УДК 621.391:004.73

МЕТОД ПОВЫШЕНИЯ СТОЙКОСТИ ЭЛЕКТРОННЫХ КОДОВЫХ ЗАМКОВ

Фауре Э. В., *к.т.н., доцент,*
Лисицына Е. С., *к.т.н.,*
Нестеренко Д. Ю.
Черкасский государственный технологический университет
Черкассы, бул. Шевченко, 460
faureemil@gmail.com

Аннотация. *В работе решаются вопросы повышения стойкости электронных кодовых замков. Исследуются возможности использования несимметричных ключевых систем, исключающих возможность вычисления ключа разблокирования по перехваченному ключу блокирования, использования систем с передачей сигналов ниже уровня шумов, скрывающих сам факт передачи команд «блокировка-разблокировка» доступа, и систем с принудительным зашумлением канала связи. Определены условия, при которых этот комплекс мер является оптимальным.*

Ключевые слова: *электронный кодовый замок, блокировка доступа, шумоподобный сигнал, принудительное зашумление.*

THE METHOD OF THE INCREASE OF DURABILITY OF ELECTRONIC COMBINATION LOCKS

Faure E. V, *Ph.D., associate professor*
Lisitsyna E. S., *Ph.D.,*
Nesterenko D. Y.
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy
faureemil@gmail.com

Abstract. *In the paper the issues of the increase of durability of electronic combination locks are solved. The possibilities of using asymmetric key systems, which exclude the possibility of unblocking key calculation by intercepted blocking key, systems with signal transmission below the level of noise to hide the fact of command "lock-unlock", and systems with forced noising of communication channel are investigated. The conditions for which this package of measures is optimal are determined.*

Keywords: *electronic combination lock, access lock, noise-like signal, forced noise pollution.*

Введение. Электронные кодовые замки получают все более широкое применение во всех сферах жизнедеятельности человека, в том числе в охранных системах ограничения доступа в здания, сооружения, помещения. Важную, если не лидирующую роль подобные устройства занимают в системах охраны автомобилей. Появление систем защиты активизировало разработку средств взлома электронных кодовых замков, что, в свою очередь, породило непрерывный состязательный процесс совершенствования систем замков и их взлома (ключей и отмычек) [1, 2, 3].

Выделение не решенных ранее частей общей проблемы. Несмотря на то, что к настоящему времени получен большой опыт взаимных состязаний в процессе совершенствования систем замков и их взлома, многие возможности повышения стойкости замков остались неисследованными. В настоящей работе приводится анализ следующих путей повышения стойкости электронных кодовых замков:

– применение несимметричных ключей для разрешения/блокировки доступа, что делает бессмысленным перехват ключа блокировки и его использования для разблокировки;

– применение сигналов, лежащих ниже уровня шума, для скрытия момента передачи кодовой комбинации (использование шумо-

подобных сигналов (ШПС) для передачи кодовых последовательностей);
– принудительное зашумление кодовой последовательности (наложение на кодовый вектор вектора шума) для противодействия криптографическому анализу кодовых последовательностей.

Постановка задачи. Задачей исследования является выбор кодовых последовательностей для несимметричных ключевых систем, определение базы ШПС с учетом преднамеренного предварительного зашумления кодовых последовательностей, имитационное моделирование системы и анализ полученных результатов. При решении поставленной задачи будем исходить из постулата, что противник располагает полным набором необходимых для взлома ресурсов: финансовых, материальных, интеллектуальных, а также будем считать, что ему доступны все средства и компоненты электронного замка.

Решение задачи. Для решения поставленной задачи, прежде всего, определим требуемое значение размерности ключевого пространства и его связь с показателем стойкости системы.

