УДК 681.3.06:519.248.681

И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук, В.Л. МОРОЗОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ

Введение

К основным показателям эффективности телекоммуникационной системы относят: помехоустойчивость, надежность, живучесть, пропускную способность сети, качество обслуживания, рентабельность и стоимость, помехозащищенность, информационную безопасность и др.

Информационный обмен в ряде приложений телекоммуникационных систем (ТКС) осуществляется в условиях внутренних и внешних негативных воздействий. Примером внутренних воздействий являются помехи, создаваемые соседними станциями многопользовательских систем. Внешние воздействия связывают с преднамеренными помехами, создаваемыми станциями противодействия. При этом станция – постановщик преднамеренных помех – ставит перед собой цель лишить легальные станции возможности осуществлять надежный информационный обмен и минимизировать собственные затраты. Задача построения защищенной ТКС – это создание системы, устойчивой к воздействию множества различных угроз. В многопользовательских телекоммуникационных системах (ТКС) при передаче информации на значительные расстояния мощность преднамеренной помехи на входе приемного устройства в его полосе пропускания может значительно превышать мощность полезного сигнала, передаваемого одной из станций данной ТКС. Будем полагать, что в канале действует наиболее характерный вид помехи, описываемый гауссовским случайным процессом, спектр которого перекрывается со спектром сигнала. В этом случае вероятность ошибки зависит только от отношения мощности сигнала к общему мешающему воздействию. Необходимо подчеркнуть, что в ряде случаев возможность аппроксимации помехи гауссовским законом не так очевидна, поскольку показатели качества решения таких задач, как оценка параметров, *М*-я передача, зависят не только от отношения указанных мощностей.

Оценка помехозащищенности и информационной безопасности при различного рода воздействиях на телекоммуникационные системы.

Помехоустойчивость приема сигналов характеризует способность ТКС функционировать в условиях воздействия на систему различных помех и определяется выражением, связывающим отношение сигнал-помеха на выходе приемника (на входе согласованного фильтра или коррелятора – q^2) с отношением сигнал-помеха на входе приемника – ρ^2 [1]:

$$q^2 = 2B\rho^2, \qquad (1)$$

где $\rho^2 = \frac{P_c}{P_П}$ (P_c, $P_п$ – мощности сигнала и помехи соответственно); B =F·T – база сигнала (T – длительность сигнала).

Выражение (1) может быть представлено в виде

$$q^2 = \frac{2E}{N_П}, \qquad (2)$$

где E – энергия сигнала, $N_П = P_П / F$ – спектральная плотность мощности помехи в полосе F сигнала.

Помехоустойчивость ТКС оценивают вероятностью ошибки $P_{ош}$, которая, в свою очередь, определяется методами приема (когерентный, некогерентный) и свойствами сигналов, являющихся физическими переносчиками данных. Кроме того, вероятность ошибки в канале связи является функцией помех. Причем помеха в ряде случаев представляет собой сумму теплового шума N_0 и помехи, создаваемой станцией противодействия $N_П$. Таким образом, полная спектральная плотность мощности, вследствие наличия помех, увеличивается до значения $N_0 + N_п$ и отношение сигнал /шум можно записать в виде $E/(N_0 + N_П)$.

Как правило, мощность станции постановщика помех значительно больше мощности теплового шума. Поэтому величину отношения сигнал/шум принимают равной $\frac{E_C}{N_П}$

Известно, что энергия сигнала определяется из соотношения [1]:

$$E_C = P_C T = \frac{P}{R}, \tag{3}$$

где P – мощность полезного сигнала; T – время передачи бита; R – скорость передачи данных (бит/с).

Тогда требуемое для обеспечения заданного значения вероятности ошибки в канале отношение энергии бита данных к спектральной плотности мощности помехи может быть найдено из соотношения [2]:

$$(\frac{E_C}{N_П})_{треб.} = (\frac{P/R}{P_П/F})_{треб.} = (\frac{F/R}{P_П/P_C})_{треб.} = \frac{B}{(P_П/P_C)_{треб.}}, \tag{4}$$

где $B = F/R$ – коэффициент расширения спектра сигнала (база сигнала).

