Алексей А. Гавришев, Александр П. Жук
Северо-Кавказский федеральный университет,
ул. Пушкина, 1, г. Ставрополь, 355009, Россия
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

РАЗРАБОТКА БЕСПРОВОДНОЙ ИМИТОЗАЩИЩЕННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИЯ И КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ

DOI: http://dx.doi.org/10.26583/bit.2018.1.04

Аннотация. В данной статье рассматриваются беспроводные системы идентификации и контроля доступа транспортных средств на охраняемые объекты. Рассмотрены известные системы. В результате установлено, что одним из перспективных подходов к идентификации и контролю доступа транспортных средств на охраняемые объекты является использование систем на основе принципа «свой-чужой». Среди данных систем выделяются «однонаправленные» и «двунаправленные» системы идентификации и контроля доступа. «Двунаправленные» системы являются более предпочтительными для вопросов идентификации и контроля доступа. Однако, в настоящее время, данные системы должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов в силу того, что потенциальный злоумышленник может достаточно легко выполнить несанкционированный доступ к радиоканалу системы. На основании этого разработана беспроводная система идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой», отличающаяся повышенной защищенностью от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей. Дополнительно к этому предлагается использовать для идентификации транспортного средства RFID-метку, содержащую дополнительную информацию о нем. Приведены некоторые технические характеристики разработанной системы (возможный частотный диапазон запросно-ответных сигналов, дальность связи, скорость передачи данных, объем передаваемых данных, рекомендации по выбору RFID-меток). Так же, с помощью аппарата нечеткой логики, была произведена оценка защищенности от несанкционированного доступа запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу, разработанной системы и аналогов. Оценка защищенности разработанной системы показывает достаточный уровень ее защищенности от комплексных угроз (просмотр, подмена, перехват и радиоэлектронное подавление трафика) по сравнению с известными системами данного класса. Среди основных преимуществ разработанной системы следует упомянуть повышенную защищенность от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей, в которых потенциально можно использовать широкий класс хаотических сигналов. Так же следует отметить повышенную вероятность идентификации проверяемых транспортных средств за счет использования принципа «свой-чужой» и RFID-меток. Среди основных недостатков предложенной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами.

Ключевые слова: идентификация, контроль доступа, транспортные средства, радиоканал, имитозащищенность, хаотические сигналы.

Для цитирования. ***ГАВРИШЕВ, Алексей А.; ЖУК, Александр П.*** *РАЗРАБОТКА БЕСПРОВОДНОЙ ИМИТОЗАЩИЩЕННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИЯ И КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 41-51, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1092>. Дата доступа: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.04.*

Aleksei A. Gavrishev, Aleksandr P. Zhuk
North Caucasus Federal University,
Pushkin St., 1, Stavropol, 355009, Russia
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

Development of a wireless protection against imitation system for identification and control of vehicle access

DOI: http://dx.doi.org/10.26583/bit.2018.1.04

Abstract. This article deals with wireless systems for identification and control of vehicle access to protected objects. Known systems are considered. As a result, it has been established that one of the most promising approaches to identifying and controlling vehicle access to protected objects is the use of systems based on the "friend or foe" principle. Among these systems, there are "one-directional" and "bedirectional" identification and access control systems. "Bidirectional" systems are more preferable for questions of identification and access control. However, at present, these systems should have a reduced probability of recognizing the structure of the request and response signals because the potential attacker can easily perform unauthorized access to the radio channel of the system. On this basis, developed a wireless system identification and control vehicle access to protected objects based on the principle of "friend or foe", featuring increased protection from unauthorized access and jamming through the use of rewritable drives chaotic sequences. In addition, it's proposed to use to identify the vehicle's RFID tag containing additional information about it. Are some specifications of the developed system (the possible frequency range of the request-response signals, the communication range, data rate, the size of the transmitted data, guidelines for choosing RFID). Also, with the help of fuzzy logic, was made the security assessment from unauthorized access request-response signals based on the system of "friend or foe", which are transferred via radio channel, developed systems and analogues. The security assessment of the developed system shows an adequate degree of protection against complex threats (view, spoofing, interception and jamming of traffic) in comparison with known systems of this class. Among the main advantages of the developed system it's necessary to mention increased security from unauthorized access and jamming through the use of rewritable drives chaotic sequences, in which you can potentially use a wide class of chaotic signals. It should also be noted the increased likelihood of identification check the vehicle through the use of the principle of "friend or foe" and RFID. Among the main disadvantages of the proposed system it should be noted the need for precise synchronization between transmitting and receiving sides.

Keywords: identification, access control, vehicles, radio channel, protection against imitation, chaotic signals.

