

УДК 621.391

СТЕГАНОГРАФИЧЕСКАЯ СЕТЬ ПЕРЕДАЧИ ДАНЫХ НА ОСНОВЕ МІМО-ТЕХНОЛОГИИ И ХАОТИЧЕСКИХ НЕСУЩИХ



К.С. ВАСЮТА, С.В. ОЗЕРОВ

Харьковский университет
Воздушных Сил им. Ивана Кожедуба

Abstract – The paper presents an analysis of the specific properties of chaotic signals (processes) such as sensitivity to the initial values of the signal and the exponential divergence of close phase trajectories, continuous power spectrum and exponentially decaying correlation function, unpredictability over long time intervals. Based on the properties of chaotic signals and MIMO-technology, synthesized version of the construction of steganographic data network system hidden command and control of operational-tactical level. In the network is hidden transmission of digital information due to increasing energy and structural secrecy of the information signal, the problem is solved electromagnetic compatibility provided by the multi-channel signal mean, the problem of increasing the speed of information transfer is solved.

The budget for the network radio "command post – unmanned aerial vehicle" is calculated. It was established that the steganographic data network level and forming a signal processing must be realized as a software-defined radio, which allows depending on the transmission signal to adaptively modify the track modulation types, the output power of the transmitter channel types of signal encoding parameters spread spectrum signal, data rate, the proportion of time for transmission and reception of communication channels, transmission data encryption parameters.

The presented approach can be implemented with the creation of a single information and communication space in a hidden system of command and control organized by the network-centric principle. This network creates a noise field in the space formed by the set of chaotic carriers, which greatly complicates the radio intelligence at the correct classification of radiation sources.

Анотація – У роботі представлено аналіз специфічних властивостей хаотичних сигналів (процесів). Спираючись на властивості МІМО-технології, синтезовано варіант побудови стеганографічної мережі передачі даних у системі прихованого управління військами оперативно-тактичного рівня. Зроблено розрахунок бюджету даної мережі. Встановлено, що для приховування факту циркуляції інформації в мережі з позиції стороннього спостерігача необхідно адаптивно змінювати види модуляції, вихідну потужність передавача, підвищувати чутливість приймача, параметри розширення спектра сигналу (застосовувати хаотичні види модуляції), швидкість передачі даних, співвідношення часу передачі і прийому, параметри шифрування переданих даних.

Аннотация – В работе представлен анализ специфических свойств хаотических сигналов (процессов). Опираясь на свойства МІМО-технологии, синтезирован вариант построения стеганографической сети передачи данных в системе скрытого управления войсками оперативно-тактического уровня. Произведен расчет бюджета данной сети. Установлено, что для скрытия факта циркуляции информации в сети с позиции стороннего наблюдателя необходимо адаптивно изменять виды модуляции, выходную мощность передатчика, повышать чувствительность приемника, параметры расширения спектра сигнала (применять хаотические виды модуляции), скорость передачи данных, соотношение времени передачи и приема, параметры шифрования передаваемых данных.

Введение

Интенсивное развитие средств вооруженной борьбы, изменение масштаба и характера ведения военных (боевых) действий обуславливают современные требования, предъявляемые к структуре, принципам построения и развития системы скрытого управления войсками. Техническую основу перспективной системы управления со-

ставляет совокупность организованных по сетевым принципам информационных, вычислительных и телекоммуникационных ресурсов (сетей), предназначенных для обеспечения устойчивого и скрытого управления войсками и оружием в любых условиях.

Обеспечение скрытого управления войсками достигается путем применения систем обмена информацией с повышенной скрытностью функционирования, так называемых стеганографических сетей передачи информации [1]. Под стеганографической сетью передачи данных следует понимать сеть, в которой реализуется скрытие самого факта обмена информацией. Назначением такой сети является скрытие системы управления войсками и вооружением.