Положим, что противник приобрел экземпляр кодового замка, вложил в него собственный ключ и передал для криптоанализа путем взлома грубой силой. Положим, что он располагает вычислительными ресурсами, достаточными для перебора 10^{18} ключей/с (такая производительность на сегодняшний день недостижима при обозримых материальных затратах). Максимальное число переборов, выполненное криптоаналитиком за год, будет равняться $3{,}15\cdot10^{25}$. Положим, что физическое старение техники (например, автомобильной) происходит на протяжении 10-20 лет, а моральное – гораздо быстрее (за 3-5 лет). С учетом этого положим, что криптостойкость ключа должна быть не менее 10 лет. За это время криптоаналитик выполнит максимум $3{,}15\cdot10^{26}$ переборов ключей. Исходя из этого, объем ключевого пространства должен быть не менее $3{,}15\cdot10^{26}$. Учтем, что не все ключи из этого пространства можно использовать – например, ключи, состоящие из одних единиц или нулей, ключи с низкой плотностью единиц или нулей и т.п. Положим, что для практических потребностей можно использовать 10 % мощности всего пространства ключей. Учтем также, что из полученного подпространства следует выбирать ключи блокировки и разблокировки, по меньшей мере, для миллионной группировки автомобилей. Все сказанное приводит к тому, что мощность ключевого пространства необходимо увеличить минимум на 10 порядков до значения $3{,}15\cdot10^{36}$ ключей. Отсюда разрядность ключа должна быть не менее $n \approx \log_2 3{,}15\cdot10^{36}$. Примем n = 120 бит или 15 байт.

Отметим, что используемые ключевые комбинации должны быть статистически независимы. Следовательно, порождающий генератор должен формировать равномерно распределенную последовательность некоррелированных случайных чисел.

Если ключевую последовательность передать по открытому радиоканалу с уровнем сигнала ниже уровня шума, то может быть скрыт сам факт передачи команды блокировки/разблокировки доступа в автомобиль. Учтем также, что время передачи в открытое радиопространство ключа блокировки/разблокировки должно быть ограничено и не зависеть от времени удержания кнопки устройства управления (брелока).

Для повышения стойкости к взлому, в дополнение к занижению уровня сигнала, на передаваемую кодовую последовательность наложим вектор шума.

С учетом изложенного, в данной работе будут исследованы свойства несимметричных ключевых систем, работающих с предварительно зашумленным сигналом ниже уровня шума. Ограничим время пребывания ключевой последовательности в открытом радиопространстве временем, равным 0,1 с. Если уровень излучаемого сигнала лежит ниже уровня шума, то выделить его из принимаемой перехватчиком смеси представляется проблематичным. Это обстоятельство затрудняет деятельность злоумышленника при попытке незамедлительного использования перехваченной ключевой комбинации.

Положим, что при передаче используется фазоманипулированный ШПС (ФМ ШПС), а прием производит когерентный ФМ ШПС приемник. Тогда в приемнике замка за время существования сигнала в пространстве (0,1 с) должны быть выполнены следующие процедуры: синхронизация когерентной несущей приемника; синхронизация тактовой частоты приемника; синхронизация циклов приемника; декодирование кодовой последовательности.

Заметим, что первые три фазы могут быть объединены единым смыслом – установ-

ление логического соединения передатчика и приемника. Они требуют случайного по величине запаса времени, в то время как процедура декодирования кодовой комбинации, по существу, не требует затрат времени. Это объясняется тем, что процедура декодирования кодовой последовательности заключается в сравнении принятой кодовой комбинации с ожидаемой. Такая последовательность операций установления соединения, случайный характер затрат времени установления синхронизации и необходимость минимизации времени установления соединения требует введения специальных сигналов. Так, для минимизации времени установления синхронизации по несущей требуется, чтобы передатчик выдавал немодулированную несущую, а для минимизации времени установления синхронизации по тактам передатчик должен выдавать несущую, модулированную последовательностью 101010…; для минимизации времени установления синхронизации по циклам передатчик должен выдавать специальную кодовую комбинацию цикловой синхронизации. Учтем также, что система не имеет канала обратной связи, а прием осуществляется в условиях, когда принимаемый сигнал ниже уровня шума.