For citation. ***GAVRISHEV, Aleksei A.; ZHUK, Aleksandr P****. Development of a wireless protection against imitation system for identification and control of vehicle access. IT Security (Russia), [S.l.], v. 25, n. 1, p. 41-51, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1092>. Date accessed: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.04.*

Введение

В настоящее время для охраны и защиты различных важных объектов и людей применяются различные системы безопасности. В последнее время большое развитие получили беспроводные системы безопасности. Целесообразность использования радиоканала в системах безопасности объясняется несколькими факторами [1, 2], среди которых выделяют простоту организации, меньшие затраты на построение и эксплуатацию, возможность применения при отсутствии проводных линий связи и в чрезвычайных ситуациях, возможность оперативного изменения структуры и параметров систем при наращивании объектов охраны.

Одной из самых распространенных беспроводных систем безопасности в настоящее время являются системы автомобильной безопасности. Среди областей ее применения

можно выделить, например, охрану транспортных средств (ТС) от угонов [3], идентификацию и контроль доступа ТС на охраняемые объекты [4]. Разработка новых методов и технологий идентификации и контроля доступа ТС на охраняемые объекты является актуальной задачей [4].

Целью данной статьи является разработка беспроводной имитозащищенной системы идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой».

Основная часть

Анализ предметной области

Как известно [5], на любом важном охраняемом объекте обычно присутствует внутренняя зона, территория объекта, а также проходная для ТС (легковые и грузовые автомобили, специальная и военная техника и т.д.) и персонала. С целью исключить несанкционированный доступ на территорию объекта, предотвращения терактов и прочее, проходная для ТС обычно ограждается с помощью различных инженерных сооружений, например, заграждения (заборы, шлагбаумы, ворота), противотаранные заграждения (надолбы, металлические ежи, бетонные блоки) и т.д. [6].

В настоящее время интерес представляют автоматизированные системы контроля доступа, которые могут провести дистанционную идентификацию и контроль доступа людей и ТС [5]. Остановимся подробнее на известных методах и технологиях идентификации и контроля доступа ТС. Так в работе [7] описываются известные системы идентификации и контроля доступа ТС: антитеррористическая система контроля доступа и въезда на социально-значимые объекты «Барьер», автоматизированная система контроля подъездных путей к охраняемым объектам «Блокхост-КСКПП», а также система контроля доступа ТС (Полезная модель РФ № 144117, опубл. 10.08.2014). Среди их основных недостатков отмечается тот факт, что функция автоматического распознавания регистрационных номеров не дает 100 % вероятности распознавания, и нет возможности отличить поддельные номера [7]. Кроме того, отмечается, что применяемые в них типы заграждений не являются достаточной защитой от несанкционированного доступа. Так же следует отметить, что, как в данных системах, так и в аналогичных системах, предусмотрена возможность исключительно ручного контроля проезжающих ТС, однако это не является удачным вариантом [4].

Другим примером системы идентификации и контроля доступа ТС является использование каких-либо уникальных идентификаторов, например, систем на основе принципа «свой-чужой». Примером использования уникальных идентификаторов является система контроля проезда автомобилей [8]. В ее основу положено использование RFID-меток (далее «Т1»). Для RFID-меток можно предусмотреть защиту от клонирования, а также криптографическую защиту передаваемой информации. Принцип функционирования системы прост [8]: при обнаружении метки считыватель сопоставляет её данные с внутренней таблицей доступа и после этого системой принимается решение о допуске/не допуске ТС на охраняемую территорию. Так же в работе [4] предлагается многоэтапная радиочастотная идентификация ТС, заключающаяся в разделении уникальных идентификационных данных (далее «Т2»). Так на первом этапе информационного обмена между меткой и считывателем запрашивается государственный регистрационный номер ТС, высота ТС и т.д. (этот процесс идет без шифрования). Затем по дополнительному запросу выдаются специальные регистрационные, конструкторские или технологические данные (в этом случае требуется шифрование с минимальной криптографической стойкостью). После этого по специальному запросу должны выдаваться наиболее секретные данные о ТС, а также его VIN (идентификационный номер транспортного средства). В этом случае необходимо шифрование с максимальной криптографической стойкостью.

Пример технологии на основе принципа «свой-чужой» приведен так же в работе [9]. Отличительной чертой данного подхода является использование в стационарном блоке управления и в мобильном брелоке управления одинаковых генераторов псевдослучайных последовательностей (ПСП), которые инициализируются общим генератором случайных чисел, находящимся в стационарном блоке управления (далее «Т3»). Таким образом, в случае легального пользователя оба генератора ПСП должны выдать одинаковые последовательности и, наоборот, в случае нелегального пользователя, выдать различные последовательности, о чем будет выдано уведомление. Данная технология хоть и заточена для охраны автомобилей от несанкционированного доступа, однако легко может быть перенесена на случай систем идентификации и контроля доступа ТС.

Так же известна система, в которой, среди прочего, применяются радиочастотные метки (содержат уникальные идентификаторы транспортного средства), сканирующее устройство и сложные сигналы с фазовой модуляцией (ФМС) [10]. Уникальные идентификаторы ТС вносятся в базу данных и могут легко быть считаны сканирующим устройством с радиочастотных меток через защищенный от несанкционированного доступа радиоканал (далее «Т4»). В качестве дополнительного уникального идентификатора может использоваться несмываемый тайнописный краситель (например, на ветровом стекле), обнаруживаемый в ультрафиолетовых лучах.

