УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2019 Том 19 № 2 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2019 Vol. 19 No 2 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 658.5.011.56; 621.395.44; 621.391.037.372

ЗАЩИТА КАНАЛА ШИРОКОПОЛОСНОЙ СВЯЗИ С ПРИМЕНЕНИЕМ ОРТОГОНАЛЬНЫХ ШУМОПОДОБНЫХ СИГНАЛЬНЫХ СИМВОЛОВ

А.Ю. Гришенцев[a], С.А. Арустамов[a], А.Г. Коробейников[a,b], О.В. Козин[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской академии наук, Санкт-Петербург, 199034, Российская Федерация
Адрес для переписки: Grishentcev@yandex.ru

Информация о статье
Поступила в редакцию 16.11.18, принята к печати 14.01.19
doi: 10.17586/2226-1494-2019-19-2-280-291
Язык статьи – русский

Ссылка для цитирования: Гришенцев А.Ю., Арустамов С.А., Коробейников А.Г., Козин О.В. Защита канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 2. С. 280–291. doi: 10.17586/2226-1494-2019-19-2-280-291

Аннотация

Предложено решение частной задачи комплексной защиты радиоканала, в котором осуществляется обмен радиосообщениями на базе взаимно ортогональных сигнальных широкополосных символов и алфавитов на их основе. Объект исследования – метод организации защищенного канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов. В качестве сигнальных широкополосных символов использовались символы, синтезированные в частотной области на базе псевдослучайных последовательностей с последующей ортогонализацией методом Грама–Шмидта трансформации в заранее определенные спектральные компоненты сигнальных символов, а также преобразованием во временную область с помощью обратного быстрого преобразования Фурье. Предложен метод, основанный на использовании комплексной скрытности: информационной, структурной и энергетической. Информационная скрытность реализуется за счет однократного использования символов из некоторого множества алфавитов. Структурная скрытность реализуется за счет фильтрации сигнальных сообщений в области склейки сигнальных символов, что осложняет определение длительности отдельных сигнальных символов и разделение сообщения на отдельные сигнальные символы, а следовательно, затрудняет декодирование всего сообщения. Энергетическая скрытность реализуется за счет сокрытия радиосигнала в шумах радиоэфира. Практическая значимость работы заключается в возможности повышения защиты широкополосных каналов связи на основании предлагаемого авторским коллективом метода.

Ключевые слова

защита информации, широкополосная связь, стеганография, ортогональные сигнальные символы, радиокриптография, радиостеганография, радиоэлектронная борьба

ORTHOGONAL NOISE-LIKE SIGNAL SYMBOLS FOR BROADBAND CHANNEL PROTECTION

A.Yu. Grishentsev[a], S.A. Arustamov[a], A.G. Korobeynikov[a,b], O.V. Kozin[a]

[a]ITMO University, Saint Petersburg, 197101, Russian Federation
[b]Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation Russian Academy of Sciences St. Petersburg Filial, Saint Petersburg, 199034, Russian Federation
Corresponding author: Grishentcev@yandex.ru

Article info
Received 16.11.18, accepted 14.01.19
doi: 10.17586/2226-1494-2019-19-2-280-291
Article in Russian

For citation: Grishentsev A.Yu., Arustamov S.A., Korobeynikov A.G., Kozin O.V. Orthogonal noise-like signal symbols for broadband channel protection. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 2, pp. 280–291 (in Russian). doi: 10.17586/2226-1494-2019-19-2-280-291

Abstract

The paper deals with development and analysis of particular case in a complex protection for a channel where radio messages are exchanged on the basis of mutually orthogonal signal broadband characters and alphabets based on them. The object of

study is a method of secure broadband channel organization using orthogonal noise-like signal symbols. The signal broadband symbols have been synthesized in the frequency domain based on pseudo-random sequences with the subsequent orthogonalization by the Gram-Schmidt method of transformation into pre-defined spectral components of the signal symbols and subsequent transformation into the time domain with the aid of the inverse fast Fourier transform. We have proposed to deploy and explore the complex secrecy approach comprising information, structural and energy secrecies. Information secrecy is brought into action with a single use of symbols retrieved out of a certain set of alphabets. Structural secrecy is reached by deployment of signal messages filtering in the area of signal symbols merge that makes difficult to determine the duration of individual signal symbols and message separation in individual signal symbols. Therefore, the decoding of entire message becomes more difficult. Energy secrecy is ensured by hiding the radio signal in the radio noise. We have carried out modeling and analysis of information, structural and energy secrecy. Practical importance of the work lies in increasing the level of protection for broadband communication channels based of the method we proposed. The conclusions have been set up in final part of the paper.

Keywords
information security, broadband communication, orthogonal signal symbols, radio-encryption, radio-stenography, radio-electronic countering

Введение

Современные системы телекоммуникаций должны обладать следующими атрибутами информационной безопасности: конфиденциальность, целостность и доступность. Системам беспроводной связи могут угрожать перехват информации, ее искажение (например, вследствие передачи неполных, искаженных или поддельных сообщений), нарушение доступности (например, с помощью постановки заградительной радиопомехи) [1, 2]. Существует достаточно много методов защиты передаваемой по радиоканалам информации, которые в общем можно разделить на: радиокриптографические (основаны на криптографическом шифровании передаваемых радиосообщений) и радиостеганографические (основаны на сокрытии самого факта передачи радиосообщений [3]). Наиболее защищены системы, использующие комплексные методы защиты, которые позволяют скрыть факт передачи сообщений и зашифровать передаваемую информацию [4–6].

В [7] представлена классификационная модель методов радиокриптостеганографии, основанных на энергетической, структурной, информационной, временной и пространственной скрытности.

В настоящей работе предложено комплексное криптостеганографическое решение частной задачи защиты информации, передаваемой по широкополосным радиоканалам с помощью алфавитов, образованных взаимно ортогональными сигнальными широкополосными символами (СШС). Предлагаемое решение позволяет обеспечивать информационно-структурно-энергетическую скрытность, с элементами криптографии на основе когерентных генераторов псевдослучайных чисел, расположенных на принимающей и передающих сторонах канала связи.

Цель исследований: разработка и анализ метода комплексной криптостеганографической системы широкополосной связи с применением взаимно ортогональных сигнальных широкополосных символов.

Концепция построения защищенных широкополосных радиоканалов

В [8–10] предложен метод СШС и алфавитов на их основе. Метод синтеза отдельного СШС основан на заполнении заранее определенной части спектра $X\left[\omega_R\right]$ случайными числами с равномерным распределением, остальная часть спектра задается равной нулю $X\left[\omega_0\right]=0$, полученные части спектра объединяются в полный спектр $X\left[\omega\right]=X\left[\omega_0\right]\cup X\left[\omega_R\right]$ отдельного СШС, затем производится обратное преобразование Фурье $\mathcal{F}^{-1}\left\{X\left[\omega\right]\right\}$ полученного спектра, в результате которого синтезируется ненормированный СШС $\hat{x}[t]$, при этом $\omega_R\in\left[-W_u;-W_l\right]\cup\left[W_l;W_u\right]$ и $\omega_0\notin\left[-W_u;-W_l\right]\cup\left[W_l;W_u\right]$, где $\left[-W_u;-W_l\right]$ – отрицательная составляющая спектра Фурье; $\left[W_l;W_u\right]$ – положительная составляющая спектра Фурье; W_l и W_u – нижняя и верхняя границы спектра.