Отношение мощности помехи к мощности сигнала может быть записано в виде

$$(\frac{P_П}{P_C})_{треб.} = \frac{B}{(E_C/N_П)_{треб.}} \tag{5}$$

Выражение (5) можно интерпретировать следующим образом. В целях подавления сигналов станции постановщик помех стремится увеличить значение $(\frac{E_C}{N_П})_{треб.}$ посредством уменьшения $N_П$. Это приводит к уменьшению значения $(\frac{P_П}{P_C})_{треб.}$. Однако защищенная система в этом случае может прибегнуть к увеличению базы сигнала, усложняя задачу станции противодействия по постановке помех.

Очевидно, что станция противодействия может иметь полную информацию о режимах функционирования ТКС, частотном диапазоне работы, классах сигналов – переносчиков данных, времени сеансов связи, объеме передаваемой информации и т.д. Кроме того, станция противодействия может владеть аналогичными образцами объектов. В указанных условиях создание радиоканалов ТКС должно осуществляться таким образом, чтобы наиболее эффективной стратегией станции противодействия была стратегия нарушение функционирования системы путем постановки так называемой заградительной помехи (помеха в виде стационарного гауссова шума с нулевым средним и равномерным распределением спектральной плотности мощности, по крайней мере, в области частот, занимаемой сигналом).

Рассмотрим воздействие заградительной помехи на ТКС. Спектральная плотность мощности помехи, создаваемой станцией противодействия,

$$N_П = P_П / F, \tag{6}$$

где F – ширина полосы диапазона, в которой создаются помехи.

Вероятность ошибки на бит сообщения при некогерентной обработке сигнала [1]:

$$P_0 = Q(\frac{\sqrt{2E_C}}{N_0}), \tag{7}$$

где Q – интеграл вероятности.

Средняя вероятность ошибки на бит сообщения при когерентной обработке при наличии широкополосного шума

$$P_0 = Q(\frac{\sqrt{2E}}{N_0 + N_П}) = Q(\sqrt{\frac{2E/N_0}{1+(\frac{E}{N_0})(\frac{P_П}{P_C})/B}}) \ . \tag{8}$$

Графики зависимости P_0 от $\frac{E}{N_0}$ при фиксированном отношении $\frac{P_П}{P_C}$ приведены на рисунке [3]. Анализ кривых, приведенных на рисунке, показывает, что вероятность ошибки может быть существенно уменьшена при увеличении коэффициента расширения спектра сигнала B.

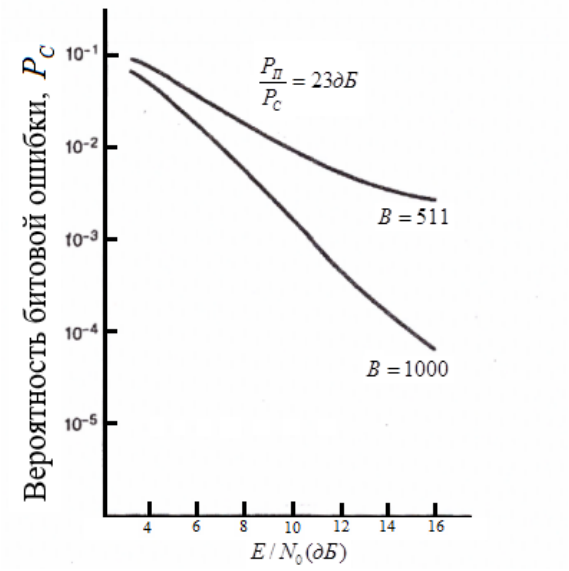

График зависимости вероятности ошибки (P_0) от $\frac{E}{N_0}$

Из соотношений (1) – (7) следует, что при ограничениях на максимальную мощность сигнала и мощность помехи, создаваемой станцией противодействия, единственной возможностью противостоять заградительной помехе является привлечение широкополосной технологии, т.е. сигналов со значительным частотно-временным ресурсом (базой сигналов).