Далее рассмотрим систему автомобильной сигнализации, предложенную в работе [11]. В ней предлагается использовать автокорреляционную широкополосную систему связи на основе модуляции фазы передаваемого сигнала. Данная система позволяет значительно повысить защищенность от несанкционированного доступа. При соответствующей адаптации данная технология может найти применение для систем идентификации и контроля доступа ТС (далее «Т5»).

Как видно из приведенного анализа, одним из самых перспективных подходов к идентификации и контролю доступа ТС на охраняемую территорию является использование систем на основе принципа «свой-чужой». Здесь следует отметить, что система на основе принципа «свой-чужой» может быть как «однонаправленная», когда уникальный идентификатор передается на блок контроля и сравнивается с эталонным списком, например, [8], так и «двунаправленная», когда присутствуют как запросные, так и ответные сигналы [9]. Второй вид системы на основе принципа «свой-чужой» является более предпочтительным для вопросов идентификации и контроля доступа ТС [4, 9]. Однако, в настоящее время отмечается, что такие «двунаправленные» системы на основе принципа «свой-чужой» должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов злоумышленником за счет высокой скрытности структуры передаваемой информации [12]. Это следует из того, что в настоящее время достаточно легко выполнить несанкционированный доступ к радиоканалу систем безопасности для злоумышленных действий (например, просмотр, подмена, перехват и подавление помехами) [13]. Методами защиты от данных угроз в беспроводных системах автомобильной безопасности потенциально могут стать криптографические методы защиты информации (КМЗИ) [3, 13], а также технологии на основе шумоподобных сигналов (ШПС) [3, 13].

Одним из самых перспективных методов одновременной защиты радиоканала от несанкционированного доступа (просмотр, подмена, перехват) и подавления помехами в системах автомобильной безопасности в настоящее время могут стать технологии на основе шумоподобных сигналов, например, использование хаотических сигналов (ХС) [3, 13, 14]. Так в работе [14] рассматривается использование сверхширокополосных сигналов на основе хаотических сигналов в системе автомобильной безопасности, в частности сигнализация, идентификация и т.д. (далее «Т6»). Отмечается, что сигналы данного вида обеспечивают защиту от помех и повышенную защищенность от несанкционированного доступа [14]. В частности, известно [15], что ХС позволяют добиться повышенной защищённости от несанкционированного доступа за счёт повышенной структурной скрытности по сравнению с «классическими» видами ШПС. Так структурная скрытность

«классических» видов ШПС сначала увеличивается, а потом, по мере увеличения базы, уменьшается, в то время, как структурная скрытность ХС быстро возрастает [15].

Разработаем на основе хаотических сигналов беспроводную имитозащищенную систему идентификации и контроля доступа ТС на охраняемые объекты на основе принципа «свой-чужой» (далее «Т7»).

Разработка беспроводной имитозащищенной системы идентификации и контроля доступа транспортных средств на охраняемые объекты

Для этих целей рассмотрим рис. 1, на котором приведена структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков [16]. Данная технология предназначена для защиты информационного обмена между блоком контроля и оконечными датчиками в охранно-пожарных системах за счет использования перезаписываемых накопителей хаотических последовательностей [17]. Концептуально данное устройство имитозащиты контролируемых объектов состоит из блока контроля, включающего в себя генератор первой псевдослучайной последовательности (ПСП-1), генератор второй псевдослучайной последовательности (ПСП-2), накопитель хаотической последовательности (НХП), накопитель копии хаотической последовательности (НКХП), устройство сравнения (УС) и контролируемого объекта (датчика), включающего в себя генератор ПСП-2, НХП, НКХП [16].