Формально метод синтеза отдельных СШС [8] возможно описать отношениями:

$$\left.\begin{array}{l}X\left[\omega_R\right]=\text{rand}()\\X\left[\omega_0\right]=0\end{array}\right\}\Rightarrow X\left[\omega\right]=X\left[\omega_0\right]\cup X\left[\omega_R\right]\Rightarrow\ \mathcal{F}^{-1}\left\{X\left[\omega\right]\right\}=\hat{x}[t].$$

Нормирование $\hat{x}[t]$ возможно выполнить путем деления на длину вектора сигнала:

$$x[t]=\frac{1}{\sqrt{\int_{-T/2}^{T/2}\hat{x}[t]^2\,dt}}\hat{x}[t],$$

где T – длительность СШС. Дискретные СШС будем обозначать $x[n]$.

Метод синтеза ансамблей ортогональных СШС [8] является развитием метода синтеза отдельных СШС. Метод основан на генерации псевдослучайных N-мерных векторов их ортогонализации методом Грама–Шмидта, последующей трансформации полученных ортонормированных векторов, по заранее определенным правилам, в соответствующие частотные спектры, которые являются образами искомых ортонормированных широкополосных сигналов в частотном пространстве. Окончательный результат синтеза получается в ходе обратного преобразования Фурье и нормирования отдельных сигналов. Полученные алфавиты ортогональных СШС обладают хорошими корреляционными свойствами [8, 9] и могут быть применены в системах связи, требующих устойчивого распознавания сигнальных сообщений при весьма малых значениях отношения сигнала к шуму [10]. Синтезированные разработанным методом СШС имеют шумоподобный характер в частотной и во временной областях.

В [9] показано, что максимальная мощность алфавита $\mathbf{A}$, т.е. максимальное число взаимно ортогональных СШС, не превышает числа отсчетов N дискретной формы СШС $x[n]$, уменьшенного на единицу, т.е. $\max(|\mathbf{A}|) = N-1$, из-за отсутствия в ортонормированном базисе, образованном СШС, постоянной составляющей, так как частотная составляющая с нулевой частотой спектра СШС приравнивалась нулю при синтезе. Следовательно, базис, образованный $(N-1)$ СШС в N-мерном пространстве, является неполным. Удвоить мощность алфавита $\mathbf{A}$ возможно за счет использования противоположных сигналов. В [9] также показано, что быстродействие предлагаемого метода позволяет выполнять синтез алфавитов СШС в масштабе реального времени со скоростью, обеспечивающей непрерывную работу передающего устройства.

Благодаря возможности синтеза СШС с $FT \gg 1$ (F – занимаемый диапазон частот) можно распределять энергию СШС в пространстве частота–время и эффективно скрывать его в шумах радиоэфира.

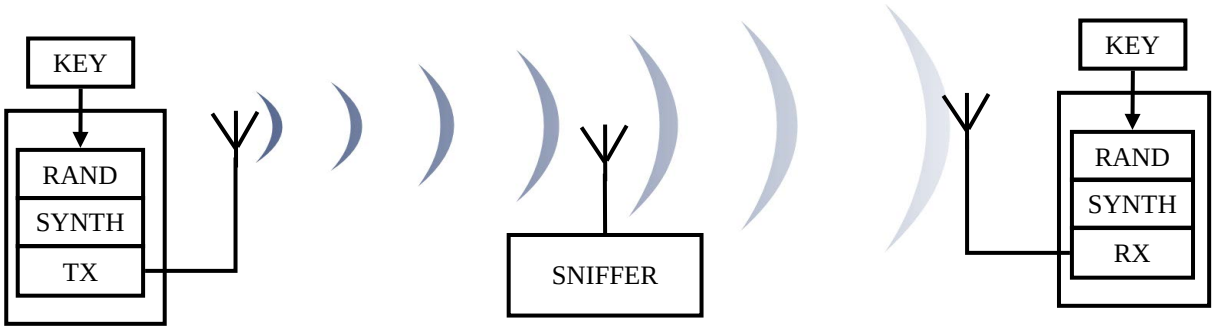


Рис. 1. Обобщенная блок-схема организации защищенного канала связи

В блок-схеме (рис. 1) модели организации защищенного канала связи передатчик TX и приемник RX располагают общим ключом KEY, который позволяет выполнять согласованную (когерентную) генерацию псевдослучайных чисел по одинаковым алгоритмам RAND. Полученные псевдослучайные числа используются для определения частотного спектра СШС с последующей трансформацией, в модуле SYNTH, во временную область (SNIFFER – злоумышленник, вероятностно реализующий различные угрозы радиоэлектронной борьбы).

Синтезированный алфавит $\mathbf{A}$ используется для передачи сообщений таким образом, чтобы повторы СШС при передаче были исключены. По исчерпанию символов в алфавите $\mathbf{A}$, т.е. когда требуется повторная передача некоторого СШС, синтезируется новый алфавит, и передача сообщений продолжается без повтора СШС, таким образом обеспечивается информационная скрытность. Ключи KEY могут распространяться с помощью таблиц, которыми абоненты обеспечиваются заранее, или с помощью других каналов связи. Структурная скрытность сообщений обеспечивается за счет того, что СШС образуют единый поток, в котором, не зная параметров передачи, сложно определить, где заканчивается один СШС и начинается другой. За счет распределения СШС в пространстве частота–время FT энергия сообщений скрывается в шумах радиоэфира, обеспечивая энергетическую скрытность.

Информационная скрытность и метод ее реализации

Пусть имеется неограниченное множество алфавитов $\mathbf{B} = \{\mathbf{A}_0, \mathbf{A}_1, \ldots\}$, мощность каждого K, каждый алфавит $\mathbf{A}_m \in \mathbf{B}$ образован взаимно ортогональными элементами (СШС) $x_k^{A_m}[n]$ ($k = 0 \ldots K-1$), синтезированными в результате обратного преобразования Фурье дискретного спектра $\mathcal{F}^{-1}\{X_k^{A_m}[n]\}$. Этот дискретный спектр получен в результате трансформации по заданному закону взаимно

ортогональных нормированных векторов $r_q^{A_m}[k], q = 0 \ldots K$, полученных в результате ортогонализации методом Грамма–Шмидта векторов $\rho_q^{A_m}[k]$. Последние образованы набором случайных чисел в результате работы генератора псевдослучайных чисел $\mathrm{rand}(\mathrm{KEY})$ с ключом-параметром KEY по равномерному закону распределения [8, 9].