Характерной ситуацией для практики мешающего воздействия на функционирование ТКС, является узкополосная помеха. Причем данный тип помех может быть реализован как станцией противодействия в целях нарушения работы системы, так и соседствующими станциями, создающими помехи вследствие своего обычного функционирования. Оптимальной процедурой обработки сигнала в этом случае можно считать фильтрацию, согласованную с мешающим воздействием (абелевый белый гауссовский шум и узкополосная помеха). Такая обработка эквивалентна вырезанию частотного интервала, в котором сосредоточена помеха. При этом вырезаются и частотные компоненты сигнала в пределах полосы помехи. Согласованный фильтр обеспечивает выходное отношение мощностей сигнала и шума (q_j^2) в виде [1]:

$$q_j^2 = q^2(1-\frac{F_j}{F}), \tag{9}$$

где $q^2 = \frac{2E}{N_0}$ – отношение мощностей сигнала и шума на выходе согласованного фильтра в отсутствие помехи; F_j – полоса помехи; F – полоса сигнала.

Известно [1, 2], что при воздействии на ТКС узкополосной помехи методом защиты является режекторная фильтрация части спектра, на которую воздействует помеха, кроме того, возможно реализовать передачу данных переносом его спектра в диапазон частот, свободный от воздействия помех.

Приведенные выше результаты справедливы для случая, когда помеха является нормальным случайным процессом и обладает равномерной спектральной плотностью. Станция противодействия для подавления системы может использовать мощные структурные помехи с неравномерным спектром. В таких условиях функционирования ТКС помехоустойчивость в значительной мере определяется подобием (различием) структур сигнала и помехи, т.е. тем, как подавляются отдельные элементы сигнала помехой.

Известно, что коэффициент передачи согласованного фильтра определяется выражением [1]:

$$k(\omega) = \frac{cg(\omega)}{N(\omega)}, \tag{10}$$

где c – постоянная; $g(\omega)$ – спектр сигнала.

Отношение сигнал / помеха при этом определяется выражением

$$q^2 = \frac{2}{\pi}\int_0^{\infty}\frac{|g(\omega)|^2}{N(\omega)}. \tag{11}$$

Соотношения (10) – (11) указывают на стратегию действий станции постановщика помех и защищенной системы. Помеха, создаваемая постановщиком помех, должна конструироваться таким образом, чтобы выполнялось равенство $N(\omega) = a\,|\,g(\omega)\,|$, где a – постоянная величина. Последнее равенство означает следующую стратегию: сильнее подавлять те спектральные составляющие, которые переносят большую часть энергии сигнала. Путем снижения усиления согласованного фильтра в области резких пиков в спектре помехи осуществляется исключение этой части спектра. Если имеет место «провал» в спектре помехи, то посредством увеличения усиления согласованного фильтра (согласно (11)) возможно повышение отношения сигнал/помеха. Таким образом, помехоустойчивость системы не снижается вследствие воздействия на систему помехи с неравномерным спектром.

Большинство приложений ТКС относятся к многопользовательским системам. В таких системах вследствие работы большого числа абонентов в общем частотном диапазоне возникают помехи множественного доступа, или взаимные помехи. Рассмотрим влияние взаимной помехи на помехоустойчивость приема данных в ТКС.

Пусть ширина общей полосы частот системы равна F. Предположим, что ширина спектра всех сигналов в ТКС равна ширине общей полосы частот и все активные абоненты создают на входе j-го приемника сигналы одинаковой мощности – P_C. В этом случае мощность взаимной помехи, создаваемой l мешающими абонентами, будет равна $l \cdot P_C$. Допустим, что спектральная плотность мощности взаимной помехи постоянна в пределах общей полосы частот

$$N_{П} = \frac{lP_C}{F}, \tag{12}$$

и взаимная помеха (по своим статистическим свойствам) приближается к нормальному случайному процессу. Таким образом, сделанные предположения позволяют считать

взаимную помеху нормальным случайным процессом с равномерной спектральной плотностью мощности. Нетрудно убедиться, что отношение сигнал/шум на входе решающего устройства приемника определяется из выражения

$$q^2 = \frac{B}{l} = FR/l \ , \tag{13}$$

где R – скорость передачи информации.

Из (13) следует, что при заданном числе активных абонентов l увеличение помехоустойчивости возможно только за счет увеличения базы *B* сигналов. Это объясняется тем, что с увеличением базы (с увеличением ширины спектра сигналов при постоянной скорости передачи информации *R*) уменьшается спектральная плотность мощности помехи $N_п$.