Отсюда следует, что задача синхронизации несущей сводится к выделению из смеси сигнала с шумом гармонического колебания априорно известной несущей и подстройку под выделенный сигнал своего генератора несущей. Задача синхронизации тактов сводится к синхронному детектированию принятого ФМ сигнала когерентной несущей и подстройку под выделенный сигнал данных (вида 101010…) своего генератора тактов. Заметим, что время удержания синхронизма после завершения процедуры установления соединения должно быть не менее 0,1 с. Для синхронизации циклов должна быть использована специальная кодовая комбинация, обладающая повышенной различимостью в векторной смеси сигнала и шума. В работе [4] показано, что для использования в этих условиях вектор синхронизации должен иметь «хорошую» автокорреляционную функцию (АКФ) – иметь равный единице основной лепесток и боковые лепестки, не превышающие величины $\left|1/T\right|$, где Т – число бит синхропоследовательности. Такими свойствами обладают М-последовательности и последовательности Баркера. Также в работе [4] предложен приемник для работы в интенсивном шуме, реализующий принцип максимального правдоподобия и обеспечивающий минимальное время вхождения в синхронизм.

В целом, будем считать, что каждая из фаз по своей длительности не должна превышать времени однократной передачи команды, а ключевая комбинация должна быть повторена не менее 3-5 раз. Тогда для гарантированного вхождения в синхронизм на каждой из фаз и последующего декодирования кодовой последовательности за время, равное 0,1 с, ключевая комбинация должна повториться 10 раз, что выполняется при скорости передачи данных B_0 = 12 Кбит/с.

Пусть уровень передачи сигнала блокировки/разблокировки доступа равен

$$P_{tr} = 10 \cdot \lg \frac{W_{tr}}{W_0}, \qquad (1)$$

где W_{tr} – мощность излучения,

W_0 – эталонная мощность, $W_0 = 1 мкВт$.

В существующих системах ограничения доступа эта мощность фиксирована, определяется запасом энергии аккумулятора брелока и, например, равна 10 мкВт.

Если уровень сигнала ниже уровня шума, то уровень передачи должен регулироваться в зависимости от мощности шума на входе приемника и величины затухания в тракте «передатчик-приемник». Отметим, что поскольку приемник замка всегда находится в режиме прослушивания канала, то, когда сигнал блокировки/ разблокировки не передается, приемник принимает шум окружающей среды и поэтому всегда «знает» уровень шума.

В общем случае [5] затухание сигнала между передатчиком и приемником

$$a(\partial Б) = 33 + 20(\lg r + \lg f), \qquad (2)$$

где r – расстояние между передатчиком и приемником в километрах,

f – частота несущей (Мгц).

Пусть уровень шума на входе приемника равен $P_ш$, порог чувствительности приемника – $P_{пор}$, защищенность (разность уровней между сигналом и шумом) – $\Delta P = P_{пм} - P_ш$, а уровень сигнала на входе приемника – $P_{пм} = P_{пд} - a$. Это значит, что

$$P_{пд} = \left(P_ш + \Delta P + a\right) \le 10 \partial Б. \qquad (3)$$

Учтем также, что $P_{пд} \le 10 \partial Б$, а порог чувствительности приемника $P_{пор} \ge -120 \partial Б$.

Заметим, что при работе на уровне чувствительности приемника не обеспечивается устойчивое «открытие-закрытие» замка. Поэтому для устойчивой работы уровень сигнала на входе приемника выберем на 10 дБ выше порога, а порогом устойчивой работы замка будем считать $P_{пор} = -110 дБ$.

Тогда условием физической реализуемости системы со скрытием сигналов управления электронным замком являются следующие соотношения:

$$\begin{aligned} P_{пд} &= \left(P_ш + \Delta P + a\right) \le 10 дБ, \\ P_{пм} &= \left(P_ш + \Delta P\right) \ge -110 дБ. \end{aligned} \quad (4)$$

На основе этих соотношений может быть построена адаптивная система – система, в которой при известных параметрах (мощности передачи, порога чувствительности приемника, несущей частоты, измеренного значения мощности шума) определяется требуемая база ШПС и оптимальное значение удаления передатчика от приемника. Сведения о параметрах системы должны вводиться в передающую часть устройства, а оптимальное значение удаления – на дисплей для пользователя.

