УДК 004.056.5

А.П. Жук, А.А. Гавришев, Д.Л. Осипов, В.А. Бурмистров
(Северо-Кавказский федеральный университет; e-mail: alekszhuk@mail.ru)

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ БЕСПРОВОДНЫХ КАНАЛОВ СВЯЗИ АВТОМОБИЛЬНЫХ СИГНАЛИЗАЦИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Анализируются методы защиты радиоканалов автомобильных сигнализаций от несанкционированного доступа (перехват, просмотр, подмена и подавление трафика). Установлено, что предпочтительным методом защиты радиоканалов от комплексных угроз является использование технологий на основе шумоподобных сигналов. Перспективным видится развитие технологии защиты радиоканалов на основе хаотических сигналов.

Ключевые слова: радиоканал, сигнализация, защищенность, шумоподобные сигналы.

A.P. Zhuk, A.A. Gavrishev, D.L. Osipov, V.A. Burmistrov

ANALYSIS OF METHODS OF PROTECTION OF WIRELESS COMMUNICATION CHANNELS OF CAR ALARM SYSTEMS FROM UNAUTHORIZED ACCESS

The analysis of methods of protection of the radio channels of car alarms from unauthorized access (interception, viewing, substitution and jamming) was carried out. It was found that the preferred method for protecting radio channels of car alarms is the use of technologies based on the noise-like signals. Sees promising safety technology development radio channel based on chaotic signals.

Key words: radio channel, alarm, safety, noise-like signals.

Статья поступила в редакцию Интернет-журнала 11 сентября 2016 г.

В последние годы наблюдается бурный рост радиоканальных технических систем охраны, к которым относится и беспроводная автомобильная сигнализация.

Беспроводные автомобильные сигнализации занимают отдельную нишу на рынке радиоканальных технических систем охраны. Рынок автомобильных сигнализаций в настоящее время насыщен, поэтому технологические прорывы по данному направлению возможны только при наличии новых научных исследований, в первую очередь, в области информационной безопасности.

В силу уязвимости беспроводного канала связи технических систем охраны к ***несанкционированному доступу (НСД)*** со стороны третьих лиц [1], чрезвычайно актуальным является разработка методов защиты радиоканала автомобильной сигнализации от НСД. К основным видам НСД к беспроводным системам связи относятся: перехват, просмотр, подмена и радиоэлектронное подавление трафика.

В настоящее время для обеспечения защиты радиоканала технических систем охраны применяются [1]:

- криптографические методы защиты информации;
- шумоподобные сигналы.

В данной статье не рассматриваются автомобильные сигнализации, в которых в качестве радиоканала используются мобильные сети.

Рассмотрим ***криптографические методы защиты (КМЗ)*** радиоканала.

В работе [2] описывается технология динамического кодирования KeeLoq и её развитие – алгоритм D2. В основу алгоритма положен псевдослучайный "прыгающий" код. "Прыгающий" код генерируется на основе 64-битного кода ключа, 28-битного серийного номера и 16-битного счетчика синхронизации. Код ключа задается пользователем с использованием кодера. Серийный номер уникален и задается производителем. Однако, данная технология не защищена от кодграбберов, что делает её уязвимой для несанкционированного доступа. Развитием KeeLoq стала ***технология двойного динамического кода D2***. Она состоит в следующем: у команд управления различные структуры и система управляется несколькими динамическими кодами. Кроме того, при каждом новом нажатии генерируется новый код, что повышает защищённость от просмотра и подмены.

В работе [3] анализируется система Zigbee в качестве защиты радиоканала автомобильной сигнализации от НСД. В основе данного стандарта лежит алгоритм шифрования AES-128. Данная технология обеспечивает защиту от подмены и просмотра трафика. Для экспериментальных исследований был построен стенд на основе радиопередатчиков XBee – стандарта Zigbee компании Digi International вкупе с макетными платами Xbib dev rev.3.0. Один передатчик выполняет функцию координатора сети и является центральным узлом охранного комплекса. Второй передатчик имитирует брелок автосигнализации. Питание беспроводных модулей осуществляется через кабели USB. В макете представлена главная функциональность брелока – постановка и снятие с охраны. Все сообщения передаются с включенной функцией шифрования на уровне стека. При передаче команды от брелока, он получает не только подтверждение о доставке на уровне стека, но и координатор отправляет сообщение об успехе включения/выключения охранных функций после их выполнения. Основным недостатком, отмеченным в ходе исследований, было значительное увеличение времени выполнения операций шифрования-расшифрования.