В практике работы ТКС возможны случаи, когда мощность одного или нескольких мешающих сигналов во много раз больше мощности полезного сигнала. Каким образом в этих условиях обеспечить необходимую помехозащищенность?

Пусть мощность полезного сигнала – P_C, а мощность мешающей составляющей – $P_П$. Мощность сигнальной составляющей на выходе согласованного фильтра в момент принятия решения (отсчета) пропорциональна P_C, а мощность мешающей составляющей – $P_П R_{jk}^2(\tau)$, где R_{jk}^2 – взаимнокорреляционная функция (ВКФ) полезного *k*-го сигнала и *j*-го – мешающего. Величина τ определяется смещением ВКФ относительно момента отсчета. Отношение сигнал-помеха на выходе устройства оптимального приема определяется соотношением [1]:

$$q^2(\tau) = \frac{P_C}{P_П R_{jk}^2(\tau)} \ , \tag{14}$$

Наименьшее отношение сигнал-помеха:

$$q^2(\tau) = \frac{P_C}{P_П R_{\max}^2(\tau)} \ , \tag{15}$$

где $R_{макс}$ – максимальное значение $R_{jk}(\tau)$.

Очевидно, что для повышения помехозащищенности ТКС необходимо выбирать сигналы, у которых максимальные пики ВКФ минимальны.

Если максимальные пики ВКФ уменьшены до среднеквадратического уровня: $\sigma_{j,k} = \sigma^2$, то отношение сигнал/помеха будет

$$q^2(\tau) = \frac{P_C}{P_П}\sigma^2 \ . \tag{16}$$

Например, если: $\sigma^2 = \frac{1}{2FT}$, то

$$q^2(\tau) = \frac{P_C}{P_П} FT \ . \tag{17}$$

Для дискретных фазоманипулированных сигналов $\sigma^2 = \frac{1}{2N}$ (*N* – число элементов сигнала). Для такого класса сигналов отношение сигнал-помеха определяется из выражения:

$$q^2(\tau) = \frac{P_C}{P_П} 2N \tag{18}$$

Из выражений (17), (18) следует, что увеличение базы сигнала приводит к увеличению q^2 (а значит, – к увеличению помехоустойчивости системы) и может компенсировать

уменьшение отношения $\frac{P_C}{P_П}$ в случае увеличения станцией противодействия мощности помехи $P_П$.

Помехозащищенность ТКС в условиях воздействия помех, преднамеренно создаваемых станцией противодействия, зависит от скрытности выбора и использования параметров системы. При этом под скрытностью системы в целом и скрытностью используемых в системе параметров будем понимать способность ТКС противостоять мерам радиотехнической разведки, направленным на обнаружение факта работы системы (энергетическая скрытность) и определение необходимых для радиопротиводействия параметров сигнала (структурная и информационная скрытность).

Энергетическую скрытность радиоканала определим как способность радиоканала функционировать с таким энергетическим потенциалом, которого недостаточно для того, чтобы станция противодействия осуществляла перехват и прием сигналов – физических переносчиков информации с требуемой достоверностью:

$$S_Э = P(E / N_0 < G_{треб}), \tag{19}$$

где E / N_0 – отношение энергии сигнала к спектральной плотности мощности шума на входе решающего устройства приемника станции противодействия; $G_{треб}$ – значение отношения E / N_0 для приема данных с требуемой достоверностью.

Другими словами, энергетическая скрытность радиоканала может быть определена как вероятность того, что отношение сигнал/шум на входе решающего устройства приемника станции противодействия не превысит требуемого значения, необходимого для обнаружения сигнала.

Структурная скрытность характеризует способность ТКС противостоять мерам станции противодействия, направленным на отождествление обнаруженного сигнала с одним из множества априорно известных сигналов (распознаванием формы сигнала, определяемой способами его кодирования и модуляции).

Введем понятие структурной скрытности сложного сигнала в виде соотношения

$$S = \frac{\prod_{i=1}^{K} M_i^*}{\prod_{i=1}^{K} M_i}, \tag{20}$$

где M_i^* – число координат сложного сигнала, которые необходимо знать для того, чтобы определить оставшиеся $M_i - M_i^*$ координаты.