Разделим каждый алфавит $\mathbf{A}_m \in \mathbf{B}$ по заранее определенному правилу на подмножества $\mathbf{T}_m$ и $\mathbf{S}_m$ так, что $\mathbf{A}_m = \mathbf{T}_m \cup \mathbf{S}_m$. Символы из $\mathbf{T}_m$ будем использовать для передачи, а из $\mathbf{S}_m$ – для пополнения множества $\mathbf{T}_m$, таким образом, чтобы передача одинаковых СШС была исключена. Мощность $\mathbf{T}_m$ определяет количество переносимой информации каждым символом из $\mathbf{T}_m$ как $\log(\mathbf{T}_m)$. Предельным случаем, с одной стороны, является отделение множества $\mathbf{T}_m$ из двух символов, тогда все остальные символы из алфавита $\mathbf{A}_m$, возможно использовать во множестве $\mathbf{S}_m$, при этом возможно передавать $K-1$ символов, каждый из которых будет нести бинарную информацию. Другим предельным является случай, когда все символы алфавита $\mathbf{A}_m$ принадлежат множеству $\mathbf{T}_m$, при этом $\mathbf{S}_m = \varnothing$ – пустое множество, что гарантирует возможность передать один символ, переносящий $\log K$ бит информации. На практике выбор принципа разделения алфавита $\mathbf{A}_m$ на $\mathbf{T}_m$ и $\mathbf{S}_m$ возможно определить двумя критериями:

1) за время передачи символов из алфавита $\mathbf{A}_m$ передающая система должна успевать синтезировать следующий алфавит $\mathbf{A}_{m+1}$;
2) принимающая система, использующая некоторый метод распознавания СШС, например, корреляционный метод, должна успеть обрабатывать за время передачи одного СШС все возможные варианты из множества $\mathbf{T}_m$.

В общем случае число потенциально передаваемых СШС без повторов из одного алфавита $\mathbf{A}_m = \mathbf{T}_m \cup \mathbf{S}_m$ возможно рассчитать как $L = |\mathbf{T}_m| + 1$.

В качестве примера рассмотрим разделение алфавита $\mathbf{A}_m$ на две равные части $\mathbf{T}_m$ и $\mathbf{S}_m$, а при исчерпании $\mathbf{A}_m$ станем использовать следующий алфавит. Вполне очевидно, что равные части $\mathbf{T}_m$ и $\mathbf{S}_m$ обеспечивают максимально возможное число отправленных символов без повторов K, а минимальное $K/2+1$. С целью гарантированного исключения повторов будем использовать каждый алфавит $\mathbf{A}_m$ для передачи не более $K/2+1$ СШС. Назовем посылку $K/2+1$ СШС из одного алфавита *серией*. Таким образом, гарантировано отсутствие повторов СШС в объеме передачи каждой серии. Использование символов в серии из одного алфавита $\mathbf{A}_m$ гарантирует, что минимальная межсимвольная дистанция будет соответствовать минимальной межсимвольной дистанции алфавита $\mathbf{A}_m$. Отметим, что взаимно ортогональные символы эквидистантны.

Рассмотрим пример. Пусть имеется алфавит $\mathbf{A}$ из восьми символов $\{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$, разделим его на два подмножества $\mathbf{T} = \{x_0, x_1, x_2, x_3\}$ и $\mathbf{S} = \{x_4, x_5, x_6, x_7\}$. Элементы $\mathbf{T}$ используются для передачи и ассоциированы с бинарным кодом $\{00, 01, 10, 11\}$. Пусть передан символ x_1, обозначим как $\mathrm{TX}(x_1)$, тогда множество $\mathbf{T}$ пополняется СШС из $\mathbf{S}$ по заранее определенному правилу, пусть для пополнения используется СШС с младшим номером, в данном случае – x_4. Таким образом, можно осуществить до пяти посылок и при этом сохранять мощность $\mathbf{T}$ за счет пополнения из $\mathbf{S}$ (рис. 2).

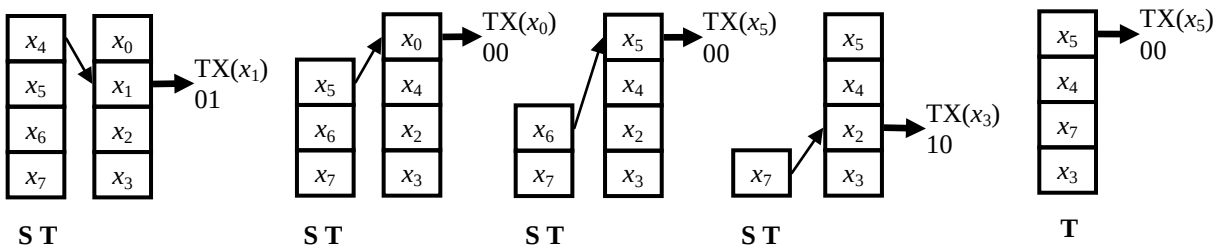


Рис. 2. Последовательность посылок и пополнения множества $\mathbf{T}$ из $\mathbf{S}$

Принимающая сторона RX должна знать не только ключ KEY генерации псевдослучайных чисел и правила синтеза СШС, но и порядок разделения множества $\mathbf{A}_m$ на $\mathbf{T}_m$ и $\mathbf{S}_m$, и правила пополнения

множества $\mathbf{T}_m$ из $\mathbf{S}_m$, а также правила объединения алфавитов во множество $\mathbf{B} = \{\mathbf{A}_0, \mathbf{A}_1, \ldots\}$.

Если принимающая сторона RX распознает символ ошибочно или не распознает вовсе, то будет искажена вся часть серии посылки от ошибочно распознанного символа до конечного, так как на принимающей стороне будет утеряна информация о последовательности выполнения операции пополнения множества $\mathbf{T}_m$ из $\mathbf{S}_m$. Зная длину серии $K/2+1$, принимающая сторона RX сможет возобновить корректный прием со следующей серии. Для более оперативного восстановления связи и повышения вероятности безошибочного приема возможно использовать интеграцию методов исправления ошибок в протокол передачи радиосообщений.

Оценка вероятности повторов сигнальных символов при информационной скрытности

Оценим вероятность повтора символов в сеансе связи. Будем рассматривать случай, когда $K = \max(|\mathbf{A}|) = N-1$, при котором повтор СШС наиболее вероятен. Как было отмечено ранее, базис, образованный $N-1$ СШС в *N*-мерном пространстве является неполным, при этом в пространстве, из которого синтезированы СШС, является полным. При унитарном линейном преобразовании Фурье сохраняется евклидова дистанция, а следовательно, возможно записать выражение для сохранения евклидовой метрики L_2 в различных пространствах:

$$d_E = \sqrt{\sum_{k=0}^{K-1}\left(r_q[k]-r_v[k]\right)^2} = \sqrt{\sum_{f=0}^{N-1}\left(X_q[f]-X_v[f]\right)^2} = \sqrt{\sum_{n=0}^{N-1}\left(x_q[n]-x_v[n]\right)^2},$$

где $q, v \in (0,1,\ldots K-1)$; $r_q[k]$ и $r_v[k]$ – векторы, синтезированные по псевдослучайному закону, из которых образуются спектры СШС. Таким образом, для анализа вероятности повторов $x_k^{A_m}[n]$ СШС возможно исследовать вероятность повторов векторов $r_q^{A_m}[k]$, $q = 0 \ldots K-1$.