Исходя из анализа литературы [2, 3], при построении радиотехнической стеганосистемы должны учитываться следующие требования:

- скрытие факта передачи информации для стороннего наблюдателя (скрытность функционирования);
- обеспечение необходимой пропускной способности (что особенно актуально для скрытой передачи данных);
- обеспечение аутентичности и целостности конфиденциальной информации для авторизованного пользователя;
- обнаружение скрытого сообщения сторонним наблюдателем не должно позволить ему выявить принцип формирования сигнала (структурная скрытность).

В системах с повышенной скрытностью функционирования в качестве несущих широко применяются широкополосные сигналы, такие как фазокодоманипулированные (ФКМ), дискретно-частотно манипулированные (ДЧМ), с применением псевдослучайных последовательностей, т.е. работа под “шум”, когда разведывательный приемник не может обнаружить (накопить) передаваемый сигнал.

Однако данные типы сигналов не отвечают требованиям скрытности в полной мере. Псевдослучайные последовательности, применяемые для расширения спектра гармонического сигнала, имеют сравнительно короткий период генерируемой последовательности, обладают ярко выраженной зависимостью между последовательными соседними значениями и неравномерностью распределения значений (амплитуд), а ФКМ и ДЧМ сигналы отличаются от шума наблюдения при корреляционном, спектральном и нелинейном анализе [1].

Альтернативой является применение сложных хаотических сигналов, которые по своим статистическим и динамическим характеристикам подобны шуму наблюдения. Таким образом, целью работы является синтез стеганографической сети передачи данных, реализованной на хаотических сигналах и ММО-технологии.

I. Анализ свойств хаотических сигналов

Хаотическими процессами [4] называют сложные колебания, порождаемые нелинейными динамическими системами. Данные процессы, в отличие от гармонических колебаний, обладают свойствами, присущими обыкновенным случайным процессам, такими как сплошной спектр мощности и экспоненциально спадающая кор-

реляционная функция [5], непредсказуемость на больших интервалах времени.

Также следует отметить, что хаотические процессы, в отличие от случайных процессов, обладают такими свойствами, как высокая чувствительность к начальным значениям x_0 и экспоненциальное разбегание близких фазовых траекторий. На рис. 1 иллюстрируется зависимость коэффициента корреляции двух хаотических процессов, сформированных при помощи полинома Чебышева первого рода третьего порядка, от различных начальных значений $x_0 \in (0..1)$ их формирования $\Delta x = x_0^{(1)} - x_0^{(2)}$.

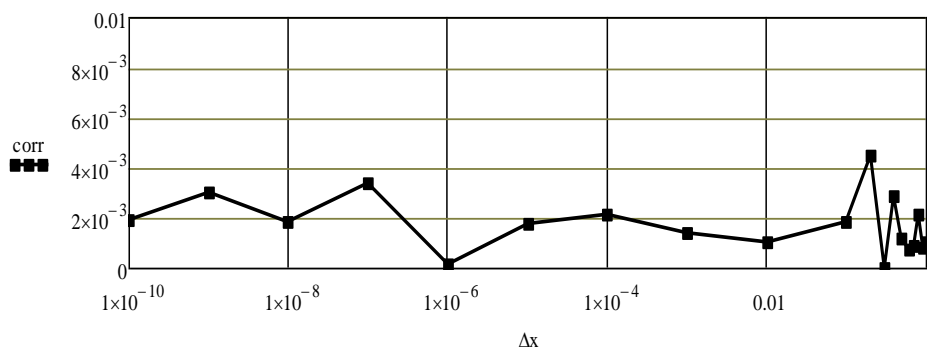


Рис. 1. Зависимость коэффициента корреляции двух хаотических процессов от расхождения начальных значений на Δx при их формировании

Из анализа рисунка следует, что хаотические процессы, сформированные с различными x_0 , отличающимися на $\Delta x \in [10^{-10} \dots 10^{-1}]$, не коррелированы.