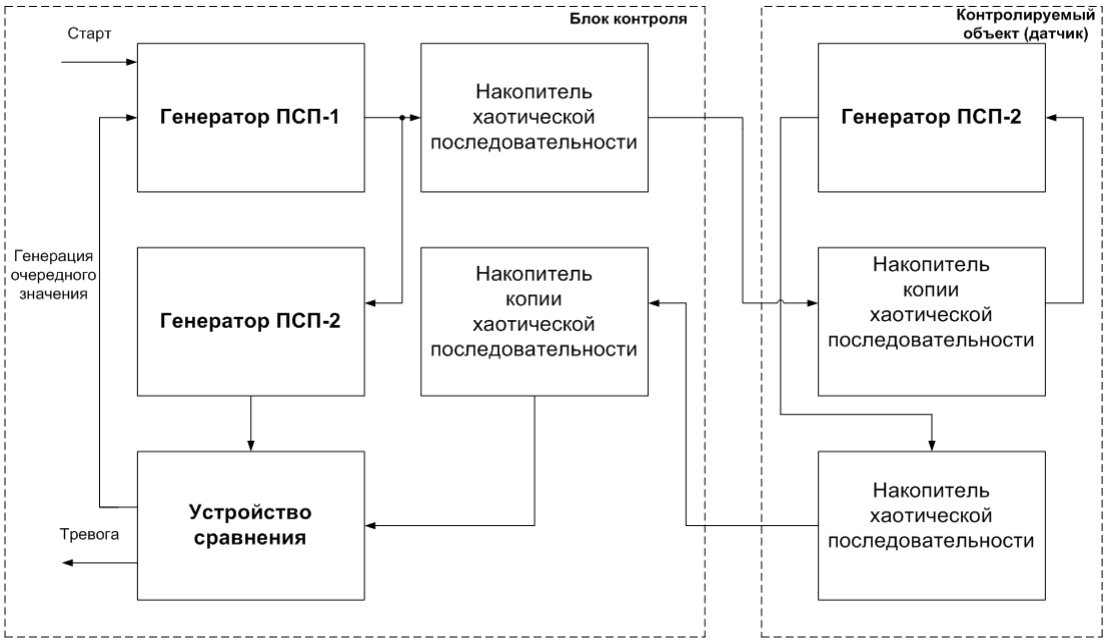

Рис.1. Структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков
(Fig. 1. Block diagram of apparatus for protection against imitation of controlled objects with high structural security of carrier signals)

Рассматриваемое устройство имитозащиты контролируемых объектов функционирует следующим образом [16]. Для запуска блока контроля на вход генератора ПСП-1 подаётся стартовая команда. Затем генератор ПСП-1 вырабатывает первую ПСП. Полученное значение отправляется на генератор ПСП-2 блока контроля и одновременно с этим в НХП перемножается с ХС и, после вхождения в режим синхронизации, через линию связи передается на контролируемый объект (датчик). После этого в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в блоке контроля, и далее декодированный сигнал в виде последовательности поступает в генератор ПСП-2, функция генерации последовательности которого идентична функции генератора ПСП-2 блока контроля. Затем в НХП происходит перемножение

последовательности ПСП-2 контролируемого объекта (датчика) с ХС и, после вхождения в режим синхронизации, через линию связи передаётся на блок контроля. Далее в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в контролируемом объекте (датчике), и после чего декодированный сигнал в виде последовательности поступает на УС, в котором проверяется отклик ранее пришедшего значения генератора ПСП-2 блока контроля и отклик генератора ПСП-2 контролируемого объекта (датчика). В случае совпадения значений, пришедших от контролируемого объекта (датчика) и блока контроля, вырабатывается сигнал «Норма», который служит для генерации следующего псевдослучайного числа генератором ПСП-1. При несовпадении значений, устройство сравнения выдает команду «Тревога».

Отдельно отметим, что более подробное описание данного подхода, в том числе, подробное описание процесса умножения информационного сигнала на ХС на передающей стороне и его восстановление на приемной стороне, приведено в работе [17].

Используем данный подход для разработки беспроводной имитозащищенной системы идентификации и контроля доступа ТС на охраняемые объекты на основе принципа «свой-чужой». Для этого воспользуемся структурной схемой (рис. 1) с изменениями и уточнениями: правую часть вместо «контролируемого объекта (датчика)» обозначим как «транспортное средство». Кроме того, заметим, что ТС так же должно иметь RFID-метку (например, на ветровом стекле), в которой должна содержаться некоторая секретная информация о ТС, например, его VIN (идентификационный номер транспортного средства). Она служит для дополнительной идентификации ТС. Так же в перезаписываемых накопителях (перезаписываемые запоминающие устройства) ТС и блока контроля должны быть записаны одинаковые наборы хаотических последовательностей (при необходимости они могут периодически перезаписываться на новые последовательности [17; 18]).

Таким образом, при въезде/выезде ТС на территорию охраняемого объекта в автономном режиме, оно находится на некотором расстоянии перед внешними воротами шлюза (для упрощения на рис. не показано). В данном варианте исполнения шлюз оборудован управляемыми преградами, выполненными в виде ворот (для упрощения на рис. не показано). Исходное состояние – внешние ворота закрыты. Могут гореть красные светофоры, запрещающие движение [7]. После этого, блок контроля вырабатывает первую ПСП, которую одновременно отправляет в свой генератор ПСП-2 и в НХП, где она перемножается с ХС, и при вхождении в режим синхронизации, отправляется в ТС. Далее ТС декодирует переданный сигнал с помощью НКХП и вырабатывает свою вторую ПСП, которая перемножается с ХС в НХП, и при вхождении в режим синхронизации, отправляется в блок контроля. Блок контроля декодирует ее в НКХП и отправляет в свое устройство сравнения, в которое так же должна прийти ранее им выработанная вторая ПСП. Таким образом, в устройстве сравнения блока контроля сравниваются вторая ПСП ТС и вторая ПСП блока контроля (рис. 1). В случае верного сравнения блоком контроля дается команда на генерацию нового значения первой ПСП (для следующего случая въезда/выезда), открываются внешние ворота, и ТС может въехать в шлюз. В этом случае могут гореть зеленые сигналы светофора, разрешающие въезд [7]. Затем внешние ворота за ТС закрываются. В случае неверного сравнения или невозможности войти в режим синхронизации ворота не открываются (дальнейшие действия зависят от должностных лиц). После этого, в шлюзе считыватель должен считать информацию с RFID-метки ТС и сравнить полученную информацию (VIN ТС) с таблицей доступа (для упрощения на рис. не показано). В случае совпадения VIN ТС с таблицей доступа, открываются внутренние ворота, и ТС может въехать на охраняемую территорию. В случае несовпадения VIN ТС с таблицей доступа, внутренние ворота не открываются (дальнейшие действия зависят от должностных лиц). Так же возможно предусмотреть процедуру досмотра ТС, а также его видеосъемку: в таком случае открытие внутренних ворот будет определяться должностными лицами в ручном режиме. Процедура выезда с территории объекта