Пусть синтезировано K ортогональных СШС в *N*-мерном пространстве, определенном значениями области возможно ненулевого спектра $\omega_R \in [-W_u; -W_l] \cup [W_l; W_u]$. Примем, что при синтезе СШС в дискретной целочисленной форме число возможных значений (уровней дискретизации) каждого отсчета ненулевого спектра СШС $\omega_R \in [-W_u; -W_l] \cup [W_l; W_u]$ будет определяться величиной $D = \left[-\frac{a}{2}; \frac{a}{2}\right]$, и все СШС будут нормированы, т.е. из всех возможных значений радиуса вектора СШС будет использован только единичный. В этом случае число возможных вариантов отдельно взятого СШС будет принадлежать множеству значений с мощностью: $\frac{2D^K}{D} = 2D^{K-1}$.

Рассмотрим пример (рис. 3) расположения взаимно ортогональных образов $r_0[k], r_1[k], r_2[k]$ в трехмерном пространстве. Вполне очевидно, что нормированные сигналы, а также их спектры могут принадлежать только определенному слою в окрестностях единичного радиуса, слой имеет ненулевую толщину, поскольку сигналы и их спектр дискретны. При бесконечно малом шаге дискретизации слой имеет форму сферы и стремящуюся к нулю толщину. При увеличении шага дискретизации сферический слой устремляется к октаэдру через различные формы многогранников.

Решение задачи о совпадении сигналов в *N*-мерном пространстве при использовании в качестве критерия евклидовой метрики $d_E = \sqrt{\sum_{k=0}^{K-1}\left(r_q[k]-r_v[k]\right)^2}$ в общем виде возможно свести к задаче об упаковке кристаллической решетки на *K*-мерной сфере, что выходит даже за пределы трехмерной *проблемы Томсона* [11], в общем виде пока нерешенной.

Поэтому для оценки вероятности совпадения воспользуемся другим подходом. Будем считать, что сигналы совпали, если совпали все их отсчеты. Не совпадающие, но максимально близкие СШС будут находиться на евклидовом расстоянии $d_E^{\min}$, причем $d_E^{\min} \neq 0$, при равномерном шаге сетки дискретизации D будет $d_E^{\min} = \frac{a}{D}$.

Таким образом, задача оценки вероятности повтора СШС сводится к задаче Томсона в предельном случае, для максимально плотной упаковки шаров на поверхности сферы в дискретном *N*-мерном пространстве.

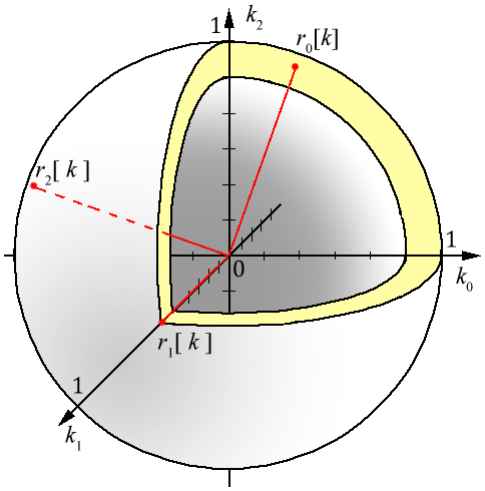


Рис. 3. Расположение взаимно ортогональных частотных образов $r_0[k], r_1[k], r_2[k]$ в трехмерном пространстве

Если рассматривать только не противоположные сигналы, т.е. половину $(K-1)$-мерной поверхности гиперсферы, образованной множеством векторов СШС в *N*-мерном пространстве, область возможных значений СШС сократится в два раза, т.е. D^{K-1}. Теперь, в заданной формулировке, оценка вероятности совпадения СШС относится к задачам теории вероятности и математической статистики «парадокс Борель–Колмогорова» [12] и криптографической «парадокс совпадения дней рождения» [13, 14]. Используя решение задачи «парадокс совпадения дней рождения», можно записать выражение для оценки совпадения хотя бы двух СШС при посылке M серий, каждая из которых образована алфавитом $\mathbf{A}_m$ мощностью K, при этом следует учесть, что в передаче участвует только часть символов $L < K$. Вероятность совпадения СШС при посылке L символов в M сериях и возможном числе вариантов несовпадающих СШС D^{K-1} оценим как: $p_{\text{rep}}(L,M,D,K) = 1 - \dfrac{\left(D^{K-1}\right)!}{\left(D^{K-1}\right)^{ML}\left(D^{K-1}-ML\right)!}$ или с помощью упрощенной формулы $p_{\text{rep}}(L,M,D,K) \approx 1 - e^{-\frac{ML(ML-1)}{2D^{K-1}}}$. Таким образом, для достаточно больших величин ML, когда $ML(ML-1) \approx (ML)^2$, можно оценить, при каком числе отправленных СШС хотя бы два повторятся с заданной вероятностью p_{rep}: $ML < \sqrt{\left|2D^{K-1}\ln\left(1-p_{\text{rep}}\right)\right|}$.

Следует отметить, что на практике не требуется полного совпадения СШС, достаточно их некоторой близости с точки зрения евклидовой метрики для сходства. В этом случае вероятностный анализ близости символов переходит в конвергентный класс «проблемы Томсона» [11, 15] в *N*-мерном пространстве и «парадокса Борель–Колмогорова», рассмотрение, и тем более решение, которых выходит за рамки работы.

Также отметим, что даже абсолютно сходные СШС могут соответствовать различной бинарной информации. Следовательно, наличие одинаковых СШС в сеансе связи может способствовать нарушению информационной скрытности. Для преодоления информационной скрытности злоумышленнику необходимо знать и уметь повторить: закон генерации псевдослучайных чисел и его ключ KEY, а также закон трансформации векторов $r_q[k]$ в спектральные образы СШС $X_k^{A_m}[n]$, закон разделения алфавитов $\mathbf{A}_m = \mathbf{T}_m \cup \mathbf{S}_m$.

Пусть вероятность совпадения СШС $p_{\text{rep}} = 0,0001$, мощность алфавитов $K = 16$, число уровней дискретизации $D = 1024$, $ML < \sqrt{\left|2D^{K-1}\ln\left(1-p_{rep}\right)\right|} = \sqrt{2\cdot 1024^{15}\ln(1-0,0001)} \approx 5,3\cdot 10^{20}$. При $L = \left(\dfrac{K}{2}\right)+1$ переданных из каждого алфавита СШС получим число серий $M \approx 5,9\cdot 10^{19}$ без полных повторений СШС с вероятностью $p_{\text{rep}} = 0,0001$.

При обнаружении факта передачи сообщения и доступности сообщения (или его части) для последующей обработки с целью нейтрализации информационной скрытности злоумышленнику

необходимо осуществить перебор возможных вариантов формирования сообщений без повторов СШС. В случае предлагаемой модели формирования серий сообщений (рис. 2) число размещений из K элементов по $K/2$ возможно оценить как $\frac{K!}{\left(\frac{K}{2}\right)!}$. Если в каждой серии использовать свой уникальный метод формирования сообщений, то сложность нейтрализации информационной скрытности значительно возрастет.