Далее будем рассматривать именно адаптивную систему скрытной передачи команд блокировки/разблокировки доступа. Прежде всего, отметим, что с точки зрения маскировки команд наиболее опасной является ситуация, когда уровень шума окружающей среды соизмерим с порогом чувствительности приемника. В этом случае о маскировании команд можно говорить лишь в условиях, когда базовая станция содержит генератор маскирующего шума с регулируемым в широких пределах уровнем излучения. Такие системы наиболее эффективны в стационарных системах ограничения доступа, поскольку оптимальные параметры системы могут быть установлены при развертывании и поддерживаться таковыми лишь подстройкой уровня маскирующего шума. В мобильных системах ограничения доступа оптимальные параметры системы должны меняться каждый раз при изменении места парковки автомобиля.

В целом, адаптивная система управления доступом представлена на рис. 1 и содержит передающую часть и базовую станцию, при этом все взаимодействия между составными частями внутри каждого из устройств происходят через адаптеры сопряжения и путем передачи сигналов по общей шине.

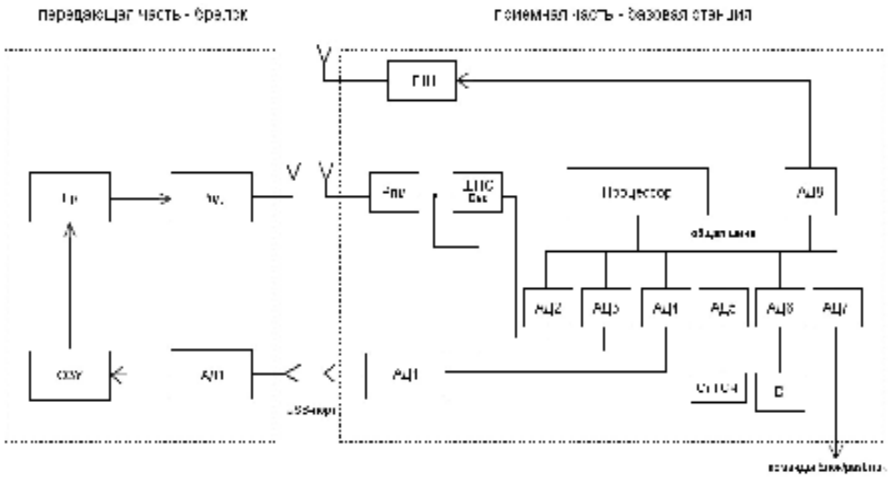

Рис. 1. Структурная схема электронного кодового замка

Передающая часть располагается в брелоке и имеет жесткие ограничения по габаритно-массовым показателям и энергетическому ресурсу. Передающая часть содержит радиопередатчик (Рпд) и адаптер связи с базовой станцией (USB-порт АД1), оперативную память (ОЗУ) и преобразователь сигналов (Пр).

До начала применения системы брелок через USB-порт подключен к базовой станции для подзарядки аккумулятора.

При остановке автомобиля и выключении двигателя приемник принимает шумы окружающей среды и через адаптер сопряжения АД8 выдает их в процессор. Процессор вычисляет мощность шума, включает (при необходимости) генератор маскирующего шума (ГШ) с необходимым уровнем излучаемой мощности, вычисляет оптимальное удаление между передатчиком и приемником, которое выводит с помощью адаптера АД6 на

экран дисплея (D) для информирования водителя. Кроме того, процессор вычисляет оптимальное значение базы ШПС, запускает посредством адаптера АД5 стохастический генератор (Ст ГСЧ) и отбирает две последовательности из потока случайных чисел, одну – как ключ блокировки, другую – как ключ разблокировки. Эти сведения процессор держит у себя в памяти для последующего использования и через адаптер АД4 и USB-порт вводит в оперативную память брелока.