аналогична процедуре въезда. Для упрощения процедуры выезда можно предусмотреть выезд с территории объекта исключительно с помощью RFID-метки.

Рассмотрим некоторые технические характеристики разработанной системы идентификации и контроля ТС. К одной из основных характеристик таких систем относится частотный диапазон запросно-ответных сигналов. В настоящее время в России для беспроводных систем безопасности самыми распространенными не лицензируемыми диапазонами частот являются 2,4 ГГц, 433 МГц, 868 МГц [19]. Как известно [19], в диапазоне 2,4 ГГц работают такие известные популярные стандарты связи, как Bluetooth, Wi-Fi и ZigBee, что очень сильно зашумляет эфир. Основными характеристиками диапазона 2,4 ГГц являются относительно большая скорость передачи данных (до десятков Мбит/с), малая дальность связи (до 100 м) и отсутствие способности волны огибать препятствия [19]. Субгигагерцевые диапазоны 433 МГц и 868 МГц, по сравнению с диапазоном 2,4 ГГц, обладают следующими характеристиками: обеспечивают приемлемую дальность связи (до 1000 м), обладают пониженным энергопотреблением, способностью волны огибать препятствия (дифракция), скоростью передачи данных свыше 200 Кбит/с [19]. Одним из главных условий их использования, является соответствие радиопередающих устройств техническим требованиям, утвержденным решением Государственной комиссии по радиочастотам [20]. Поэтому в разработанной системе идентификации и контроля ТС, в силу функционирования, в том числе, и на открытой местности, а также необходимости удаленной идентификации ТС, предлагается использовать субгигагерцевые диапазоны.

Другим важным вопросом является объем передаваемых данных между ТС и блоком контроля. Так как в данной системе идентификации и контроля доступа ТС не передаются «тяжелые» данные (например, видеоизображения), а также нет постоянного непрерывного радиообмена, то объем передаваемых данных будет незначительным. Для рассматриваемых условий можно предположить, что длина используемой ПСП будет равна 128 бит, такую же длину будет иметь ХС, с которым ПСП перемножается. Дополнительно к этому, для различных служебных данных, можно предусмотреть несколько 8-битных полей. В этом случае длина ХС будет чуть больше. В итоге, общий объем передаваемых данных между ТС и блоком контроля не будет выходить за значения максимальной скорости передаваемых данных, которая определена для субгигагерцевых диапазонов (200 Кбит/с).

Среди основных технических недостатков разработанной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами. Поэтому для создания точной синхронизации в системах данного класса целесообразно использовать внешние средства, например, на основе концепции программно-конфигурируемого радио [18].

Далее рассмотрим требования к RFID-метке, служащую в качестве дополнительного метода идентификации ТС. В качестве RFID-метки можно применять, например, пассивные метки (без питания и аккумуляторов), содержащие только уникальный идентификационный номер и функционирующие только на малом расстоянии от считывателя [8], или применять более сложные радиочастотные метки, например, на основе сложных сигналов с фазовой модуляцией [10]. Их частотный диапазон может быть разнообразными, например, 13,553-13,567 МГц (нелицензируемый диапазон частот) или 866-868 МГц (лицензируемый диапазон частот) [20].

Далее проведем оценку защищенности рассмотренных систем идентификации и контроля доступа ТС от комплексных угроз (просмотр, подмена, перехват и подавление помехами), применяемых одновременно. Оценку защищенности будет проводить для запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу. В случае разработанной системы, оценку защищенности проведем для этапа, когда ТС находится перед воротами. Оценку защищенности проведем на основе методики, изложенной в работе [21]. Ее основные этапы изложены ниже:

1) задание кортежа «*Параметры ИБ АвС*»={*At*, *P*}, где «*At*» – уровень атаки, «*P*» – уровень защиты;

2) преобразование нечетких значений переменных «очень низкий», «низкий», «средний», «высокий», «очень высокий» в числовые значения [1, 5];

3) задание важности инцидента ИБ $I_{АвС} = k(m) \times At \times P$;

4) задание численной оценки защищенности радиоканала сигнализации в целом $P_{АвС} = 1 - I_{АвС}$;

5) вычисление обобщенных показателей уровня атаки $At_O = \sum_{i=1}^{n} A_i$ и уровня защиты $P_O = \sum_{i=1}^{n} P_i$;

6) вычисление коэффициента нормирования *k(m)*;

7) вычисление оценки защищенности $P_{АвС} = 1 - k(m) \times At_O \times P_O$;

8) перевод количественной оценки в качественную оценку с помощью таблицы сопоставления.