Весь сеанс связи осуществляется передача не повторяющихся (с высокой вероятностью) СШС. Каждый новый сеанс связи передача осуществляется вновь синтезированными алфавитами на основе новых СШС. Так обеспечивается информационная скрытность в канале связи.

Как известно, криптографические алгоритмы оцениваются временной (или вычислительной) сложностью – *криптостойкостью*, к наиболее эффективной криптоатаке, нарушающей безопасность. Вычислительная сложность задается асимптотически, с помощью показателя степени двойки. Приведем показатели криптостойкости (вычислительную сложность) некоторых известных алгоритмов [16–18] (см. таблицу, L_{μ} и N_{μ} – длина открытого и закрытого ключа; R_{μ} – число раундов).

Таблица. Криптостойкость алгоритмов шифрования

Алгоритм	Параметр	Криптостойкость
3TDEA [16]	$L_{\mu}=2048;\ N_{\mu}=224$	2^{112}
AES-256 [16]	$L_{\mu}=15360;\ N_{\mu}=512$	2^{256}
ГОСТ 28147-89[1], [17, 18]	$N_{\mu}=256;\ R_{\mu}=32$	$2^{43}\ldots2^{224}$
Предлагаемый	$K=16$	2^{8}
	$K=32$	2^{73}

Сравнение с известными методами криптографии показывает достаточно высокий уровень криптостойкости предлагаемого метода информационной скрытости, при этом его использование не исключает совместного применения традиционных криптографических методов.

Структурная скрытность и метод ее реализации

В качестве дополнительных средств повышения защищенности канала связи предлагается метод реализации структурной скрытности.

Структурную скрытность обеспечивают непрерывная склейка СШС, фильтрация в области сшивки и передача непрерывного потока, в котором при неизвестной длительности отдельных СШС затруднительно выявить структуру сообщения. В соответствии с методом синтеза отдельных СШС в частотной области спектр отдельных СШС определен и локализован. В точке склейки возникает область (*артефакт*) смены фазы и/или амплитуды (рис. 4, $x[n]$ – амплитуда в условных единицах, n – номер отсчета), непрерывный анализ и сбор статистики периодичности артефакта позволяет злоумышленнику оценить длительность СШС, следовательно, получить больше информации о канале связи и передаваемой информации.

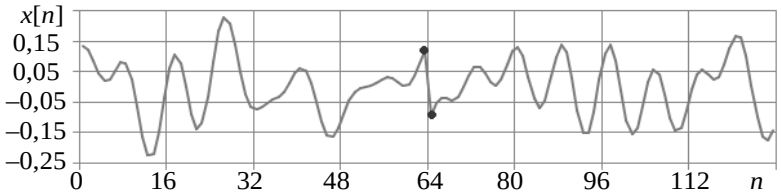


Рис. 4. Изменение фазы в области склейки сигналов,
смежные границы сигналов обозначены красными точками

Противодействовать обнаружению артефакта возможно с помощью фильтрации сообщения (образованного последовательностью СШС) в областях склейки или по всей протяженности. Фильтрацию в области склейки СШС возможно производить, например, с помощью сплайн-интерполяции (рис. 5) или фильтрации.

[1]ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 01.07.1993. М.: Изд-во стандартов, 1996. 32 с.

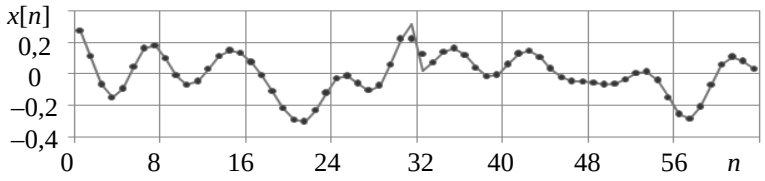


Рис. 5. Сплайн-интерполяция сообщения $x[n]$ в месте склейки СШС, сигнал обозначен сплошной кривой, интерполяция красными точками

Хорошие результаты фильтрации для гладкой сшивки смежных СШС показал предлагаемый метод фильтрации сообщений в окне в области склейки СШС (рис. 6).

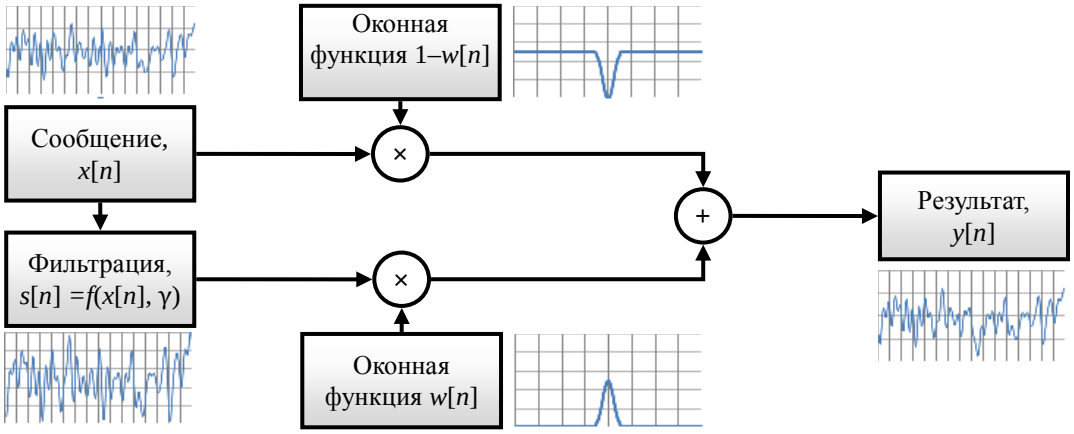


Рис. 6. Блок-схема фильтрации сообщений в окне в области склейки сигналов $x[n]$, умножение и сумма производятся поэлементно

Сообщение $x[n]$ фильтруется с помощью $s[n]=f\left(x[n],\gamma\right)$, с заданными параметрами γ, диапазон частот $[W_l;W_u]\sim[2\pi F_l;2\pi F_u]$ принимается за полосу пропускания. Далее результат фильтрации $s[n]$ поэлементно умножается на оконную функцию $w[n]$ с ненулевыми значениями в области склейки СШС, ширина области склейки (т.е. ширина оконной функции N_w) принимается исходя из удвоенного отношения числа отсчетов N в СШС, деленного на максимальную нормированную частоту F_u в спектре СШС $[2\pi F_l;2\pi F_u]$, измеренную в герцах при длительности СШС, принятой за 1 с (т.е. $T=1$). Исходное сообщение $x[n]$ поэлементно умножается на функцию $\left(1-w[n]\right)$. Затем результаты поэлементного умножения поэлементно складываются: $y[n]=s[n]\times w[n]+x[n]\times\left(1-w[n]\right)$.

При любом виде фильтрации каждый отдельный СШС $x_k^{A_m}[n]$ в составе сообщения $x[n]$ претерпевает изменения по краям (в области склеек), что сказывается на распознавании СШС на принимающей стороне.