Когда владелец автомобиля вышел из него и нажал кнопку «блокировка доступа», передатчик брелока выводит в окружающее радиопространство в заданном формате сначала последовательность установления логического соединения, а затем команду блокировки доступа. Радиоприемное устройство (Рпм) с использованием адаптера АД3 принимает смесь ШПС с шумом, декодирует ее с помощью декодера (ШПС Dec) через адаптер АД2 и формирует команду управления на блокировку, передаваемую адаптером АД7. Аналогичные процедуры производятся и при разблокировке доступа.

Произведем оценку требуемой базы ШПС. База ШПС, в конечном итоге, определяется граничным значением вероятности битовой ошибки, которую требуется получить в результате демодуляции ШПС. Для рассматриваемого класса систем ограничения доступа зададим следующий диапазон вероятности битовой ошибки на выходе демодулятора ШПС: $0{,}1 \le P_{дем} \le 0{,}3$.

Для опытной проверки принятых решений произведено имитационное моделирование системы. На рис. 2 приведены полученные экспериментальные значения вероятности битовой ошибки когерентного приемника ФМ ШПС при различных значениях базы ШПС в зависимости от защищенности.

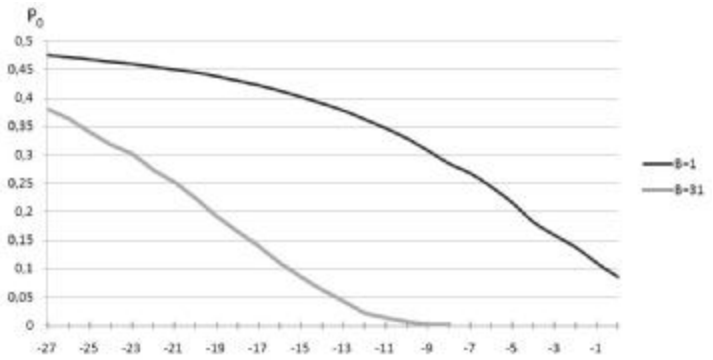

Рис. 2. Вероятность битовой ошибки когерентного приемника ФМ ШПС при разном значении базы ШПС

Как следует из рис. 2, при В = 1 вероятность появления ошибки $0{,}1 \le P_{дем} \le 0{,}3$ обеспечивается при защищенности (-1÷-8) дБ. Использование шумоподобного сигнала с базой В = 31 обеспечивает то же значение вероятности появления ошибки при защищенности (-16÷-23) дБ или, что то же самое, позволяет уменьшить уровень сигнала на входе приемника на 15 дБ.

Положим, что маскирующие свойства сигнала достигаются при защищенности -3 дБ, а уровень шума в месте стоянки равен некоторому значению *Рш*. Тогда из (3) по известному значению измеренного уровня шума можно найти максимально допустимое затухание тракта и оптимальное значение расстояния, при котором будет выполнено условие скрытности сигналов «блокировка-разблокировка» доступа. При $\Delta P = -15 дБ$ $P_{пм} = P_{ш} - 15$, $P_{пм} = P_{пд} - a$, а отсюда при $P_{пд} = 10 дБ$

$$a = 25 - P_{ш}. \qquad (5)$$

По формулам (2) и (5) выполнен расчет оптимального значения расстояния $r_м$ в зависимости от измеренного значения уровня шума в окружающей среде (*Рш*). Расчетные данные сведены в табл. 1.

Таблица 1

Зависимость оптимального расстояния от уровня шума в окружающей среде

r (м)	1000	100	50	25	10	1
a (дБ)	106	86	60	54	46	26
Рш (дБ)	-81	-61	-35	-29	-21	-1

Из табл. 1 следует, что базовая станция должна содержать генератор маскирующего шума с возможностью генерации шума с предельным значением уровня *Pmax* = -1 дБ и регулировать его значение в пределах 80 дБ.

Определим метод защиты данных от ошибок и скорость передачи данных в радиотракте.

Учтем, что при приеме ключевой последовательности вероятность ошибки будет лежать в пределах $0{,}1 \le P_{дем} \le 0{,}3$, а число ошибочных бит в блоке из 120 бит в среднем будет лежать в пределах $12 \le n_{ош} \le 36$, что приводит к необходимости их исправления.