Более подробно с данной методикой оценки защищенности, в том числе с начальными условиями, примерами расчетов, таблицей перевода количественных оценок защищенности в качественные, можно ознакомиться в работах [13, 21].

Проведем необходимые подготовительные вычисления (таблица 1). Условимся [13], что угроза «просмотр» обозначается как «У1», угроза «подмена» – как «У2», угроза «перехват» – как «У3», угроза «подавление помехами» – как «У4».

В таблице 2 приведен ранжированный список количественных и качественных оценок защищенности беспроводных систем идентификации и контроля доступа ТС, описанных в данной статье. Анализ таблицы 2 показывает, что наиболее защищенными запросно-ответными сигналами в системах идентификации и контроля доступа ТС обладают технологии на основе хаотических сигналов, а наименее защищенными – технологии на основе КМЗИ.

Таблица 1. Результаты подготовительных расчетов

Угрозы	*P*-уровень защиты							*At*-уровень атаки						
	T1	*T2*	*T3*	*T4*	*T5*	*T6*	*T7*	*T1*	*T2*	*T3*	*T4*	*T5*	*T6*	*T7*
У1	3	3	5	3	3	2	2	4	4	5	4	4	4	4
У2	3	3	2	2	2	2	2	4	4	4	4	4	4	4
У3	5	5	5	3	3	2	2	5	5	5	5	5	4	4
У4	5	5	5	3	3	2	2	5	5	5	5	5	4	4

Таблица 2. Количественные и качественные оценки защищенности

№	Устройство (способ)	Метод защиты радиоканала	Количественная оценка защищенности	Качественная оценка защищенности
1	Т7	ШПС (ХС)	0,6800	Высокая
2	Т6	ШПС (ХС)	0,6800	Высокая
3	Т5	ШПС (ФМС)	0,5050	Средняя
4	Т4	ШПС (ФМС)	0,5050	Средняя
5	Т2	КМЗИ	0,2800	Низкая
6	Т1	КМЗИ	0,2800	Низкая
7	Т3	КМЗИ	0,1925	Очень низкая

Заключение

Таким образом, в данной работе проведен анализ известных систем идентификации и контроля доступа ТС на охраняемый объект. Установлено, что одним из самых

предпочтительных вариантов реализации данных систем является использование «двунаправленных» систем на основе принципа «свой-чужой». Однако, в настоящее время отмечается, что такие «двунаправленные» системы на основе принципа «свой-чужой» должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов злоумышленником за счет высокой скрытности структуры передаваемой информации [12]. Это следует из того, что в настоящее время достаточно легко выполнить несанкционированный доступ к радиоканалу систем безопасности для злоумышленных действий (например, просмотр, подмена, перехват и радиоэлектронное подавление передаваемых по радиоканалу данных) [13]. В качестве возможного метода защиты от данных угроз рассматриваются технологии на основе шумоподобных сигналов, а именно – хаотические сигналы [3, 13, 14].

На основании этого была разработана беспроводная имитозащищенная система идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой», отличающаяся повышенной защищенностью от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей. Дополнительно к этому предлагается использовать для идентификации ТС RFID-метку, содержащую VIN ТС.

Были приведены некоторые технические характеристики разработанной системы (возможный частотный диапазон запросно-ответных сигналов, дальность связи, скорость передачи данных, объем передаваемых данных, рекомендации по выбору RFID-меток).

Так же, с помощью аппарата нечеткой логики [21], была произведена оценка защищенности от несанкционированного доступа запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу, разработанной системы и аналогов. Оценка защищенности разработанной системы показывает ее достаточный уровень защищенности от комплексных угроз (просмотр, подмена, перехват и радиоэлектронное подавление трафика) по сравнению с известными системами данного класса.

Среди основных преимуществ разработанной системы следует упомянуть повышенную защищенность от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей, в которых потенциально можно использовать широкий класс хаотических сигналов. Так же следует отметить повышенную вероятность идентификации проверяемых транспортных средств за счет использования принципа «свой-чужой» и RFID-меток. Среди основных недостатков предложенной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами. Для ее создания в системах данного класса предложено использовать внешние средства, например, на основе концепции программно-конфигурируемого радио [18].

