Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 629.067

ШИФРОВАНИЕ В АВТОМОБИЛЬНЫХ СИСТЕМАХ: УЯЗВИМОСТИ, ЭВОЛЮЦИЯ И СОВРЕМЕННЫЕ РЕШЕНИЯ[1]

Огородников Святослав Александрович,
специалитет, Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва, ogorodnikovslava023@gmail.com

Пестрецова Анастасия Александровна,
специалитет, Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва, nastyapestretsova1313@gmail.com

Аннотация

В статье рассматриваются эволюция и современные принципы построения алгоритмов шифрования, применяемых в автомобильных охранных системах. Описаны конструктивные элементы сигнализации, методы обмена данными между брелоком и блоком управления, а также типичные угрозы безопасности, включая перехват и воспроизведение команд с использованием кодграбберов. Анализируются основные этапы развития технологий: статическое, динамическое и диалоговое кодирование, их криптостойкость, преимущества и уязвимости. Рассмотрены современные тенденции развития защиты автомобильных охранных комплексов.

Ключевые слова: автомобильная сигнализация, шифрование, статическое кодирование, динамическое кодирование, диалоговое кодирование, KeeLoq, PKES, кодграббер, криптоанализ, защита автомобиля.

ENCRYPTION IN AUTOMOTIVE SYSTEMS: VULNERABILITIES, EVOLUTION, AND MODERN SOLUTIONS

Ogorodnikov Svyatoslav Alexandrovich,
Specialist, Bauman Moscow State Technical University (National Research University), Moscow, ogorodnikovslava023@gmail.com

Pestretsova Anastasiya Alexandrovna,

[1] Научный руководитель: Деменев Дмитрий Андреевич – Заместитель декана факультета «Информатика и системы управления» МГТУ им. Н. Э. Баумана, заместитель декана факультета «Ракетно-космическая техника» МГТУ им. Н. Э. Баумана, старший преподаватель кафедр ФН-7 (Электротехника и промышленная электроника), ИУ-1 (Системы автоматического управления), Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва.
ORCid: 0009-0004-8500-7531, SPIN-код автора: 4626-7826
Scientific supervisor: Demenev Dmitriy Andreevich – Deputy Dean of the Faculty of Computer Science and Control Systems at Bauman Moscow State Technical University, Deputy Dean of the Faculty of Rocket and Space Technologies at Bauman Moscow State Technical University, Senior Lecturer at Departments FN-7 (Electrical Engineering and Industrial Electronics), IU-1 (Automatic Control Systems management), Bauman Moscow State Technical University (National Research University), Moscow, demenev@bmstu.ru.
ORCid: 0009-0004-8500-7531, SPIN-код автора: 4626-7826

Specialist, Bauman Moscow State Technical University (National Research University), Moscow, nastyapestretsova1313@gmail.com

ABSTRACT

The article examines the evolution and modern principles of constructing encryption algorithms used in automotive security systems. It describes the structural elements of car alarm systems, methods of data exchange between the remote control and the control unit, as well as common security threats, including interception and replay of commands using code grabbers. The main stages in the development of these technologies—static, dynamic, and dialog encoding—are analyzed in terms of their cryptographic strength, advantages, and vulnerabilities. Current trends in the development of protection methods for automotive security complexes are also discussed.

Keywords: car alarm system, encryption, static encoding, dynamic encoding, dialog encoding, KeeLoq, PKES, code grabber, cryptanalysis, vehicle protection.

Алгоритм шифрования, применяемый в автомобильных охранных системах, представляет собой формализованный набор правил и процедур, регулирующих обмен данными между пультом дистанционного управления (брелоком) и центральным блоком управления сигнализацией. Основная задача данного алгоритма — обеспечить надежную защиту информационного канала, по которому передаются управляющие команды и служебные сообщения, чтобы минимизировать вероятность несанкционированного доступа к автомобилю. Иными словами, даже в ситуации, когда злоумышленник способен перехватывать радиопередачу, он не должен получить возможность воспроизвести корректные команды и обойти систему защиты.

Ключевой функцией автомобильной сигнализации является обеспечение многоуровневого оповещения владельца транспортного средства о любых попытках вмешательства в его состояние или целостность. Система фиксирует такие события, как несанкционированное открытие дверей, капота или багажного отделения, удары по кузову, попытки поднятия или перемещения автомобиля, а также действия, связанные с подготовкой к угону. Большинство современных охранных комплексов обладают расширенным функционалом, повышающим удобство эксплуатации автомобиля: дистанционный запуск двигателя, управление бортовым электрооборудованием, поиск автомобиля на парковке, контроль его состояния в режиме реального времени.

История развития автомобильных сигнализаций — это, по сути, история технологического противостояния производителей охранных систем и злоумышленников. С момента появления первых систем защиты автомобилистов разработчики постоянно совершенствовали методы кодирования сигналов, однако параллельно развивались и способы их взлома, что вынуждало индустрию переходить на более сложные алгоритмы шифрования и многоуровневые протоколы обмена данными.

В общем случае автомобильная сигнализация состоит из трех основных конструктивных частей:

1.) Входные устройства — главным образом брелок дистанционного управления, который в штатных системах часто интегрирован с механическим ключом зажигания. С его помощью осуществляется постановка автомобиля на охрану, снятие с охраны, а также контроль и диагностика состояния охранной системы.