Исправление ошибок в кодовой комбинации возможно путем применения различных методов. Рассмотрим метод повышения помехоустойчивости [6], который предусматривает замену каждого бита данных ПСП с «хорошей» АКФ (прямой – при передаче «нуля» и инверсной – при передаче «единицы») длиной T = 2t+1, где t – кратность исправляемой ошибки. Выберем значение t = 40. Тогда T = 2t + 1 = 81. Произведем замену каждого бита данных на последовательность длины 81. С учетом базы ШПС B = 31 и замены каждого бита данных последовательностью из 81 бита, скорость передачи данных в радиотракте составит $B_{pm} = B_0BT = 12 \cdot 10^3 \cdot 31 \cdot 81 = 30{,}132$ Мбит/с.

Увеличение числа исправляемых ошибок с 36 до 40 обусловлено тем, что момент нажатия кнопки брелока совсем не обязательно происходит на оптимальном расстоянии от злоумышленника. Наиболее опасным, с точки зрения скрытия факта блокировки доступа, является подача команды блокировки на небольшом удалении от злоумышленника. В этом случае затухание в тракте передачи сигнала является небольшим и, следовательно, защищенность сигнала в точке его перехвата может быть относительно велика. Вероятность битовой ошибки становится минимальной, а сама кодовая последовательность является достоверной и наиболее подходящей для криптоанализа.

Эта проблема может быть решена, если в кодовую последовательность преднамеренно внести ошибку. Кратность исправляемой ошибки t = 40 обеспечивает возможность внесения четырехкратной ошибки в передаваемую кодовую последовательность непосредственно в брелоке. Для этого процессор базовой станции выбирает две сеансовые ключевые последовательности и несколько векторов ошибки. Вектор ошибки имеет ту же размерность, что и кодовый вектор. Вектор, передающийся по радиоканалу, образуется побитным суммированием по модулю два кодового вектора и вектора ошибки.

В случае нажатия кнопки «блокировка/разблокировка» на удалении, большем граничного, число ошибок в кодовой последовательности может превысить допустимое значение t = 40. Вследствие этого команда может быть не исполнена, что потребует повторного нажатия кнопки. В этом случае меняется вектор ошибки, что приводит к изменению комбинации в целом, исключая возможность перехвата кодовой комбинации в «чистом» виде.

Определим, каким образом могут быть получены кодовые последовательности, обладающие требуемыми свойствами. Как показано в работе [7], такими последовательностями могут быть стохастические последовательности, построенные на основе линейных конгруэнтных генераторов. Путем конкатенации всех циклов графа и изменения порядка обхода вершин графа в каждом цикле достигается создание равномерно распределенной некоррелированной последовательности чисел с очень большим периодом повторения. В частности, при мощности графа $M = 2^{16}$ и конструкции графа Г = 8x8192 период повторения случайной последовательности может достигать $T = 3{,}4 \cdot 10^{28512}$. Если криптоаналитик способен перебирать 10^{18} слов/с, то криптоанализ методом грубой силы займет не более 10^{28287} лет, что вполне удовлетворяет требованиям поставленной задачи и позволяет сделать вывод о том, что поставленная задача может быть решена предложенным способом.

Выводы. Проведенное исследование показывает, что решением поставленной задачи является комплекс мер, включающий:

– выбор асимметричной ключевой системы;

– передачу сигналов «блокировка/разблокировка» ниже уровня шума на 3 дБ;

– преднамеренное введение в ключевую последовательность вектора ошибки с весом Хэмминга, равным четырем.

Показано, что для обеспечения криптостойкости системы в течение не менее 10 лет при взломе ключа методом грубой силы разрядность ключа должна составлять не менее 120 бит. Такая размерность ключа обусловлена тем, что не все ключи допускаются к использованию из-за особенностей применяемого ме-

тода, а также учитывая тот факт, что ключи блокировки и разблокировки следует выбрать для миллионной группировки автомобилей.