СПИСОК ЛИТЕРАТУРЫ:

1 Эсауленко А. В. Моделирование и обеспечение надежности радиоканала в системах безопасности: автореферат дисс. канд. тех. наук. Воронеж. 2015. 19 с.
2 Драгун С. Организация беспроводных охранно-пожарных систем на базе радиосистемы «Стрелец» Технологии безопасности. 2011. № 6. С. 14-15.
3 Жук А. П., Гавришев А. А., Осипов Д. Л., Бурмистров В. А. Анализ методов защиты беспроводных каналов связи автомобильных сигнализаций от несанкционированного доступа Интернет-журнал «Технологии техносферной безопасности». 2016. № 5 (69). С. 173-177.
4 Пономарев В. А., Мороз С. М. Обоснование применения радиочастотной идентификации транспортных средств Журнал автомобильных инженеров. 2017. № 1(102). С. 32-36.
5 Бондарев П. В., Измайлов А. В., Толстой А. И. Физическая защита ядерных объектов: Учебное пособие для вузов. М.: МИФИ, 2008. 584 с.
6 Тарасов Р. А., Упрунина А. А. Основы профессиональной деятельности: учебное пособие для самостоятельной подготовки слушателей. Волжский: ФКОУ ДПО МУЦ УФСИН России по Волгоградской области. 2014. 76 с.
7 Полевой В. Г., Грачев С. Н. Григорьев С. А. Система автоматизированного управления пропуском транспорта Патент РФ № 2610925. 2017. 11 С.

8 Автономная система контроля и управления проездом автомобилей URL: http://www.isbc-rfid.ru/_solutions/id_9/ (дата обращения: 28.11.2017).
9 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.
10 Дикарев В. И., Шубарев В. А., Калинин В. А., Мельников В. А. Способ маркировки автотранспорта Патент РФ № 2464644. 2012. 8 С.
11 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.
12 Бельтов А. Г., Попов А. Р., Жуков И. Ю., Левицкий Н. Е. Способ передачи информации шумоподобными сигналами в системе опознавания «свой-чужой» Патент РФ № 2532085. 2014. 12 С.
13 Гавришев А. А., Жук А. П., Осипов Д. Л. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа Труды СПИИРАН. 2016. Вып. 4(47). С. 28-45.
14 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.
15 Сиващенко С. И. Скрытность радиосистем со сложными и хаотическими сигналами Системи управління, навігації та зв’язку. 2009. № 3(11). С. 56-58.
16 Жук А. П., Гавришев А. А. Альтернативный подход повышения структурной скрытности сигналов-переносчиков устройства имитозащиты контролируемых объектов Спецтехника и связь. 2015. № 2. С. 59-63.
17 Осипов Д. Л., Жук А. П., Гавришев А. А. Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков Патент РФ № 2560824. 2015. 15 с.
18 Мохсени Т. И., Кикот А. М. Когерентная передача цифровой информации с двоичной модуляцией хаотического импульса Журнал радиоэлектроники. 2015. № 6. 24 с.
19 Пушкарев О. Использование диапазонов 433 И 868 МГц в системах промышленной телеметрии Беспроводные технологии. 2012. № 2. С. 42-48.
20 Решение ГКРЧ при Мининформсвязи России от 07.05.2007 N 07-20-03-001 (ред. от 04.07.2017) «О выделении полос радиочастот устройствам малого радиуса действия». 2007. 35 с.
21 Гавришев А. А., Бурмистров В. А., Осипов Д. Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе понятий нечеткой логики Прикладная информатика. 2015. Т. 10. № 4(58). С. 62–69.

REFERENCES:

[1] Jesaulenko A. V. Modelirovanie i obespechenie nadezhnosti radiokanala v sistemah bezopasnosti [Modeling and ensure the reliability of the radio channel security systems]. Ph.D. Thesis. Voronezh Institute of the Ministry of Interior of Russia. Voronezh. Russia. 2015. 19 p. (in Russian).
[2] Dragun S. Organizacija besprovodnyh ohranno-pozharnyh sistem na baze radiosistemy «Strelec» [Organization of wireless fire and security systems based on radio systems «Strelec»]. Tehnologii bezopasnosti. 2011, no. 6, pp. 14–15. (in Russian).
[3] Zhuk A. P., Gavrishev A. A., Osipov D. L., Burmistrov V. A. Analysis of methods of protection of wireless communication channels of car alarm systems from unauthorized access. Tehnologii tehnosfernoj bezopasnosti – Technology of technosphere safety. 2016, no. 5 (69), pp. 173-177. (in Russian).
[4] Ponomarev V. A., Moroz S. M. Obosnovanie primenenija radiochastotnoj identifikacii transportnyh sredstv [The rationale for the use of radio frequency identification of vehicles]. Zurnal AAI. 2017, no. 1(102), pp. 32-36. (in Russian).
[5] Bondarev P. V., Izmajlov A. V., Tolstoj A. I. Fizicheskaja zashhita jadernyh ob’ektov: Uchebnoe posobie dlja vuzov [Physical protection of nuclear facilities: textbook]. Moscow. MIFI Publ. 2008, 584 p. (in Russian).
[6] Tarasov R. A., Uprunina A. A. Osnovy professional'noj dejatel'nosti: uchebnoe posobie dlja samostojatel'noj podgotovki slushatelej [Fundamentals of professional activity: teaching aid for independent preparation of students.]. Volzhskij. FSE IAPE "Interregional training centre of the Department of Federal service of execution of punishments across the Volgograd region". 2014. 76 p. (in Russian).
[7] Grigorev S. A., Grachev S. N., Polevoj V. G. Transport passage automated control system. Patent RF, no. 2610925, 2017, 11 p. (in Russian).
[8] Avtonomnaja sistema kontrolja i upravlenija proezdom avtomobilej [Autonomous system of control and management of passing cars]. URL: http://www.isbc-rfid.ru/_solutions/id_9/ (access: 28.11.2017) (in Russian).
[9] Gavrishev A. A., Burmistrov V. A., Anzin I. V. K voprosu ob ispol'zovanii psevdosluchainykh posledovatel'nostei dlya predotvrashcheniya nesanktsionirovannogo dostupa k radiokanalu avtomobil'noi signalizatsii [To question about the use of pseudo-random sequences to prevent unauthorized access to the radio car alarm]. Sbornik nauch-nykh statei XI Mezhdunarodnoi nauchno-tekhniches-koi konferentsii «Novye informatsionnye tekhnologii i sistemy» [Proceeding of the Eleventh International Conference of Science and Technology «New information technology and systems» (2014, Penza, Russia)]. Penza, PGU Publ., 2014, pp. 270-272. (in Russian).