2.) Блок управления — центральный вычислительный узел системы, скрытно установленный внутри автомобиля. Он соединяется с сетью датчиков, регистрирующих различные параметры и события (датчики удара, перемещения, положения, давления и др.), и принимает решения о подаче сигналов тревоги или выполнении управляющих команд.

3.) Исполнительные устройства — сирены, замки, модули управления освещением, приводящие в действие физические механизмы и оповещающие владельца о срабатывании сигнализации.

Обмен информацией между брелоком и блоком управления осуществляется по радиоканалу, который является открытым и может быть перехвачен сторонними лицами. Радиосигнал распространяется в эфире во всех направлениях, что делает его уязвимым для прослушивания и анализа. Чтобы снизить риск несанкционированного воспроизведения передаваемых команд, применяются алгоритмы шифрования, преобразующие исходные данные в закодированные пакеты. Каждый пакет представляет собой небольшую структуру данных, содержащую команду (например, «Открыть замки»), подтверждение выполнения команды («Замки открыты») или информационное сообщение («Включено зажигание»).

Несмотря на то, что при передаче информации применяются обратимые криптографические преобразования с использованием ключей шифрования, в отечественной литературе до сих пор распространены некорректные с точки зрения криптографии термины — «статическое кодирование», «динамическое кодирование» и «диалоговое кодирование». Фактически же речь идет о трех различных схемах шифрования данных, которые и будут рассмотрены далее в рамках исследования.

Статическое кодирование

Первые поколения автомобильных охранных систем использовали предельно простую схему передачи данных, известную как статическое кодирование. Принцип её работы заключался в том, что каждой команде, посылаемой с брелока, соответствовал фиксированный набор двоичных данных — командный пакет, который никогда не менялся. Именно неизменность передаваемого сигнала и дала название данному методу. Для иллюстрации: команда «Открыть двери» могла всегда передаваться в одном и том же формате. Эти пакеты задавались пользователем или производителем сигнализации на этапе настройки, чаще всего с помощью механических переключателей (DIP-переключателей) или запаянных перемычек в корпусе брелока.

Главный недостаток подобного подхода заключался в малом количестве возможных комбинаций кодов. Из-за этого в реальных условиях нередко происходили ситуации, когда один и тот же брелок случайно открывал автомобиль соседа, если в их системах сигнализации совпадали форматы пакетов. Помимо этого, такой способ передачи данных практически не обеспечивал защиты от перехвата: достаточно было однажды записать радиосигнал, соответствующий команде «Снять с охраны», а затем воспроизвести его — и автомобиль снимался с блокировки так же, как если бы команду отправил оригинальный брелок.

Именно эта уязвимость стала причиной появления специальных электронных устройств, получивших название кодграбберы. Кодграббер — это компактное техническое средство, способное перехватывать радиосигнал, расшифровывать его структуру и воспроизводить его повторно, эмулируя работу оригинального брелока без участия владельца автомобиля.

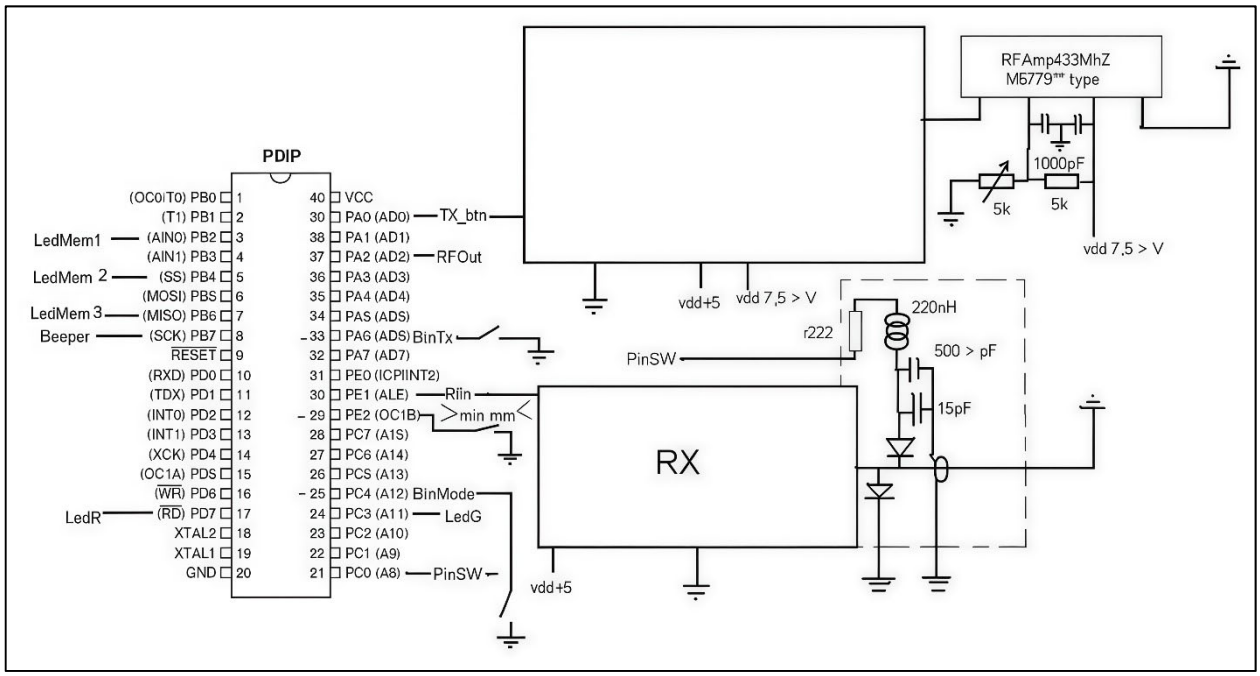

Рис. 1 – Типовая электрическая схема кодграббера сигнализации [10]