В работе [4] предлагается альтернативный способ защиты радиоканала автомобильной сигнализации от несанкционированного доступа за счёт использования псевдослучайных последовательностей. Концептуально устройство,

реализующее данный способ защиты, состоит из ***стационарного блока управления (СБУ)***, в состав которого входят ***генератор случайных чисел (ГСЧ)***, ***генератор псевдослучайной последовательности (ПСП)***, ***устройство сравнения (УС)***, ***мобильного брелока управления (МБУ)***, в состав которого входит генератор ПСП. Устройство функционирует следующим образом: при вхождении в режим синхронизации СБУ и МБУ на ГСЧ СБУ поступает команда "старт", по которой он вырабатывает случайное значение. Полученное случайное значение одновременно отправляется на генератор ПСП СБУ и через радиоканал на генератор ПСП МБУ. Затем генератор ПСП СБУ функция генерации последовательности которого идентична функции генератора ПСП МБУ, вырабатывает последовательность, поступающую в УС. Одновременно с этим выработанная в генераторе ПСП МБУ, функция генерации последовательности которого идентична функции генератора ПСП СБУ, последовательность через радиоканал также поступает в УС. Далее в УС происходит сравнение откликов генераторов ПСП СБУ и МБУ. В случае совпадения значений, выдаётся сигнал "норма", служащий для оповещения о санкционированном доступе к автомобильной сигнализации. При несовпадении значений выдаётся сигнал "тревога", служащий для оповещения о несанкционированном доступе к автомобильной сигнализации. На данную технологию авторами получен патент РФ № 2592385 от 20.07.2016.

Несмотря на повсеместное использование в беспроводных автомобильных сигнализациях КМЗ, они обладают общим недостатком, заключающимися в том, что у них отсутствует защита против перехвата и подавления трафика помехами. Особенно это актуально в тех случаях, когда злоумышленники применяют комплексные угрозы (перехват, просмотр, подмена и радиоэлектронное подавление трафика). Также в качестве недостатка можно отметить продолжительное время выполнения операций шифрования-расшифрования.

Рассмотрим использование ***шумоподобных сигналов (ШПС)*** для обеспечения защиты радиоканала автомобильной сигнализации.

Анализ применения технологий на основе ШПС показал, что наиболее распространёнными для защиты радиоканалов автомобильных сигнализаций являются технологии на основе ***фазоманипулированных сигналов (ФМС)***, на основе ***псевдослучайной перестройки рабочей частоты (ППРЧ)***, на основе ***сверхширокополосных сигналов (СШП)***.

Рассмотрим применение технологии на основе ФМС. В работе [5] предлагается система защиты транспортного средства от НСД, характеризующаяся повышенной устойчивостью и достоверностью приема сигналов за счет применения сложных сигналов с фазовой модуляцией. Это достигается за счет повы-

шения отношения сигнал/шум на выходе блока вычитания с помощью двух универсальных демодуляторов. Недостатком данного устройства является излишняя техническая сложность, приводящая к усложнению аппаратуры. В работе [6] предлагается для повышения защищённости информационного обмена использовать автокорреляционную широкополосную систему связи на основе модуляции фазы передаваемого сигнала. Данная система позволяет значительно повысить защищенность от НСД.

Рассмотрим применение технологии на основе ППРЧ. В работе [7] рассмотрена система мониторинга "Риф Стринг-202", которая каждый выход в эфир осуществляет на одной из 1024 заранее запрограммированных частот связи на основе ППРЧ. Также дополнительно в данном устройстве реализовано помехоустойчивое кодирование.

Рассмотрим применение технологии на основе СШПС. В работе [8] рассматривается использование СШПС сигналов на основе хаотических сигналов. Отмечается, что сигналы данного вида обеспечивают защиту от помех, простоту технической реализации и повышенную защищенность от НСД. В работе [9] рассматривается использование радиомодулей на основе СШПС. Отмечается, что такой подход, за счет очень широкой полосы частот, делает трудной задачу обнаружения сигнала, а также его подавление помехами.

Рассмотрим альтернативные методы на основе технологии ШПС.

В работе [10] предлагается обеспечивать защиту радиоканала автомобильной сигнализации за счет анализа длительности принимаемого импульса. Это позволяет обнаруживать искажаемые области сигнала. Данная защита идеальна против кодграбберов, однако бессильна против перехвата и просмотра сигнала, то есть недостатком данного способа защиты является необходимость наличия дополнительной защиты автомобильной сигнализации, направленной на замену уже скомпрометированной, но пока не использовавшейся злоумышленником ключевой информации.

