был кодграббер статического кода. Перед ним были бессильны системы со статическим сигналом радиобрелока. К списку вскрываемых сигнализаций можно отнести практически весь модельный ряд предлагаемой в то время продукции.

Новые разработки в сфере устройств для взлома автосигнализаций появились вслед за новинками итальянских и российских производителей средств защиты. Вскоре за статическими устройствами рынок предложил преступному миру *кодграббер с замещением* (замещающий кодграббер), *кодграббер с ретрансляцией* и *алгоритмический кодграббер*.

**Замещающий кодграббер**, как правило, вмонтирован в корпус игрушки «Тетрис» и действует против систем с динамическим кодом.

Для начала разберемся, как работает сама сигнализация. Основной принцип действия устройств с динамическим кодом заключается в том, что каждая следующая посылка брелока сильно отличается от предыдущей, даже если нажимается одна и та же кнопка (кстати, при ста-

тическом коде все послышки при нажатии одной кнопки одинаковы). Посылка брелока состоит из двух частей: открытой и шифрованной. Открытая посылка содержит уникальный номер брелока и информацию о том, какая кнопка нажата. Шифрованная указывает на номер нажатия, который увеличивается при каждом нажатии любой кнопки. Это как раз и обеспечивает динамичность кода. Сигнализация принимает посылку, убеждается в том, что ее отправил брелок с номером, который она знает, и расшифровывает вторую часть посылки – номер нажатия. Дальше сигнализация анализирует, больше или меньше последнего поступавшего номер нажатия. Если номер меньше, значит, это нажатие уже отработывалось и оно игнорируется. Если больше предыдущего, команда принимается.

Кстати, брелок не знает о функциях сигнализации, он лишь отправляет информацию о том, какая кнопка нажата. Дальше сигнализация сама разбирается, как именно на это реагировать. Поэтому один и тот же брелок можно использовать как при однокнопочной, так и при двухкнопочной системе постановки/снятия.



Как раз однокнопочная система и есть лазейка для замещающего кодграббера. Взламывается она следующим образом.

Понятно, что нажатие одной и той же кнопки приводит к смене состояния сигнализации «охрана/не охрана». И даже если вы нажимаете разные кнопки на брелоке в случае их наличия, система понимает это действие как нажатие одной и той же кнопки. В это время кодграббер перехватывает первую посылку, которую отправляет брелок, и искажает так, что сигнализация ее не принимает и не ставится на охрану. При этом у граббера она сохраняется в правильном виде. Затем средство для взлома перехватывает вторую посылку и вместо нее отправляет системе перехваченную первую. Подмена занимает доли секунды и почти незаметна владельцу. Сигнализация ставится на охрану, водитель уходит, после чего кодграббер передает системе перехваченную вторую посылку и сигнализация снимается с охраны.

Метод борьбы – *переход к двухкнопочной системе постановки/снятия*, когда закрывает машину одна кнопка, а открывает другая. При этом у каждой свои коды.

Кодграббер с ретрансляцией работает по принципу, собственно, самой ретрансляции, что означает прием сигналов в промежуточном пункте, их усиление и передачу в прежнем или

в другом направлении. В принципе, ретрансляция предназначена для увеличения дальности связи.

Такой кодграббер применяется для взлома автосигнализаций и иммобилайзеров, оборудованных сложными системами кодирования, такими как «диалоговый код», когда происходит передача сигнала от одного объекта к другому на большом расстоянии через вспомогательные электронные устройства.

Принцип работы кодграббера с ретрансляцией строится, кроме всего прочего, на способности создавать помехи различных типов в сочетании с неустойчивой психикой владельцев автомобилей.



Простой пример. Как ведет себя клиент автоугонщика, стоя перед запертой (реже – незапертой) машиной, если его брелок подавлен помехой? То, что описано ниже, не шутка, не курьез, а суровая действительность.