Для случая использования в системе фазоманипулированных сигналов выражение (20) имеет вид

$$S = \frac{l}{L}, \tag{21}$$

где l – число символов, которое необходимо знать для определения правила (закона) формирования оставшихся L – l символов.

Качество услуг, которые предоставляет ТКС, оценивают уровнем обеспечения информационной безопасности [4]. При этом под информационной безопасностью будем понимать способность ТКС обеспечивать защиту от уничтожения, модификации, блокирования информации, ее несанкционированной утечки или от нарушения установленного порядка ее маршрутизации. Также под информационной безопасностью следует понимать состояние защищенности систем обработки и хранения данных, при котором обеспечивается сохранение конфиденциальности, целостности и доступности информации, аутентичности, неопровержимости и надежности и также других свойств информации.

Одной из составляющих информационной безопасности (наряду с информационной

скрытностью) является система имитозащиты (обеспечение целостности) информации. Под имитозащищенностью понимают комплекс организационно-технических мероприятий и средств, а также законодательных норм, которые направлены на обеспечение определенного уровня имитостойкости. По сути, имитостойкость является сложной услугой, которая обеспечивается предоставлением таких услуг как целостность, подлинность (аутентичность), и которая поддерживается применением различных криптографических алгоритмов и криптографических протоколов [4] .Основным методом обеспечения необходимого уровня имитостойкости является внесение в сообщение избыточности, которая может формироваться в виде контрольных сумм, избыточных символов кодов, определяющих ошибки, криптографических контрольных сумм (кодов аутентификации сообщений – имитовставок) и др. В качестве показателей оценки имитостойкости могут быть использованы сложность процедур и вероятность навязывания неправдивой (ложной, модифицированной и т.д.) информации, с учетом методов и вычислительных мощностей средств, используемых злоумышленником. К настоящему времени разработан ряд методов обеспечения имитостойкости. В основном они ориентированы на использование методов и средств криптографической защиты информации и избыточного кодирования. В то же время, как показали исследования [4], обеспечить требуемую в ТКС имитостойкость возможно на уровне источника сложных сигналов за счет: увеличения размерности пространства сигналов и размерности пространства параметров сигналов, относительно которых создается неопределенность использования сигналов со сложной структурой; изменения (через определенные промежутки времени) параметров сигналов; использования сигналов с нелинейными законами формирования, обладающих свойствами, близкими к свойствам случайных последовательностей.

На уровне источника сигналов (на физическом уровне) имитостойкость I_c зависит от размерности пространства сигналов M, числа разрешенных к использованию в интервале времени t сигналов Z, числа попыток навязывания (имитации) C и политики навязывания X:

$$I_c = F(M, Z, C, X); \tag{22}$$

или

$$I_c = l - P_{нав}, \tag{23}$$

где $P_{нав}$ – вероятность навязывания (имитации) сообщения станцией противодействия.

При равновероятном и независимом выборе сигналов, используемых в качестве физических переносчиков данных, значение имитостойкости может быть рассчитано с использованием соотношения

$$P_{нав} = C / M . \tag{24}$$

Среди основных направлений улучшения показателей эффективности функционирования ТКС, в частности помехозащищенности, скрытности, информационной безопасности, можно выделить направления, связанные с применением каналов с большой частотной избыточностью, высокой пространственной, структурной, энергетической и временной скрытностью [4]. Для обеспечения частотной избыточности в настоящее время на физическом уровне используются фазоманипулированные широкополосные сигналы (ФМ ШПС) и частотно-фазоманипулированные (ЧФМ) сигналы. При этом анализ методов информационного обмена в телекоммуникационных системах (ТКС) показывает, что для передачи данных в таких системах используют дискретные сигналы с линейными законами их формирования. Такие сигналы обладают ограниченными ансамблевыми характеристиками и, в соответствии с критерием (21), низкой кодовой устойчивостью против раскрытия законов их формирования (низкой структурной скрытностью). Применение указанных систем сигналов в ТКС не позволяет обеспечивать требуемые показатели по помехозащищенности и скрытности их функционирования [1]. Кроме того, применяемые в ТКС методы цикловой синхронизации и управления предполагают, что в течение продолжительного времени в канале синхронизации передается один и тот же широкополосный сигнал линейной формы, а в