К общим недостатками технологий защиты радиоканалов автомобильных сигнализаций на основе ШПС можно отнести ограниченный ансамбль используемых шумоподобных сигналов, отсутствие возможности периодической смены используемых сигналов и сложность приёмо-передающей аппаратуры. Однако, технологии защиты на основе ШПС обеспечивают одновременную защиту от перехвата, просмотра, подмена и радиоэлектронного подавления трафика.

Таким образом, в данной статье был проведён анализ технологий защиты радиоканалов автомобильных сигнализаций, который подтвердил, что базовыми методами защиты являются КМЗ и технологии на основе ШПС. КМЗ не обеспечивают защиту против перехвата и подавления трафиками помехами. Технологии на основе ШПС, напротив, обеспечивают одновременную защиту

радиоканала от перехвата, просмотра, подмены и радиоэлектронного подавления. Поэтому они являются предпочтительными при использовании в беспроводных автомобильных сигнализациях.

По мнению авторов, дальнейшие исследования, направленные на совершенствование и повышение защищённости радиоканалов автомобильных сигнализаций, следует вести в области технологий на основе ШПС, например, технологии на основе хаотических сигналов.

Литература

1. ***Брауде-Золотарев Ю.*** Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64-66.

2. ***Шелованов Е.Л., Суков С.Ф.*** Защита данных в радиоканале при дистанционном управлении стационарными и движущимися объектами. http://ea.donntu.org:8080/jspui/bitstream/123456789/14083/1/ %D0 %A8 %D0 %B5 %D0 %BB %D0 %BE %D0 %B2 %D0 %B0 %D0 %BD %D0 %BE %D0 %B2 %20 %D0 %95. %D0 %9B., %20 %D0 %A1 %D1 %83 %D0 %BA %D0 %BE %D0 %B2 %20 %D0 %A1. %D0 %A4.pdf.

3. ***Грязин Д.С., Данилова А.А.*** Охранный комплекс автомобиля на базе стандарта Zigbee // Наука вчера, сегодня, завтра: сб. ст. по матер. IX междунар. науч.-практ. конф. № 2(9). Новосибирск: СибАК, 2014. http://sibac.info/13311.

4. ***Гавришев А.А., Бурмистров В.А., Анзин И.В.*** К вопросу об использовании псевдослучайных последовательностей для предотвращения несанкционированного доступа к радиоканалу автомобильной сигнализации // Новые информационные технологии и системы: сб. науч. ст. XI Междунар. науч.-техн. конф. Пенза: изд-во ПГУ, 2014. С. 270-272.

5. ***Система*** защиты от несанкционированного доступа для транспортных средств: патент 2481978 Рос. Федерация: B60R 25/00 / В.А. Калинин, В.А. Шубарев, В.А. Мельников, В.И. Дикарев № 2011142956/11; заявл. 24.10.2011; опубл. 20.05.2013, Бюл. № 14. 14 с.

6. ***Фролов В.Я., Ковтунов Ю.А., Кубата В.Г.*** Методы обеспечения помехоустойчивости при управлении автомобильной противоугонной сигнализацией // Автомобильный транспорт. 2013. Вып. 33. С. 105-109.

7. ***Плотников Г.Г., Картавцев Д.В., Сердюк А.С.*** Современные системы мониторинга для охраны подвижных объектов // Вестник Воронежского института МВД России. 2007. № 2. С. 186-189.

8. ***Мохсени Т.И., Рыжов А.И., Лазарев В.А.*** Эксперименты по применению СШП средств связи в автомобиле // Труды 55-й научной конференции МФТИ. Радиотехника и кибернетика. Том 2. М.: МФТИ, 2012. С. 103.

9. ***Автономное*** устройство сигнализации и пуска: полезная модель 85244 Рос. Федерация: G06F 9/00, G05G 19/00 / М.А. Гайдамак, В.И. Панюшкин № 2009116224/22; заявл. 29.04.2009; опубл. 27.07.2009. 7 с.

10. ***Дубина С.С., Козлов К.С., Сечко Г.В., Чернецкий А.М.*** Обеспечение целостности информации в автосигнализации мобильных объектов // Международная научно-техническая конференция, приуроченная к 50-летию МРТИ-БГУИР: материалы конф. В 2 ч. Ч. 1. Минск: БГУИР, 2014. С. 384-385.