Итак, в 90 случаях из 100 происходит следующее.

1. Преступник кодграббером ставит помеху без выдачи ответа. Посылки фиксируются.
2. Автовладелец давит на открывающую кнопку 5-10 секунд, тут же пробует другую (номер кнопки фиксируется изделием).
3. Внимательно смотрит на брелок.
4. Подходит ближе к машине, давит на кнопку секунд 30.
5. Далее все предсказуемо: владелец авто начинает бегать вокруг машины и «светить» брелоком в замочные скважины (!) то левой, то правой двери. Возможно, он и знает, что такое антенна, но с автосигнализацией это понятия не связывает. Интуиция подсказывает: чтобы открыть замок, надо «светить» в замочную скважину. Логично.

6. Затем, что также логично, немыслимое количество раз нажимает все кнопки брелока, какие только есть.

7. Все это время кодграббер работает в режиме накопления и, собственно, собирает посылки брелока. В результате получится что-то вроде приведенной последовательности, состоящей из десятков посылок:

1-1-1-1-1-1-2-1-2-2-1-1-1-1-3-4-1-1-3-3-1-1-1-1-2-2-2-1-2-1-2-1-2-3-3-4-4-1...,  
где 1 – кнопка открытия; 2 – кнопка закрытия; 3,4 – дополнительные кнопки.

Затем происходит развинчивание брелока, рассматривание и зачистка контактов и батарейки. Это как раз и есть очень удобный момент для автоугонщика. Он сначала отключает кодграббер на несколько секунд, затем переводит устройство из режима накопления в режим выдачи.

Система охраны автомобиля, словно по волшебству, начинает работать как часы, автовладелец с чувством глубокого уважения к себе за ремонт брелока, удовлетворенный этим, отправляется наверстывать отставание от графика...

Злоумышленник едет следом за «жертвой». На ближайшей же парковке владелец машины, отправляясь по делам, снова нажимает кнопку брелока с целью поставить авто на сигнализацию. В это время кодграббер работает в режиме выдачи и с задержкой всего 30 миллисекунд на посылку «закрыть» выдает свою накопленную ранее посылку «закрыть». Когда хозяин машины удаляется на безопасное расстояние, преступник кодграббером открывает авто с помощью опять-таки ранее накопленной посылки «открыть» и беспрепятственно уезжает.

Однозначно защищены от кодграббера с ретрансляцией устройства, которые не имеют пассивного принципа работы радиоключа (метки брелока). Таким образом, радиосигнал посылается владельцем охранной системы только в нужное время и в нужном для него месте. Как правило, это происходит только с системами автосигнализаций, обладающими брелоком с кнопками управления постановкой/снятием с охраны.

Следует заметить, что взлому кодграббером с ретрансляцией подвергаются сигнализации с диалоговым кодом, работающие в режиме «свободные руки на снятие с охраны». Что же касается иммобилайзеров, то при выборе одного нужно обратить внимание на то, чтобы система с диалоговой кодировкой не работала в режиме «фона», то есть сигнал имел посылку только в нужный момент времени!

**Алгоритмический кодграббер** с мануфактурными кодами дешифрования (отсюда второе название – мануфактурный кодграббер) в виде брелока сигнализации – наиболее распространенное сегодня оружие угонщика. Причиной тому служит его универсальность – устройство вскрывает большинство современных автосигнализаций, которые работают в FM-или AM-диапазоне (то есть для которых применяется частотная модуляция в радиоканале). Собственно, сегодня они практически все так и работают.

Принцип работы кодграббера заключается в следующем. Зашифрованный цифровой сигнал охранной системы модулируется с помощью амплитудной или частотной модуляции. На выходе получается аналоговый сигнал, который передается на определенную несущую частоту, там демодулируется (преобразуется опять в цифровой), в результате чего снова получается зашифрованный цифровой сигнал.



## **Конец ознакомительного фрагмента.**

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.