С инженерной точки зрения кодграббер почти полностью повторяет конструкцию штатного пульта сигнализации. Он содержит радиоприёмник и радиопередатчик, управляющий микроконтроллер, набор кнопок и световые индикаторы. Для удобства и маскировки угонщики часто используют корпус настоящего брелока — это упрощает изготовление устройства, ведь готовый корпус уже оснащён антенной, кнопками и светодиодами.

Рис. 2 - Кодграббер pandora d605 [9]

В результате внешне кодграббер практически неотличим от оригинального брелока, что делает его использование особенно опасным: владелец автомобиля не может визуально определить факт наличия рядом потенциального злоумышленника.

Существует несколько способов взлома кодграббером. Первый метод особенно эффективен против сигнализаций, в которых постановка и снятие автомобиля с охраны осуществляются нажатием одной и той же кнопки. Суть атаки заключается в создании направленной радиопомехи в момент, когда автовладелец нажимает кнопку на брелоке. Из-за помехи управляющий сигнал не достигает блока управления сигнализацией, однако он фиксируется и сохраняется кодграббером. Как правило, водитель, заметив, что автомобиль не подал характерного сигнала постановки на охрану, нажимает кнопку повторно. В этот момент злоумышленник снова создаёт помеху и перехватывает второй пакет данных. После второго нажатия сигнал всё же достигает блока управления, и автомобиль ставится на охрану, однако один из ранее перехваченных пакетов остаётся в памяти кодграббера. Когда владелец покидает автомобиль, злоумышленник воспроизводит этот пакет и тем самым снимает машину с охраны, получая доступ к салону. [2]

Научно-техническое решение этой проблемы заключается во внедрении алгоритмов формирования сообщений с привязкой ко времени их создания и строго ограниченным временем жизни — аналогично принципу одноразовых паролей TOTP. Это обеспечивает быстрое «устаревание» пакета данных, что делает его бесполезным для злоумышленника уже через доли секунды после передачи. Однако в случае компрометации криптографического алгоритма или заводских секретных ключей остаётся вероятность полного клонирования брелока.

Второй подход злоумышленников — так называемый аналитический взлом. Он основан на использовании уязвимостей, оставленных производителями на уровне архитектуры алгоритмов. Например, в ряде штатных систем для всех автомобилей одной серии могут применяться одинаковые секретные ключи. [3] Это позволяет злоумышленникам создавать так называемые алгоритмические кодграбберы. Принцип работы такого устройства заключается в идентификации марки и модели сигнализации по цифровой посылке, сравнения полученных данных с базой заводских «секретных» кодов и дальнейшей генерации корректных команд, которые воспринимаются блоком управления как команды от оригинального брелока. Источником подобных баз данных становятся как утечки информации от производителей, так и технические просчёты, такие как применение одинаковых ключей для всей серии устройств.

Динамическое кодирование

Для противодействия угрозе радиоперехвата и воспроизведения статических пакетов был разработан метод динамического кодирования, также называемый «плавающим кодом» (rolling code). Суть данного подхода заключается в том, что каждый передаваемый пакет является уникальным и больше не повторяется. С каждой новой командой брелок генерирует пакет, включающий серийный номер устройства, секретный ключ (записанный в брелок и блок управления на заводе-изготовителе) и счётчик нажатий, обеспечивающий синхронизацию между брелоком и приёмником. Передача пакета сопровождается криптографическим преобразованием, благодаря чему анализ его содержимого без знания ключа становится практически невозможным.