Верхнюю границу изменения пика автокорреляционной функции (АКФ) в результате применения фильтрации возможно оценить следующим образом. При максимальной частоте в спектре СШС $F_u=N/2$ $\left(N_w=2\right)$ изменению не более чем на $0,5\max\left(\left|x[n]\right|\right)\approx 0,5\max\left(\left|x_k^{A_m}[n]\right|\right)$ подвергнется два отсчета, по одному с каждой стороны СШС, при $F_u=N/4$ $\left(N_w=4\right)$ изменению не более чем на $0,5\max\left(\left|x[n]\right|\right)$ подвергнется четыре отсчета и т.д. Величина пика АКФ соответствует $r_{\max}=\sum_{n=0}^{N-1}x_k^{A_m}[n]x_k^{A_m}[n]^*$, здесь $x_k^{A_m}[n]^*$ – СШС комплексно сопряженный к $x_k^{A_m}[n]$, при условии нормирования СШС получим $r_{\max}=1$. Оценить величину изменения $r_{\max}$ в результате фильтрации сообщения $x[n]$ в области склейки возможно с помощью выражения $\Delta r_{\max}\approx 0,5\sum_{n=0}^{N_w-1}w[n]\max\left(\left|x_k^{A_m}[n]\right|\right)^2$.

Вследствие шумоподобного характера СШС вклад каждого произведения $x_k^{A_m}[n]x_k^{A_m}[n]^*$ отсчетов

$x_k^{A_m}[n]$ в пиковое значение АКФ возможно оценить как $\approx \frac{r_{\max}}{N} = \frac{1}{N}$, поэтому среднее значение изменения пика АКФ в результате применения фильтрации можно оценить как $\Delta r_{\text{mean}} \approx \frac{0,5}{N} \sum_{n=0}^{N_w-1} w[n]$.

Так, например, принимая в качестве оконной функции окно Хемминга [19] при $N_w = 4$ и $N = 128$ получим величину оценки при фильтрации сообщений в окрестности склейки СШС среднего изменения пика АКФ $\Delta r_{\max} = 0,0066$, что составляет примерно $0,7$ % от $r_{\max}$.

Анализ различных методов показывает, что наилучшие результаты позволяет получить предложенный метод фильтрации сообщений в окне (рис. 6). На спектрограммах (рис. 7, *f* – частота; *k* – номер сигнального символа из алфавита) отображены результаты спектрального анализа сообщения без фильтрации (рис. 7, *а*) и с различными видами фильтрации в области склейки СШС (рис. 7, *б*–*г*).

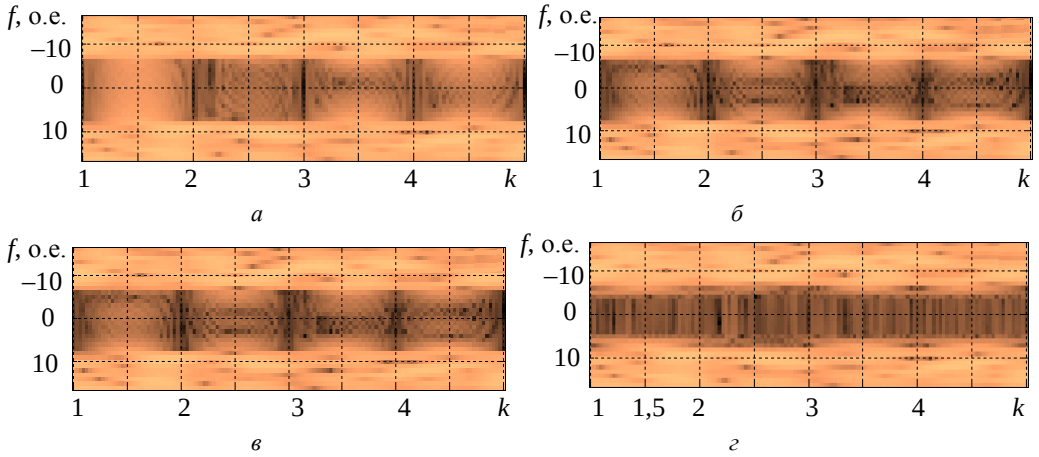


Рис. 7. Спектрограммы сообщений, образованных склейкой пяти СШС длиной 33 отсчета. Приведены логарифмы амплитуды спектра: *а* – без фильтрации; *б* – фильтрация скользящего среднего в окне 8 отсчетов; *в* – сплайн-фильтрация в окне 8 отсчетов; *г* – фильтрация в окне 8 отсчетов (окно Хемминга)

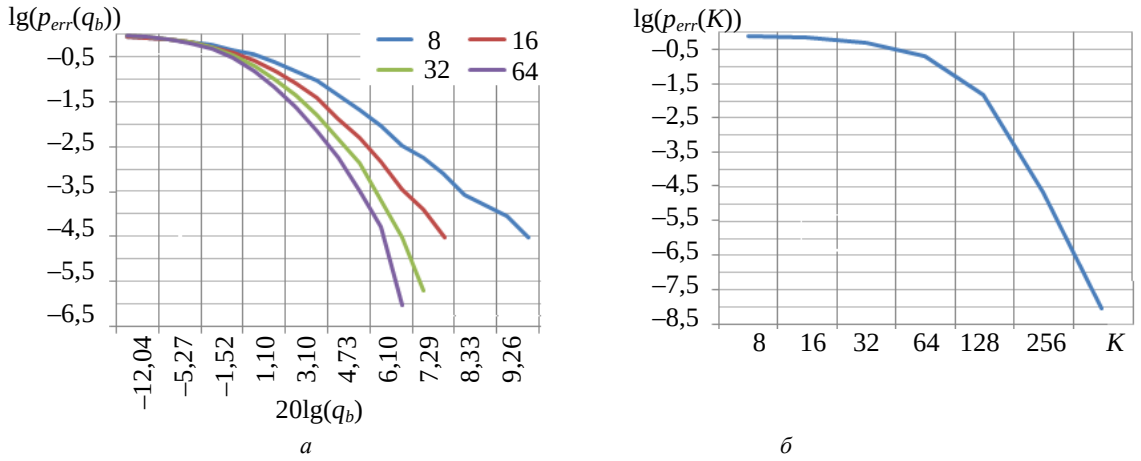
На рис. 7 более светлые оттенки соответствуют большим значениям амплитуды. По диаграммам заметны границы спектра отдельных СШС $F_l = 8$ и $F_u = 16$ относительных единиц частоты. Так же заметны расширения спектра в области склейки СШС. Наиболее заметно расширение спектра в области склейки на диаграмме сообщения без фильтрации (рис. 7, *а*), практически отсутствует специфичное расширение спектра в области склейки на диаграмме (рис. 7, *г*), т.е. на спектрограмме сообщения, прошедшего фильтрацию в областях склеек СШС в окне Хемминга.

Следует отметить, что в условиях многолучевого распространения по райсовской или рэлеевской модели для снижения межсимвольной интерференции между отдельными сигнальными символами добавляют паузу (межсимвольный интервал), при наличии таких пауз применение фильтрации для структурной скрытности теряет смысл. Но сама по себе фильтрация сообщения, с учетом межсимвольных интервалов, имеет смысл для улучшения контроля занимаемой сообщением полосы частот.