Применение хаотических несущих в радиотехнических системах позволяет получить следующие преимущества:

- хаотические колебания можно получать при помощи достаточно простых динамических схем или цифровых формирователей сигналов;
- возможность формирования множества ортогональных сигналов, что позволит обеспечить многоканальность сложных систем и их электромагнитную совместимость;
- возможность самосинхронизации приемника и передатчика;
- потенциально большая информационная емкость хаотических систем связи;
- возможность получения разнообразных методов введения сообщения в хаотический сигнал.

Шумоподобность систем, основанных на хаосе, дают им потенциальные преимущества над традиционными системами с расширением спектра, базирующимися на псевдослучайных последовательностях. Кроме того, они позволяют получить более простую аппаратную реализацию с большей скрытностью, более высокую скорость операций. Однако хаотические сигналы (процессы) имеют структурированные (упорядоченные) аттракторы (фазовые портреты), отличающие их от шума. В свою очередь степень структурированности аттрактора хаотического процесса определяет его скрытность.

Применение сторонним наблюдателем современных методов нелинейного анализа [6] увеличивает вероятность правильной классификации наблюдения (белый шум или хаотический процесс) и приводит к снижению потенциальной скрыт-

ности хаотического сигнала до уровня, обусловленного шумом его наблюдения. Для увеличения скрытности хаотического процесса необходимо усложнять его аттрактор, т.е. уменьшать степень его структурированности.

Среди различных возможностей усложнения аттрактора хаотического процесса можно выделить метод усложнения сигнала путем частотной фильтрации хаотической несущей, предложенный в работе [7] (рис. 2).

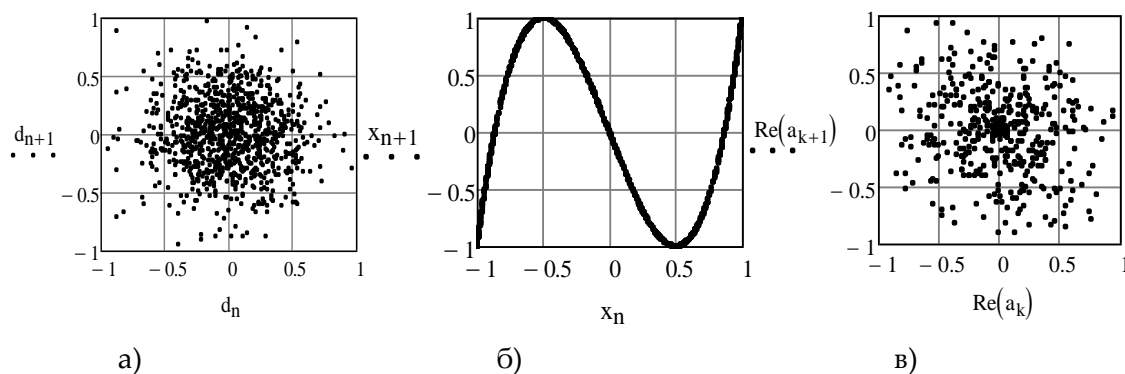


Рис. 2. Фазовый портрет: белого шума (а), хаотического сигнала (б),
фильтрованного хаотического сигнала (в)

Анализ рисунка показывает, что аттрактор фильтрованного хаотического сигнала подобен аттрактору белого шума, что повышает его скрытность.

Следует также отметить, что применение хаотических сигналов (процессов) приводит к расширению спектра передаваемого сигнала и, как следствие, при ограниченной полосе пропускания канала связи к уменьшению скорости передачи информации. Однако эта проблема решается путем применения ММО-технологии на хаотической несущей [8] за счет реализации множества хаотических сигналов с различными начальными значениями формирования.

II. Синтез стеганографической сети передачи данных

Опираясь на проведенный анализ свойств ортогональных хаотических сигналов, рассмотрим возможность построения стеганографической сети передачи данных на хаотических несущих с применением ММО-технологии.