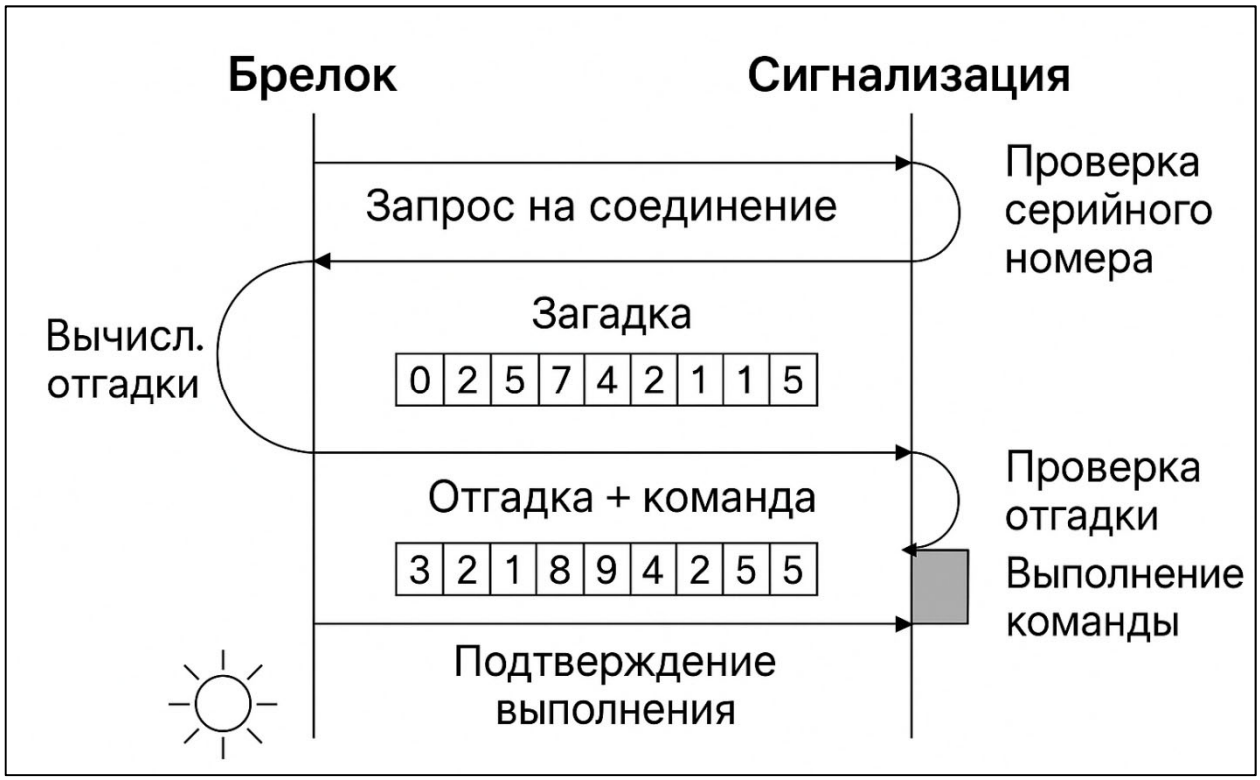

Рис. 3 – Принцип работы динамического кодирования [4]

Наиболее известным примером реализации динамического кодирования является алгоритм KeeLoq, разработанный компанией Microchip Technology. KeeLoq представляет собой симметричный блочный шифр, использующий 32-битный блок данных и 64-битный ключ. Ключевая особенность алгоритма — применение нелинейного регистра сдвига с обратной связью (NLFSR), что обеспечивает высокую стойкость к линейному криптоанализу. На сегодняшний день сам алгоритм KeeLoq остаётся криптографически стойким: его теоретический взлом не реализован. Однако на практике уязвимости возникают из-за неудачных реализаций. Так, некоторые производители используют один и тот же ключ для целых серий устройств, что делает возможным клонирование брелоков и изготовление «мануфактурных» кодграбберов.

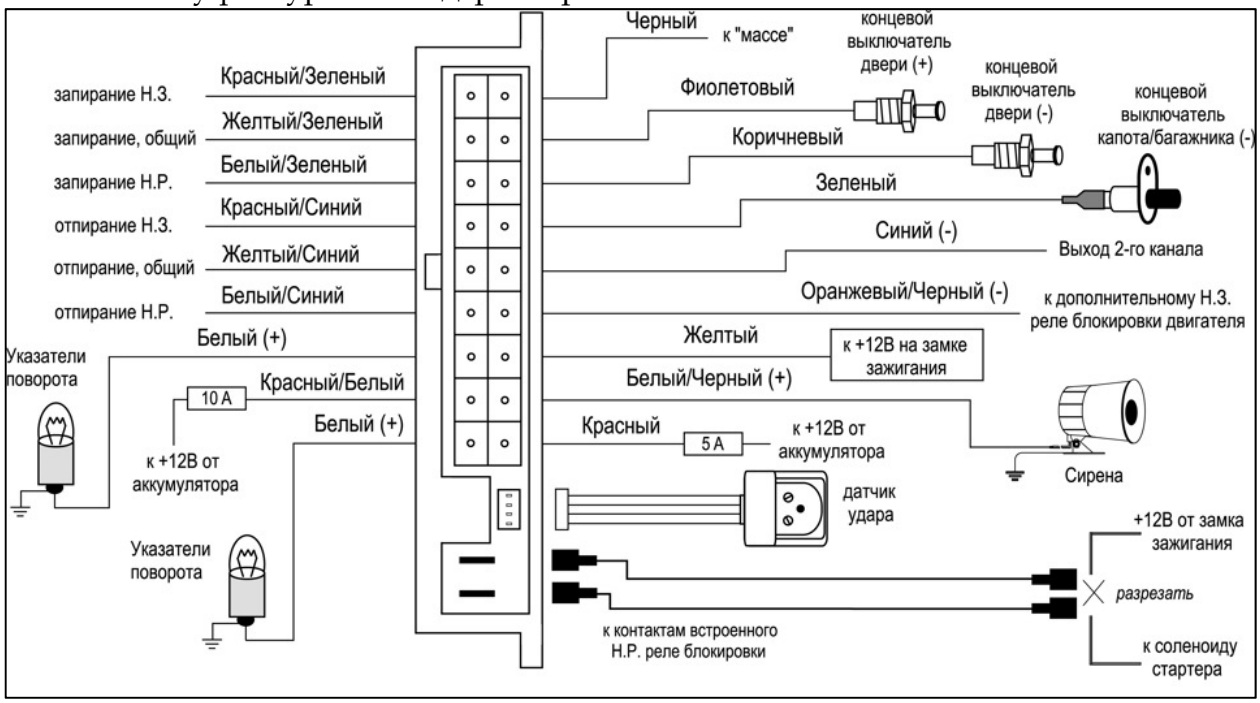

Рис. 4 - Система A.P.S. 7200. Монтажная схема [1]

Несмотря на то, что динамическое кодирование стало серьёзным шагом вперёд по сравнению со статическим, оно также не гарантирует абсолютной защиты автомобиля. С течением времени данный метод устарел, и на смену ему пришли более совершенные решения, основанные на принципе диалогового кодирования, при котором брелок и блок управления обмениваются не только командами, но и криптографическими вызовами-ответами, что существенно повышает уровень защиты.