Энергетическая скрытность, метод реализации

Для сокрытия широкополосных сообщений используется метод энергетической скрытности. Благодаря хорошим автокорреляционным свойствам достаточно эффективно возможно скрывать СШС в шумах радиоэфира. Итак, энергетическая скрытность реализуется за счет стеганографического сокрытия передаваемых сообщений в шумах радиоэфира [20–22].

На рис. 8 приведены зависимости логарифма вероятности ошибок при различных отношениях сигнал–шум на бит $q_b = \sqrt{\frac{2E_b}{N_0}}$ (рис. 8, *а*) для алфавитов различной мощности $K \in \{8,16,32,64\}$ и при постоянном отношении амплитуд сигнал–шум $\frac{A_s}{A_N} = 0,33$, в зависимости от мощности алфавита (рис. 8, *б*).



а *б*

Рис. 8. Логарифмы вероятности ошибки: *а* – в зависимости от различных отношений сигнал–шум на бит для алфавитов ортогональных СШС; *б* – в зависимости от мощности алфавита K

Для обеспечения энергетической скрытности сигнала при одновременном условии уверенного приема следует учитывать вероятное расположение злоумышленника, диаграмму направленности антенны и закон затухания сигнала при удалении от передающей антенны. Как известно [23], плотность потока мощности радиоволн, приходящаяся на единицу поверхности, убывает обратно пропорционально квадрату расстояния r от передающей антенны: $P(r)=\frac{W_1}{4\pi r^2}$, где W_1 – мощность излучения передающей антенны, принимаемая мощность $W_2=\frac{W_1 G_a S_a}{4\pi r^2}$, G_a – коэффициент усиления и S_a – эффективная поверхность принимающей антенны.

Обеспечить эффективную энергетическую скрытность возможно при использовании алфавитов ортогональных СШС. Известно (рис. 8), что потенциал энергетической скрытности возрастает с ростом занимаемого СШС ресурса частота–время. При этом ортогональные алфавиты не позволяют эффективно использовать этот ресурс, причем чем он больше, тем ниже скорость передачи сообщений [24]. Предельная скорость передачи в ресурсе частота–время рассчитывается как $v_{\max}=\frac{2WT\log(SNR+1)}{T}$, максимальная скорость передачи информации при использовании взаимно ортогональных сигнальных символов $v_{\text{ort}}=\frac{\log(2WT)}{T}$, эффективность использования ресурса частота–время $\frac{v_{\text{ort}}}{v_{\max}}=\frac{\log(2WT)}{2WT\log(SNR+1)}$.

Таким образом, при использовании ортогональных СШС приходится решать задачу выбора: повышения энергетической скрытности и мощности алфавитов сообщений при одновременном понижении эффективности использования ресурса частота–время за счет доминирования роста потребления ресурса над ростом скорости передачи сообщений или снижение энергетической скрытности, уменьшение мощности алфавитов при повышении эффективности использования ресурса частота–время за счет высвобождения его части.

Заключение

В статье предложено решение частной задачи криптостеганографической защиты канала широкополосной связи. Разработан метод оценки вероятности повтора сигнальных широкополосных символов при обеспечении информационной скрытности. Разработан метод фильтрации сигнальных широкополосных символов в области сшивки для снижения вероятности определения длительности отдельных символов злоумышленником. Выполнена оценка параметров энергетической скрытности при использовании взаимно ортогональных сигнальных широкополосных символов.

Выполнена оценка параметров энергетической скрытности при использовании взаимно ортогональных сигнальных широкополосных символов.

Результаты исследований показывают, что защита канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов позволяет обеспечить передачу сообщений, практически исключающую повтор сигнальных широкополосных символов в сообщении, что и обеспечивает информационную защищенность.

Дополнительному повышению защищенности канала связи способствует применение структурной и энергетической скрытности.

Применение информационной, а возможно и совокупности информационной, структурной и энергетической, скрытности позволяет создавать дополнительную защиту радиосообщений, что повышает защищенность, обеспечиваемую методами криптографии.

Литература

1. Радзиевский А.Г. Современная радиоэлектронная борьба. Вопросы методологии. М.: Радиотехника, 2006. 424 с.
2. Цветнов В.В., Демин В.П., Куприянов А.И. Радиоэлектронная борьба. Радиоразведка и радиопротиводействие. Т. 2. М.: МАИ, 1998. 248 с.
3. Balaban P., Jeruchim M.C., Shanmugan K.S. Simulation of Communication Systems. NY: Plenum Press, 1992. 750 p.
4. Гришенцев А.Ю., Коробейников А.Г. Применение некоторых вейвлетов для генерации широкополосных сигналов // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 8. С. 712–720. doi: 10.17586/0021-3454-2017-60-8-712-720
5. Гришенцев А.Ю., Елсуков А.И. Адаптивная синхронизация в системах скрытой широкополосной связи // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 4. С. 640–650. doi: 10.17586/2226-1494-2017-17-4-640-650
6. Гришенцев А.Ю., Коробейников А.Г. Алгоритм поиска, некоторые свойства и применение матриц с комплексными значениями элементов для стеганографии и синтеза широкополосных сигналов // Журнал радиоэлектроники. 2016. № 5. С. 9.
7. Макаренко С.И., Иванов М.С., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. СПб: Свое издательство, 2013. 166 с.
8. Гришенцев А.Ю. Способ синтеза и применение шумоподобных широкополосных сигналов в задачах организации защищенных каналов связи // Радиотехника. 2017. № 9. С. 91–101.
9. Гришенцев А.Ю. Метод синтеза алфавитов ортогональных сигнальных широкополосных сообщений // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1074–1083. doi: 10.17586/2226-1494-2018-18-6-1074-1083
10. Гришенцев А.Ю., Коробейников А.Г., Елсуков А.И. Исследование и анализ некоторых свойств алфавитов на базе ортогональных широкополосных сигналов // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 1. С. 134–143. doi:10.17586/2226-1494-2019-19-1-134-143
11. Thomson J.J. On the structure of the atom: an investigation of the stability and periods of oscillation of a number of corpuscles arranged at equal intervals around the circumference of a circle; with application of the results to the theory of atomic structure // The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science. Series 6. 1904. V. 7. N 39. P. 237–265. doi: 10.1080/14786440409463107
12. Jaynes E.T. Probability Theory: The Logic of Science. Cambridge University Press, 2003. 758 p.
13. Suzuki K., Tonien D., Kurosawa K., Toyota K. Birthday paradox for multi-collisions // Lecture Notes in Computer Science. 2006. V. 4296. P. 29–40. doi: 10.1007/11927587_5
14. Mathis F.H. A generalized birthday problem // SIAM Review. 1991. V. 33. N 2. P. 265–270. doi: 10.1137/1033051
15. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы. В 2-х томах. Т. 1. М.: Мир, 1990. 415 с.
16. Barker E. Recommendation for Key Management. Part 1: General, 2016. 53 p. doi: 10.6028/nist.sp.800-57pt1r4
17. Панасенко С.А. Алгоритмы шифрования. Специальный справочник. СПб: БХВ-Петербург, 2009. 576 с.
18. Dinur I., Dunkelman O., Shamir A. Improved attacks on full GOST // Lecture Notes in Computer Science. 2012. V. 7549. P. 9–28. doi: 10.1007/978-3-642-34047-5_2
19. Lyons R.G. Understanding Digital Signal Processing. Prentice Hall PTR, 2001. 538 p.