Сложность проблемы, связанной с проектированием сети передачи данных, обусловлена необходимостью учета достаточно большого количества факторов (исходных данных), влияющих на эффективность ее решения. К основным из них стоит отнести следующие: численность и размещение потенциальных пользователей (абонентов) и их требования к перечню и содержанию предоставляемых услуг связи, уровень качества обслуживания, требования к срокам проектирования, окупаемости и т.д. Процесс проектирования сетей передачи данных включает в себя несколько этапов (рис. 3).

Определение числа абонентов (каналов связи) проводится исходя из "ранга" сети, в данном случае сеть оперативно-тактического уровня – необходимость одно-временного подключения до нескольких сотен абонентов.

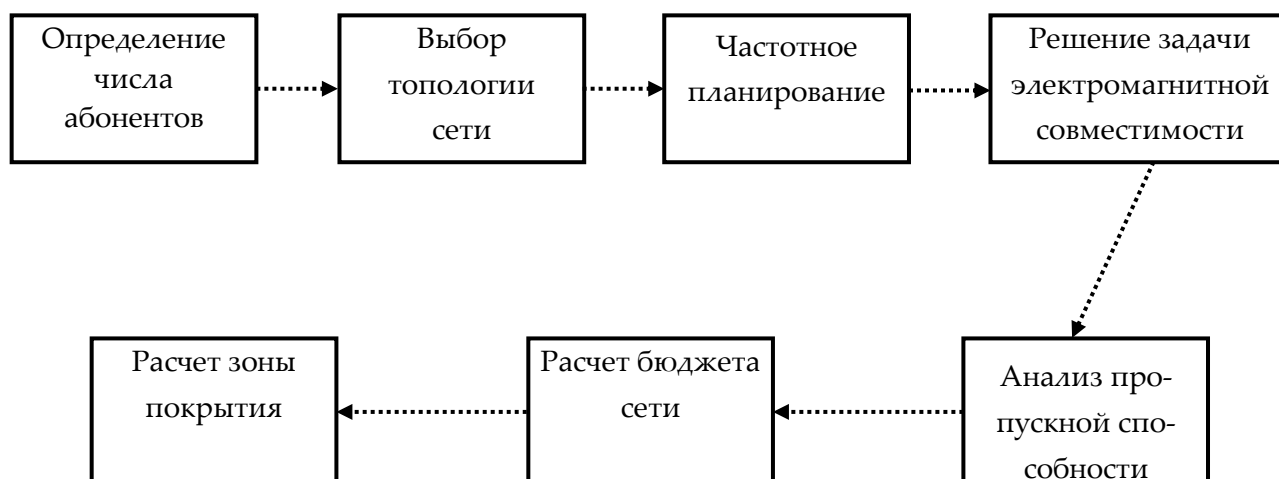


Рис. 3. Формализованный алгоритм планирования радиосети передачи данных

Выбор топологии сети. Понятие структуры сети раскрывает схему связей и взаимодействия ее элементов. При рассмотрении структуры сети выделяют следующие аспекты ее описания: физический, определяющий состав и связи элементов, и логический, отображающий взаимодействие элементов в процессе функционирования сети. Физическая структура сети – это схема связей физических элементов сети: узлов коммутации (УК), оконечных пунктов (ОП) – станций и линий передачи в их взаимном расположении с характеристиками передачи и распределения сообщений. Топологическая структура сети, или просто топология [9], – это обобщенная геометрическая модель физической структуры сети.

Более конкретный состав аппаратно-программных средств и схема их связей называется конфигурацией сети. Топология сети оказывает значительное влияние на основные показатели сети, особенно на надежность и живучесть. На рис. 4 приведены разновидности древовидной топологии [9].