Диалоговое кодирование

Современные охранные комплексы премиум-класса используют диалоговое кодирование, которое на сегодняшний день считается наиболее надежным и криптостойким методом защиты от несанкционированного доступа. Главная особенность этого подхода заключается в необходимости двустороннего обмена данными между брелоком и центральным блоком управления сигнализацией. Оба устройства — и брелок, и блок — оснащены как передатчиком, так и приемником радиосигнала, что позволяет организовать полноценный протокол взаимной аутентификации.

Принцип работы диалогового кода аналогичен криптографическим протоколам с динамическим обменом ключами, например протоколу Диффи — Хеллмана. Последовательность действий при постановке или снятии автомобиля с охраны включает несколько этапов. Когда владелец нажимает кнопку на брелоке, на блок управления отправляется запрос на выполнение команды. В ответ блок генерирует случайное число (или случайную последовательность бит) и пересылает его обратно на брелок. Брелок, используя свой секретный ключ, производит криптографическую обработку полученного числа и возвращает результат на блок управления. Параллельно центральный блок самостоятельно выполняет аналогичные вычисления и сравнивает результат с ответом брелока. Только при полном совпадении данных команда считается подлинной и исполняется.

Стоит отметить, что конкретные алгоритмы обработки случайных чисел и схема обмена сообщениями являются собственностью производителей и закладываются в систему на стадии проектирования. Эти алгоритмы, как правило, составляют коммерческую тайну и не раскрываются в открытых источниках, что дополнительно повышает их устойчивость к атакам.

Диалоговое кодирование обеспечивает крайне высокий уровень защиты. Даже для простейшего уравнения с несколькими неизвестными требуется многократный перехват данных для решения системы уравнений, однако в диалоговых системах каждое сообщение уникально и не может быть использовано повторно. Перехват и аналитическая расшифровка пакетов в таких системах практически невозможны, поскольку каждый брелок содержит индивидуальный криптографический ключ, записанный однократно при его регистрации в системе. Современные сигнализации используют ключи длиной не менее 128 бит, а в последних поколениях — 256 бит. Объем возможных комбинаций при такой длине ключа настолько велик, что полный перебор вариантов займет огромное количество времени. Дополнительную защиту обеспечивает аппаратный генератор случайных чисел, встроенный в блок управления и защищенный от аппаратных атак. Более того, процесс передачи пакетов сопровождается специально введенными паузами и вариациями частоты передачи, что усложняет анализ и синхронизацию для потенциального злоумышленника.

В результате на сегодняшний день диалоговые автосигнализации остаются почти неуязвимыми для кодграбберов и других методов перехвата. Некоторые ведущие производители даже объявляют открытые конкурсы на поиск уязвимостей своих систем, предлагая значительные денежные вознаграждения. Однако до настоящего времени публично подтверждённых успешных взломов диалогового кода не зарегистрировано.

Системы бесключевого доступа (PKES)

В последние годы получила широкое распространение технология Passive Keyless Entry and Start (PKES) — «пассивный бесключевой доступ и запуск двигателя». [2]

Рис. 5 - Система бесключевого доступа Toyota [7]

Такие системы выводят удобство эксплуатации автомобиля на новый уровень, поскольку больше не требуют от владельца нажатия кнопок на брелоке: достаточно приблизиться к автомобилю, чтобы двери автоматически разблокировались, а при удалении — чтобы они заблокировались, и сигнализация снова встала на охрану. Кроме того, PKES позволяет запускать двигатель с помощью кнопки, исключая необходимость использования механического ключа зажигания. Принцип работы PKES также основан на диалоговом обмене данными, но с применением дополнительных механизмов радиочастотной идентификации. Когда владелец приближается к автомобилю и касается сенсорной зоны на дверной ручке, автомобиль активируется и инициирует сеанс связи с ключом. На частоте 125 кГц в эфир отправляется запрос следующего содержания:

«Привет, я автомобиль X с идентификатором Z. А ты кто?»

Если смарт-ключ находится в зоне действия антенн, он мгновенно отвечает автомобилю, используя уже другую рабочую частоту (чаще всего 433 или 868 МГц), и передает криптографически сформированный ответ:

«Привет, я твой ключ! Код ответа: X123.Y456.Z789.»

Этот обмен происходит за доли секунды, а ключ авторизуется только при корректной обработке запроса, что обеспечивает высокую степень безопасности. Чтобы исключить электронные подтасовки (воспроизведение заранее записанных посылок, передачу кода по каналам сотовой связи или мобильного интернета), ответ от электронного ключа должен поступить в режиме реального времени (счет задержкам ведется на наносекунды), так что любые попытки открыть машину обречены на провал. Но даже такие хитроумные действия не всегда спасают от угона.