информационном канале, т.е. на физическом уровне, соответствие: бит (m бит) сообщения – сигнал линейной формы (2^m сигналов) с течением времени остается фиксированным. Такой метод информационного обмена позволяет нарушителю на основе определения параметров используемых в системе сигналов осуществить постановку преднамеренных структурных помех с минимальными энергетическими затратами. Такие помехи (с точки зрения станции противодействия) являются оптимальными и могут быть созданы при некоторой априорной определенности нарушителя относительно пространства состояний канала передачи данных (несущие частоты, формы используемых сигналов и др.). Указанный тип помехи представляет собой либо ретранслированные, либо имитационные помехи, обработка которых совместно с полезным сигналом, приводит к энергетическому подавлению последнего. В указанных условиях, в процессе информационного противодействия, нарушитель с большой вероятностью может подавлять радиоканал, применяя станции помех с энергетическим потенциалом, соизмеримым с энергетикой радиоканала, а также осуществить навязывание ложных режимов работы системы (синхронизации, управления), ложных сообщений, что, в свою очередь, может привести к существенному ухудшению показателей функционирования ТКС (помехозащищенности, информационной безопасности, имитостойкости, живучести, вероятностно-временных показателей передачи сообщений).

Основным решением указанной проблемы является повышение помехозащищенности (в частности, энергетической, структурной и информационной скрытности) и информационной безопасности (в частности, имитостойкости) ТКС на основе усовершенствования методологических основ построения ТКС путем разработки методов информационного обмена, синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствами.

Известно, что для технологии распределенного спектра свойства сигналов-переносчиков данных полностью определяются свойствами дискретных последовательностей (ДП), манипулирующих информационные биты данных пользователей системы [5]. Именно поэтому актуальным является поиск эффективных методов синтеза дискретных сигналов (последовательностей), отвечающих потенциально достижимым граничным характеристикам (минимаксным свойствам). Задача синтеза ДП оказывается еще более сложной, если выдвигаются требования к размерности (объему) системы сигналов, структурным свойствам и числу элементов ДП. При этом анализ [1 – 3, 5,6] показал, что в настоящее время отсутствуют регулярные методы синтеза дискретных последовательностей (ДП), являющихся оптимальными по минимаксному критерию и обладающих необходимыми для построения защищенных ТКС ансамблевыми, корреляционными и структурными свойствами

В работах [6 – 9] сформулирована и решена задача синтеза нелинейных дискретных последовательностей, обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования телекоммуникационной системы. Сложные сигналы, полученные на основе таких последовательностей при использовании системы расширения спектра методом прямой последовательности, обладают, с одной стороны, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, а с другой – требуемыми ансамблевыми и корреляционными свойствами. Кроме того, такие системы сигналов существуют и обладают указанными выше свойствами для широкого спектра значений периода последовательностей. Метод синтеза нелинейных криптографических дискретных сигналов (КС), представленный в [7], основан на использовании случайных или псевдослучайных процессов, и позволяет создавать последовательности символов (сигналов) определенного алфавита, которые удовлетворяют требованиям необратимости, неразличимости, непредсказуемости [10 – 11] и при этом обладают необходимыми (для тех или иных приложений ТКС) ансамблевыми и корреляционными свойствами [9, 12]. Практическое использование данной системы сигналов позволит повысить

(в соответствии с критерием (21)) скрытность функционирования ТКС. Так, для периода сигналов порядка 1000 элементов структурная скрытность КС превышает данный показатель для линейных классов сигналов (*M* последовательностей) более чем в 30 раз.