Как показало имитационное моделирование в системе «MATLAB», применение шумоподобных сигналов позволяет уменьшить уровень сигнала относительно шума с целью маскировки факта передачи команды с брелока.

Предложено использовать операцию преднамеренного искажения кодовой последовательности, которая выполняется путем наложения на нее вектора шума, что создает дополнительные трудности для криптоанализа в случае перехвата противником передаваемой ключевой информации.

Таким образом, решенная задача повышения стойкости электронных кодовых замков обеспечивает возможность создания нового типа криптографически стойкой системы защиты электронных кодовых замков от «взлома».

Список литературы

1. Виноградов Ю. А. Электронная охрана (элементы и узлы охранных систем) / Ю. А. Виноградов – М.: Символ-Р, 1996. – 96 с.
2. Андрианов В. И. Охранные устройства для автомобилей / В. И. Андрианов, А. В. Соколов. – СПб.: Лань, 1997. – 320 с.
3. Андрианов В. И. «Шпионские штучки» и устройства для защиты объектов и информации / В. И. Андрианов, В. А. Бородин, А. В. Соколов. – СПб.: Лань, 1996. – 272 с. – (Справочное пособие).
4. Лисицына Е. С. Разделение векторной смеси сигнала и помехи по методу максимального правдоподобия / Е. С. Лисицына, В. В. Швыдкий, А. И. Щерба, Э. В. Фауре // Системи обробки інформації. – 2010. – № 8 (89). – С. 62–67.
5. Грудинская Г. П. Распространение радиоволн / Г. П. Грудинская – М. : Высшая школа, 1967. – 244 с.
6. Пат. 60633 Україна, МПК H04L 1/20. Спосіб вилучення сигналу даних, що міститься в модульованому по фазі шумоподібному сигналі, з підвищеною вірогідністю / Швидкий В. В., Лісіцина О. С., Лега Ю. Г., Щерба А. І.; заявник та патентовласник ЧДТУ. – №u201014204; заявл. 29.11.2010; опубл. 25.06.2011, Бюл. №12.
7. Береза А. С. Генерация конгруэнтных последовательностей чисел с заданными свойствами / А. С. Береза, А. А. Лавданский, В. В. Швыдкий, Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2012. – № 2. – С. 3–8.

References

1. Vinogradov, Y. A. (1996) Electronnaia ohrana (elementy i uzly ohrannyh sistem). Moskva: Simvol-P, 96 p. [in Russian]
2. Andrianov, V. I. and Sokolov, A. V. (1997) Ohrannye ustroistva dlia avtomobilei. St. Peterburg: Lan, 320 p. [in Russian]
3. Andrianov, V. I., Borodin, V. A. and Sokolov, A. V. (1996) "Shpionskie shtuchki" i ustroistva dlia zashchity objektov i informacii. St. Peterburg: Lan, 272 p. Spravochnoe posobie. [in Russian]
4. Lisitsyna, E. S., Shvydkyi, V. V., Scherba, A. I. and Faure, E. V. (2010) Razdelenie vektornoy smesi signala i pomehi po methodu maksimalnoho pravdopodobiya. *Systemy Obrobky Informacii*, 8 (89), pp. 62–67. [in Russian]
5. Grudinskaya, G. P. (1967) Rasprostranenie radiovoln. Moskva: Visshaya Shkola, 244 p. [in Russian]
6. Pat. 60633 Ukraine. The method of removal of data signal, which is included in phase-modulated noise-type signal, with enhanced probability. Shvydkyi, V. V., Lisitsyna, O. S., Leha, Yu. H., and Scherba, A. I. Cherkasy state technological university, assignee. № 201012464; appl. 29.11.2010; publ. 25.06.2011, Bulletin №12. [in Ukrainian].
7. Bereza, A. S., Lavdanskii, A. A., Shvydkyi, V. V. and Faure, E. V. (2012) Generaciya kongruentnyh posledovatelnostei chisel s zadannymi svoistvami. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitety,* (2), pp. 3–8. [in Russian]