О криминальной уязвимости PKES-систем заговорили в 2011 году, когда команда швейцарских программистов продемонстрировала метод «удлинения» канала связи «автомобиль-ключ». Технологию назвали Relay Station Attack. К тому времени российские угонщики уже вовсю пользовались такими устройствами. Злоумышленнику потребуется специальный ретранслятор (его еще называют "удочкой"/"длинной рукой"), который стоит десятки тысяч евро, и помощник, который должен находиться рядом со смарт-ключом, то есть рядом с Владельцем. Когда угонщик нажимает кнопку открытия машины, сигнал по

ретранслятору передается на устройство помощника, который уже общается с брелоком сигнализации. С помощью таких действий можно угнать любой автомобиль.

Приведем пример угона. Вы припарковали свой автомобиль около торгового центра, закрыли двери и пошли по делам, двери автоматически при этом заблокировались. К Вашему автомобилю подходит Злоумышленник №1 с приемником, а около Вас находится Злоумышленник №2 с ретранслятором сигнала Вашего ключа. Автомобиль в этот момент идентифицирует, что Вы якобы находитесь рядом и открывается. Злоумышленник №1 садится в автомобиль и уезжает (рис.6).

Рис. 6. Угон авто с помощью ретранслятора

Как бороться с данной уязвимостью? Существует прошивки, которые изменят код управления сигнализацией на другой, а значит радиоканал будет вне досягаемости ретрансляторов. Также есть проверенный на практике способ — прятать брелок сигнализации в металлизированный экран из фольги — простой, но действенный способ, позволяющий физически заблокировать диалог между брелоком и БУ, как только вы отошли от автомобиля и спрятали брелок.

Современные тенденции развития защиты автомобильных охранных комплексов

1. Переход к принципу «Безопасность с момента проектирования»

Раньше системы безопасности в автомобиле часто создавались «вдогонку»: сначала разрабатывали электронику и программы, а потом добавляли защиту, когда находили уязвимости. Сегодня подход меняется — безопасность закладывается с самого начала разработки машины. Это значит, что каждая электронная система (двигатель, тормоза, охранный блок, мультимедиа) разрабатывается с учётом потенциальных угроз. Производители создают архитектуры доверия — специальные микросхемы и алгоритмы, которые проверяют, что программное обеспечение не подделано. Помимо этого, используются технологии Secure Boot — загрузка начинается только если прошивка подписана цифровым ключом. Обновления (через интернет, OTA) проходят криптографическую проверку: если кто-то попытается подменить файл, система не установит его.

2. Искусственный интеллект и машинное обучение в охране автомобиля

Автомобиль становится всё более «умным», и защита тоже. Современные охранные комплексы могут использовать искусственный интеллект (AI) и машинное обучение (ML) для анализа поведения автомобиля и его систем. Например, система анализирует обмен данными между блоками (по шинам CAN, LIN, Ethernet). Если появляется необычный сигнал (например, команда «открыть двери», когда ключ далеко), ИИ фиксирует это как аномалию. Модели машинного обучения могут распознавать привычки владельца —

например, типичные маршруты, манеру вождения, время поездок. Если стиль резко меняется — система может заподозрить, что за рулём не хозяин. В облачных сервисах ИИ объединяет данные тысяч автомобилей, чтобы предсказывать и блокировать новые типы атак. Вся сложность заключается в том, что модели должны быть устойчивы к «обману» — злоумышленники могут специально генерировать ложные сигналы, чтобы сбить ИИ с толку. Поэтому важно обучать системы на надёжных данных и постоянно обновлять их.

3. Биометрия и многофакторная аутентификация

Классические брелоки и «keyless»-ключи можно перехватить и скопировать. Поэтому производители всё чаще вводят многофакторную аутентификацию — когда для доступа требуется не один, а сразу несколько признаков: отпечаток пальца на ручке двери, распознавание лица водителя камерой, голосовая идентификация. Все чаще и чаще появляется поведенческая биометрия — автомобиль узнаёт «почерк» вождения (ускорения, повороты, торможения). Если данные не совпадают, доступ блокируется или требует дополнительного подтверждения (например, PIN-кода). Плюсы очевидны - защита становится персонализированной. Но стоит быть аккуратным, т.к. нужно соблюдать законы о персональных данных и хранить биометрию в зашифрованном виде, чтобы не допустить утечек.

4. Борьба с атаками на системы «бесключевого доступа» (keyless)

Одни из самых частых взломов — так называемые ретрансляционные атаки («relay attack»): преступники с помощью двух устройств перехватывают сигнал ключа у владельца и передают его к машине, открывая и заводя двигатель, даже если хозяин дома. Современные методы защиты:

Использование временной метки: ключ и автомобиль сверяют не только код, но и задержку сигнала. Если сигнал слишком «долгий», система понимает, что это подмена.

Блокировка сигнала ключа при бездействии — ключ «засыпает» через несколько секунд, если его не двигают.

Защищённые радиопротоколы с динамическими кодами и шифрованием.

Физические меры — «мешки Фарадея» для ключей, чтобы глушить радиосигнал.

Также растёт популярность дополнительных иммобилайзеров, которые требуют второе подтверждение (например, через мобильное приложение или PIN на панели).