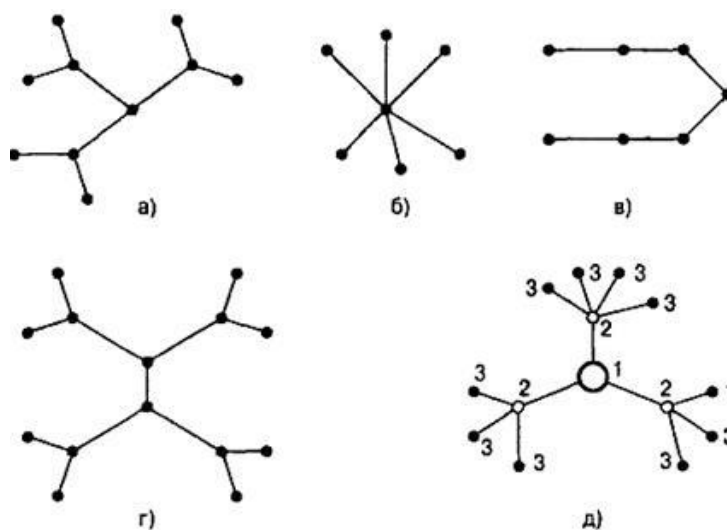


Рис. 4. Особенности древовидной топологии: дерево (а); звезда (б); линейная (общая шина) (в); снежинка (г); узловая с иерархией узлов (д)

Из анализа рисунка следует, что ни один из подходов построения сети не удовлетворяет требованиям повышенной живучести, что особенно актуально при построении систем управления военного назначения. Поэтому для повышения живучести системы управления необходимо применять принцип полносвязной сети (рис. 5), однако для его реализации требуется максимальное число каналов и, следовательно, сеть имеет высокую стоимость.

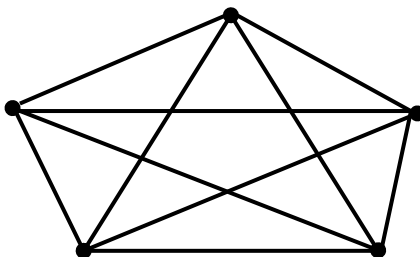


Рис. 5. Сеть с полносвязной топологией

Задача частотного планирования, электромагнитной совместимости и обеспечения максимальной пропускной способности решается за счет применения в сети в качестве несущей хаотических сигналов и MIMO-технологии. Главным способом достижения высокой скорости передачи данных в MIMO-системах является передача данных от источника к получателю через несколько радиосоединений, откуда данная технология и получила свое название [10]. Как показано в работах [10, 11], для организации MIMO-технологии необходима установка нескольких антенн на передающей и на приемной стороне. Под системой в данном случае понимается радиосоединение.

Пропускная способность MIMO-радиосистемы теоретически может быть увеличена (при заданной полосе частот и излучаемой мощности) пропорционально числу используемых антенных каналов по сравнению с обычной системой с одной передающей и одной приемной антеннами [10, 11]. На рис. 6 приведена MIMO-система связи, где в качестве несущего сигнала используется хаотический процесс с разными начальными условиями x_0 для каждого подканала h , состоящая из M передающих и N приемных антенн [8].

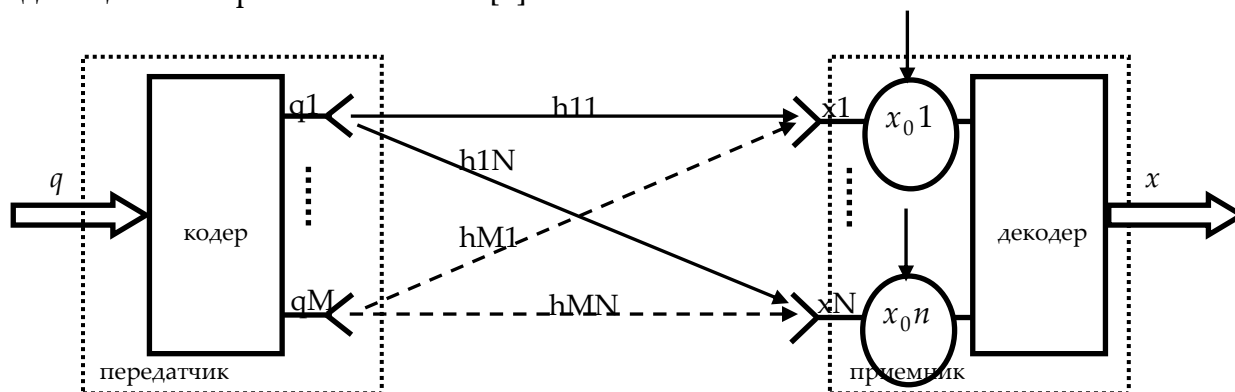


Рис. 6. MIMO-система связи с хаотической несущей

Распространение сигналов описывается $(N \times M)$ -размерной матрицей H , состо-