[10] Dikarev V. I., Shubarev V. A., Kalinin V. A., Mel'nikov V. A. Method of labelling vehicles. Patent RF, no. 2464644, 2012, 8 p. (in Russian).
[11] Frolov V., Kovtunov J., Kubata V. Methods of providing noise immunity in automobile anti-theft system control. Road transport. 2013, i. 33, pp. 105-109. (in Ukrainian).
[12] Bel'tov A. G., Popov A. R., Zhukov I. J., Levitskij N. E. Method to transmit information by noise-like signals in friend-or-foe detection system. Patent RF, no. 2532085, 2014, 8 p. (in Russian).
[13] Gavrishev A. A., Zhuk A. P., Osipov D. L. Analysis of protection technologies radio fire alarm systems against unauthorized access. SPIIRAS Proceedings. 2016, i. 4(47), pp. 28-45. (in Russian).
[14] Mohseni T. I., Ryzhov A. I., Lazarev V. A. Jeksperimenty po primeneniju SShP sredstv svjazi v avtomobile [Experiments on the use of UWB communications in the car]. Trudy 55-j nauchnoj konferencii MFTI. Radiotehnika i kibernetika [Proceedings of the 55th scientific conference of MIPT. Radio engineering and Cybernetics]. V. 2. Moscow. MIPT Publ. 2012, P. 103. (in Russian).
[15] Sivashchenko S. I. Secrecy of radio system with difficult and chaotic signals. Systemy upravlinnja, navigacii' ta zv'jazku – Systems of control, navigation and communication. 2009, v. 3(11), pp. 56–58 (in Russian).
[16] Zhuk A. P., Gavrishev A. A. Alternative approach of increased structural stealth signal-carrying device simulation protection of the controlled objects. Spetstekhnika i svyaz' – Specialized machinery and communication. 2015, v. 2, pp. 59–63. (in Russian).
[17] Osipov D. L., Zhuk A.P., Gavrishev A. A. Apparatus for protection against imitation of controlled objects with high structural security of carrier signals. Patent RF, no. 2560824, 2015, 15 p. (in Russian).
[18] Mohseni T. I., Kikot A. M. Kogerentnaya peredacha tsifrovoi informatsii s dvoichnoi modulyatsiei khaoticheskogo impul'sa [Coherent transfer of digital information with binary modulation of the chaotic pulse]. Zhurnal radioelektroniki. 2015, no. 6, 24 p. (in Russian).
[19] Pushkarev O. Ispol'zovanie diapazonov 433 I 868 MGc v sistemah promyshlennoj telemetrii [The use of ranges 433 And 868 MHz systems industrial telemetry]. Wireless Technologies. 2012, no. 2, pp. 42-48. (in Russian).
[20] Reshenie GKRCh pri Mininformsvjazi Rossii N 07-20-03-001 (red. ot 04.07.2017) «O vydelenii polos radiochastot ustrojstvam malogo radiusa dejstvija» [The decision of SCRF the Ministry of communications of Russia No. 07-20-03-001 (ed. by 04.07.2017) "On the allocation of radio frequencies to devices of small radius of action"]. 2007, 35 p. (in Russian).
[21] Gavrishev A. A., Burmistrov V. A., Osipov D. L. Assessment the security of wireless alarm from unauthorized access based on the concepts of fuzzy logic. Prikladnaya informatika – Journal of Applied Informatics. 2015, v. 10, no. 4(58), pp. 62–69. (in Russian).

Поступила в редакцию – 01 декабря 2017 г. Окончательный вариант –05 февраля2018 г.
Received – December 01, 2017. The final version – February 05, 2018.