5. Защита электромобилей и зарядной инфраструктуры

Электромобили подключаются к зарядным станциям, которые передают и принимают данные — о владельце, состоянии батареи, оплате. Если злоумышленник вмешается в этот процесс, он может: бесплатно заряжать свою машину за счёт другого, получить доступ к аккаунту владельца и даже повредить оборудование, послав неправильные команды. Борются с этим путем шифрования данных между автомобилем и станцией и двусторонней аутентификацией (и машина, и станция подтверждают личность друг друга).

6. Аппаратные модули безопасности (HSM, TPM, Secure Element)

Чтобы защитить важные криптографические ключи и пароли, используются специальные микросхемы — аппаратные модули безопасности. Они действуют как «железный сейф» внутри автомобиля: ключи не хранятся в открытом виде в памяти, а операции шифрования выполняются внутри самого чипа. Даже если взломщик получит доступ к ЭБУ, вытащить ключи он не сможет. На данный момент существует уже несколько видов модулей:

TPM (Trusted Platform Module) — часто используется в бортовых компьютерах;

HSM (Hardware Security Module) — более мощные устройства для защиты коммуникаций;

Secure Element (SE) — мини-чипы для безопасного хранения данных, как в банковских картах.

7. Стандартизация и регулирование в области автомобильной кибербезопасности

Многие страны уже ввели обязательные требования по кибербезопасности для автопроизводителей. Примеры — стандарты ISO/SAE 21434, UNECE WP.29, которые определяют: как нужно разрабатывать безопасные системы, как выявлять и устранять уязвимости, как проводить обновления и реагировать на инциденты. Все это означает, что каждый производитель должен теперь иметь команду по безопасности, проводить тесты и аудит, документировать все меры защиты. Это повышает общий уровень защиты и заставляет компании думать о безопасности заранее.

8. Безопасность цепочки поставок и обновлений

Современный автомобиль — это сотни электронных блоков, поставленных десятками компаний. Если хотя бы один поставщик предоставит уязвимую прошивку, безопасность всей машины окажется под угрозой, поэтому развивается учёт происхождения всех программных компонентов (так называемый SBOM — Software Bill of Materials), цифровая подпись прошивок и их проверка при установке, а также контроль обновлений по защищённым каналам OTA. Это помогает защититься от поддельных или вредоносных обновлений.

9. Мониторинг, реагирование и обмен информацией об угрозах

Всё чаще автомобили подключены к облаку, а производители создают центры мониторинга безопасности (SOC). Они в реальном времени отслеживают попытки взлома, подмену данных, необычные маршруты и команды. Если что-то подозрительное происходит, система может автоматически заблокировать удалённый доступ и предупредить владельца, отправив отчёт инженерам. Также формируются отраслевые сообщества обмена данными о кибератаках, чтобы быстро реагировать на новые угрозы и предотвращать их массовое распространение.

Вывод

Проведённый анализ подтверждает, что эволюция автомобильных охранных систем представляет собой последовательный переход от простых схем статического кодирования к высокозащищённым диалоговым протоколам с криптографической аутентификацией и индивидуальными ключами. Развитие автомобильной безопасности идёт в сторону интеллектуальных, сетевых и самозащищённых систем. Если раньше охранный комплекс был просто сигнализацией с сиреной, то теперь это — сложная киберсистема, способная анализировать угрозы в реальном времени, защищать программное обеспечение, обеспечивать безопасный обмен данными и автоматически восстанавливаться после попыток взлома. Будущее автомобильных охранных комплексов — это сочетание кибербезопасности, искусственного интеллекта, криптографии и биометрии в едином, самоуправляемом защитном контуре.

Список литературы:

1. Алгоритмический кодграббер и диалоговый код [Электронный ресурс]. – 2025. – URL: https://www.drive2.ru/l/8375339/ (дата обращения: 22.10.2025). – Текст: электронный.
2. Алгоритмы шифрования в автосигнализациях [Электронный ресурс]. – 2025. – URL: https://ru.wikipedia.org/wiki/Алгоритмы_шифрования_в_автосигнализациях (дата обращения: 22.10.2025). – Текст: электронный.