References

1. Radzievskiy A.G. *Modern Electronic Warfare. Methodology*. Moscow, Radiotehnika Publ., 2006, 424 p. (in Russian)
2. Tsvetnov V.V., Demin V.P., Kupriyanov A.I. Electronic Warfare. Radio Radioprospecting and Radio Resistance. Moscow, MAI Publ., 1998, 248 p. (in Russian)
3. Balaban P., Jeruchim M.C., Shanmugan K.S. *Simulation of Communication Systems*. NY, Plenum Press, 1992, 750 p.
4. Grishentcev A. Yu., Korobeinikov A.G. Application of several wavelets for generating wideband signals. *Journal of Instrument Engineering*, 2017, vol. 60, no. 8, pp. 712–720. (in Russian) doi: 10.17586/0021-3454-2017-60-8-712-720
5. Grishentcev A.Yu., Elsukov A.I. Adaptive synchronization in hidden broadband systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 4, pp. 640–650 (in Russian). doi: 10.17586/2226-1494-2017-17-4-640-650
6. Grishentsev A.Yu., Korobeinikov A.G. Algorithm of search, some properties and application of matrices with complex values of elements for steganography and synthesis of broadband signals. *Zhurnal Radioelektroniki*, 2016, no. 5, p. 9. (in Russian)
7. Makarenko S.I., Ivanov M.S., Popov S.A. *Interference Immunity of Pseudo-Random Frequency Tuning Systems*. St. Petersburg, Svoe Izdatel'stvo Publ., 2013, 166 p. (in Russian)
8. Grishentsev A.Yu. On the method of synthesis and application of broadband noise-like signals in the task organization of protected communication channels. *Radioengineering*, 2017, no. 9, pp. 91–101. (in Russian)
9. Grishentsev A.Yu. Synthesis method for alphabets of orthogonal signaling broadband communications. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1074–1083 (in Russian). doi: 10.17586/2226-1494-2018-18-6-1074-1083
10. Grishentsev A.Yu., Korobeinikov A.G., Elsukov A.I. The study and analysis of some properties of the alphabets on the basis of the mutually orthogonal broadband signals. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 1. (in press)
11. Thomson J.J. On the structure of the atom: an investigation of the stability and periods of oscillation of a number of corpuscles arranged at equal intervals around the circumference of a circle; with application of the results to the theory of atomic structure. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, Series 6*, 1904, vol. 7, no. 39, pp. 237–265. doi: 10.1080/14786440409463107
12. Jaynes E.T. *Probability Theory: The Logic of Science*. Cambridge University Press, 2003, 758 p.
13. Suzuki K., Tonien D., Kurosawa K., Toyota K. Birthday paradox for multi-collisions. *Lecture Notes in Computer Science*, 2006, vol. 4296, pp. 29–40. doi: 10.1007/11927587_5
14. Mathis F.H. A generalized birthday problem. *SIAM Review*, 1991, vol. 33, no. 2, pp. 265–270. doi: 10.1137/1033051
15. Conway J.H., Sloane N.J.A. *Sphere Packing, Lattices and Groups*. Springer, 1988.
16. Barker E. *Recommendation for Key Management. Part 1: General*, 2016, 53 p. doi: 10.6028/nist.sp.800-57pt1r4
17. Panasenko S.A. *Encryption Algorithms. Special Handbook*. St. Petersburg, BKhV-Peterburg Publ., 2009, 576 p. (in Russian)
18. Dinur I., Dunkelman O., Shamir A. Improved attacks on full GOST. *Lecture Notes in Computer Science*, 2012, vol. 7549, pp. 9–28. doi: 10.1007/978-3-642-34047-5_2
19. Lyons R.G. *Understanding Digital Signal Processing*. Prentice Hall PTR, 2001, 538 p.
20. Telatar E. Capacity of multi-antenna Gaussian channels. *European Transactions on Telecommunications*, 1999, vol. 10, no. 6, pp. 585–596. doi: 10.1002/ett.4460100604
21. Ipatov V.P. *Spread Spectrum and CDMA. Principles and*

20. Telatar E. Capacity of multi-antenna Gaussian channels // European Transactions on Telecommunications. 1999. V. 10. N 6. P. 585–596. doi: 10.1002/ett.4460100604
21. Ipatov V.P. Spread Spectrum and CDMA. Principles and Applications. Wiley, 2004. 396 p.
22. Proakis J.G. Digital Communications. 4th ed. McGraw-Hill, 2001. 938 p.
23. Яковлев О.И., Якубов В.П., Урядов В.П., Павельев А.Г. Распространение радиоволн. М.: Ленанд, 2009. 496 с.
24. Ziemer R.E., Peterson R.L. Introduction to Digital Communication. Prentice-Hall, Upper Saddle River, 2000. 464 p.

Applications. Wiley, 2004, 396 p.
22. Proakis J.G. *Digital Communications*. 4th ed. McGraw-Hill, 2001, 938 p.
23. Yakovlev O.I., Yakubov V.P., Uryadov V.P., Pavel'ev A.G. *Radiowaves Spread*. Moscow, Lenand Publ., 2009, 496 p. (in Russian)
24. Ziemer R.E., Peterson R.L. *Introduction to Digital Communication*. Prentice-Hall, Upper Saddle River, 2000, 464 p.

Авторы

Гришенцев Алексей Юрьевич – доктор технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56321138400, ORCID ID: 0000-0003-1373-0670, Grishentsev@yandex.ru

Арустамов Сергей Аркадьевич – доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 59695216400, ORCID ID: 0000-0002-7520-8987, sergey.arustamov@gmail.com

Коробейников Анатолий Григорьевич – доктор технических наук, профессор, заместитель директора по науке, Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В.Пушкова Российской академии наук, Санкт-Петербург, 199034, Российская Федерация; профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56128063300, ORCID ID: 0000-0002-9968-0207, Korobeynikov_A_G@mail.ru

Козин Олег Владимирович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-0080-4688, urgentpost@yandex.ru

Authors

Alexey Yu. Grishentsev – D.Sc., Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56321138400, ORCID ID: 0000-0003-1373-0670, Grishentsev@yandex.ru

Sergey A. Arustamov – D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 59695216400, ORCID ID: 0000-0002-7520-8987, sergey.arustamov@gmail.com

Anatoly G. Korobeinikov – D.Sc., Professor, Deputy director for science, Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation Russian Academy of Sciences St. Petersburg Filial, Saint Petersburg, 199034, Russian Federation; Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56128063300, ORCID ID: 0000-0002-9968-0207, Korobeynikov_A_G@mail.ru

Oleg V. Kozin – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-0080-4688, urgentpost@yandex.ru