Характеристики корреляционных функций синтезированных КС не уступают, а в ряде случаев превосходят, соответствующие характеристикам линейных сигналов. В частности, КП обладают улучшенными по сравнению с *M*-последовательностями, взаимно-корреляционными свойствами. Так, применение синтезированных систем нелинейных криптографических сигналов (КС) позволит при использовании КС с периодом 256 элементов в качестве синхронизирующих последовательностей более чем на 3 дБ повысить помехоустойчивость приема сигналов. Значения максимальных боковых лепестков периодической функции взаимной корреляции (ПФВК) КС меньше, чем у широко применяемых в ТКС линейных классов сигналов, построенных на основе *M*-последовательностей. При этом объем системы, составленной из КС, например при периоде КС 1023 элементов, более чем на четыре порядка больше, чем объем системы, составленной из *M*-последовательностей (таблица).

Известно, что в классе линейных последовательностей, образованных на основе *M*-последовательностей, улучшенными ансамблевыми и корреляционными свойствами обладают множества Голда и Касами (так называемые последовательности с трехуровневой функцией взаимной корреляции – ПФВКТ). Так, для периода последовательностей N=1023 элемента, значения максимальных боковых лепестков ПФВК не превосходят 33 (так называемая «граница плотной упаковки» – $2\sqrt{L}$, таблица). При значении уровня боковых лепестков ПФВК $R_{max} = 3\sqrt{L}$, объем системы, составленной из КС, более чем в 15 раз больше объема множеств Голда и Касами. За счет улучшенных ансамблевых свойств КС появляется возможность улучшить, в соответствии с критерием (24), показатели информационной безопасности.

Класс сигналов	Период последовательности	Значение границы «плотной упаковки»	Число пар последовательностей, удовлетворяющих границе
M-последовательности	127	27	36
ПФВКТ	127	17	11610
КП	127	23	47 053
M-последовательности	511	63	276
ПФВКТ	511	33	147500
КП	511	63	2666671
M-последовательности	1023	100	435
ПФВКТ	1023	65	338000
КП	1023	100	5293538

Выводы

В целях улучшения показателей помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий необходимы новые решения научной проблемы взаимодействия удаленных информационных объектов на основе усовершенствования методологических основ построения телекоммуникационной системы путем разработки методов синтеза сложных нелинейных дискретных сигналов с необходимыми ансамблевыми, структурными и корреляционными свойствами, а также методов обработки данных в телекоммуникационной системе. Исследования и сравнительный анализ известных методов информационного

обмена показали, что одним из перспективных направлений комплексного обеспечения требуемых значений показателей помехозащищенности и информационной безопасности является реализация в радиоканалах ТКС динамического режима функционирования, когда с течением времени соответствие: m – бит – 2^m сложных сигналов изменяется по сложному закону, а в качестве сложных сигналов применяются сигналы, основанные на нелинейных принципах построения, в частности нелинейные криптографические сигналы, для синтеза которых используются случайные (псевдослучайные) процессы, и нелинейные сигналы в базисе простых и расширенных полей Галуа [6, 7, 9]. Данные классы сигналов обладают необходимыми для создания защищенных ТКС ансамблевыми, структурными и корреляционными свойствами.

Список литературы: 1. *Варакин, Л. Е.* Системы связи с шумоподобными сигналами / Л.Е Варакин. – М. : Радио и связь, 1985. – 384 с. 2. *Ipatov, Valery P.* Spread Spectrum and CDMA.Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University ‘LETI’, Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2005. – 385 p. 3. *Sklar, B.* Digital Communications [Текст] / B Sklar. – Prentice-Hall, Upper Saddle River, NJ, 2001. – 1082 с. 4. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків : Форт, 2012. – 880 с. 5. *Sarvate, D.V.* Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90. 14. *Gold, R.* Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory. – 1967. – Vol. 13. – P. 619–621. 6. *Замула, А.А.* Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях / А.А. Замула, Е.А. Семенко // Системи обробки інформації. – Харьков : ХУПС, 2015. – Вип. 5 (130). – С. 129 – 134. 7. *Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. P. 169-178. 8. *Замула, А.А.* Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций корреляции / А.А. Замула // Системи обробки інформації. – Харків : ХУПС, 2015. – Вип. 10 (135). – С. 35-39. 9. *Горбенко, И.Д., Замула, А.А.* Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах // Радиотехника. – 2016. – Вып. 186. – С. 7 – 23. 10. *Application* Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001. 11. *NIST 800-90* b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

Харьковский национальный университет
имени В.Н.Каразина

Поступила в редколлегию 20.04.2017