3. Алгоритмы шифрования сигнализации [Электронный ресурс]. – 2025. – URL: https://www.mazbook.ru/article/alarm/explore/algoritmy-shifrovaniya-avtomobilnoy-signalizacii (дата обращения: 22.10.2025). – Текст: электронный.
4. Автомобильная сигнализация: советы по выбору [Электронный ресурс]. – 2025. – URL: https://autolocked.ru/avtosignalizacii/avtomobilnaya-sovety-po-vyboru (дата обращения: 22.10.2025). – Текст: электронный.
5. Безопасность системы автомобильной сигнализации [Электронный ресурс]. – 2025. – URL: https://xakep.ru/2016/05/16/bladerf-attack (дата обращения: 22.10.2025). – Текст: электронный.
6. Диалоговые принципы в защите радиоканала автосигнализаций и иммобилайзеров [Электронный ресурс]. – 2025. – URL: https://alarmtrade-ural.ru/dialogovyie-printsipyi-v-zashhite-radiokanala-avtosignalizatsij-i-immobilajzerov/ (дата обращения: 22.10.2025). – Текст: электронный.
7. EASYGUARD EC003N-V 1: antirrobo seguridad arranque [Электронный ресурс]. – 2025. – URL: https://www.amazon.com/-/es/EASYGUARD-EC003N-V-1-antirrobo-seguridad-arranque/dp/B07RJHP4Q7 (дата обращения: 22.10.2025). – Текст: электронный.
8. Кауфман К., Перлман Р., Спекнер М. Сетевая безопасность: частная связь в публичном мире. – 2-е изд. – Прентис Холл, 2002. – 712 с.
9. Кодграбберы Pandora D605 v2.4 full [Электронный ресурс]. – 2025. – URL: https://spb.barahla.net/kuplyu-prodam/zapchasti-aksessuary/26175942_prodam-kodgrabbery-pandora-d605-v-2-4-full.html (дата обращения: 22.10.2025). – Текст: электронный.
10. Компанец Д. Радиолюбители — Грабители [Электронный ресурс]. – 2025. – URL: https://dzen.ru/a/ZDzQIwAyoF1aBVS1 (дата обращения: 22.10.2025). – Текст: электронный.
11. Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S. и др. Experimental Security Analysis of a Modern Automobile [Электронный ресурс]. – 2010. – URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Koscher.pdf (дата обращения: 22.10.2025). – Текст: электронный.
12. Checkoway S., McCoy D., Kantor B., Koscher K., Anderson D., Shacham H., Savage S. и др. Comprehensive Experimental Analyses of Automotive Attack Surfaces [Электронный ресурс]. – 2011. – URL: https://www.usenix.org/conference/usenixsecurity11 (дата обращения: 22.10.2025). – Текст: электронный.
13. Смит К. The Car Hacker's Handbook: A Guide for the Penetration Tester. – No Starch Press, 2016. – 304 с.
14. Электронные реле автомобильных охранных сигнализаций, управляемые по силовой электропроводке автомобиля / Васюков С. А., Мурзин И. А. [Электронный ресурс]. – 2018. – URL: http://www.pribory-smi.ru/ (дата обращения: 22.10.2025). – Текст: электронный.

References:

1. Algorithmic Code Grabber and Dialog Code [Electronic resource]. (2025). Available at: https://www.drive2.ru/l/8375339/ (accessed 22 Oct 2025).
2. Available at: https://ru.wikipedia.org/wiki/Алгоритмы_шифрования_в_автосигнализациях (accessed 22 Oct 2025).
3. Car Alarm Encryption Algorithms [Electronic resource]. (2025). Available at: https://www.mazbook.ru/article/alarm/explore/algoritmy-shifrovaniya-avtomobilnoy-signalizacii (accessed 22 Oct 2025).
4. Car Alarm Systems: Tips for Choosing [Electronic resource]. (2025). Available at: https://autolocked.ru/avtosignalizacii/avtomobilnaya-sovety-po-vyboru (accessed 22 Oct 2025).
5. Security of Car Alarm Systems [Electronic resource]. (2025). Available at: https://xakep.ru/2016/05/16/bladerf-attack (accessed 22 Oct 2025).
6. Dialog Principles in Car Alarm Radio Channel Protection [Electronic resource]. (2025). Available at: https://alarmtrade-ural.ru/dialogovyie-printsipyi-v-zashhite-radiokanala-avtosignalizatsij-i-immobilajzerov/ (https://alarmtrade-ural.ru/dialogovyie-printsipyi-v-zashhite-radiokanala-avtosignalizatsij-i-immobilajzerov/?ysclid=mhxh66ievf459525712) (accessed 22 Oct 2025).
7. EASYGUARD EC003N-V 1: Antirrobo Seguridad Arranque [Electronic resource]. (2025). Available at: https://www.amazon.com/-/es/EASYGUARD-EC003N-V-1-antirrobo-seguridad-arranque/dp/B07RJHP4Q7 (accessed 22 Oct 2025).
8. Kaufman C., Perlman R., Speciner M. (2002). Network Security: Private Communication in a Public World. 2nd ed. Prentice Hall, 712 p.
9. Pandora D605 v2.4 Full Code Grabbers [Electronic resource]. (2025). Available at: https://spb.barahla.net/kuplyu-prodam/zapchasti-aksessuary/26175942_prodam-kodgrabbery-pandora-d605-v-2-4-full.html (accessed 22 Oct 2025).
10. Kompanets D. Radio Amateurs — Burglars [Electronic resource]. (2025). Available at: https://dzen.ru/a/ZDzQIwAyoF1aBVS1 (accessed 22 Oct 2025).
11. Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S. et al. (2010). Experimental Security Analysis of a Modern Automobile [Electronic resource]. Available at: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Koscher.pdf (accessed 22 Oct 2025).
12. Checkoway S., McCoy D., Kantor B., Koscher K., Anderson D., Shacham H., Savage S. et al. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces [Electronic resource]. Available at: https://www.usenix.org/conference/usenixsecurity11 (accessed 22 Oct 2025).
13. Smith C. (2016). The Car Hacker's Handbook: A Guide for the Penetration Tester. No Starch Press, 304 p.
14. Electronic relays of automotive security alarm systems controlled via the vehicle's power wiring / Vasyukov S. A., Murzin I. A. [Electronic resource]. – 2018. – URL: http://www.pribory-smi.ru/ (accessed: 22.10.2025). – Text: electronic.