ящей из коэффициентов передачи $h_{m,n}$ между m -й передающей и n -й приемной антеннами [8]:

$$H = \begin{pmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,N} \\ h_{2,1} & h_{2,2} & \dots & h_{2,N} \\ \dots & \dots & \dots & \dots \\ h_{M,1} & h_{M,2} & \dots & h_{M,N} \end{pmatrix}. \quad (1)$$

На передающей стороне сигнал q кодируется в пространственном кодере и разделяется на несколько потоков, каждый из которых передается в эфир по отдельному подканалу. На приемной стороне несколько антенн принимают сигнал из радиоэфира. Причем антенны на приемной стороне также устанавливаются с некоторым разнесением. Принятые сигналы поступают на приемники, число которых соответствует числу антенн и трактов передачи. На каждый из приемников поступают сигналы от всех антенн системы. Каждый из таких приемников (сумматоров) выделяет из общего потока только энергию сигнала, настроенного на свое значение x_0 .

Расчет бюджета сети. При проектировании сети передачи данных необходимо решить вопрос, насколько далеко приемник и передатчик абонентской и базовой станций могут находиться друг от друга, чтобы уровень качества связи при этом не падал ниже требуемого. Для ответа на этот вопрос в первую очередь необходимо рассчитать максимальное затухание радиосигнала на трассе, или бюджет радиолинии. На рис. 7 приведен упрощенный вариант построения стеганографической сети передачи данных оперативно-тактического уровня на основе ММО-технологии на хаотических несущих.



Рис. 7. Стеганографическая сеть передачи данных оперативно-тактического уровня на основе ММО-технологии с хаотическими несущими (упрощенный вариант построения)

Стеганографическая сеть передачи данных состоит из командного пункта (сер-

вера), информационно-измерительных систем, средств разведки, средств радиоэлектронной борьбы, наземных и воздушных средств огневого поражения. Информация в сети циркулирующая на множестве ортогональных хаотических сигналов x_0, y_0, z_0, c_0, v_0 в реальном масштабе времени поступает на командный пункт. На основании этого на командном пункте (который в свою очередь включен в более глобальную информационно-коммуникационную сеть) производится оценка боевой обстановки и выдача команд управления соответствующим звеньям сети (например средствам огневого поражения). Для возможности одновременного приема и выдачи информации всем абонентам сети командный пункт организован по принципу ММО-технологии.

В контексте анализа канала связи и оценки его бюджета рассмотрим более подробно одно из звеньев сетевых радиосвязей – радиолинию "командный пункт – беспилотный летательный аппарат (БПЛА)", приведенную на рис. 7.

Для удовлетворения требований к пропускной способности канала связи при передаче как данных телеметрии, так и разведывательных данных с борта БПЛА, а также для скрытия самого факта передачи информации, необходимо расширять полосу частот приемопередающего оборудования, применять шумоподобные (хаотические) сигналы в качестве несущей. Или использовать спектрально-эффективные методы модуляции гармонической несущей (например, хаотическую MSK-модуляцию [12]).

Как показано в работе [13], максимальная дальность радиосвязи определяется по формуле:

$$r_0 = 3,57(\sqrt{h_1} + \sqrt{h_2}), \quad (2)$$

где r_0 – максимальная дальность радиосвязи, км; h_1 – высота антенны на командном пункте, м; h_2 – высота полета БПЛА, м. При $h_1=10, h_2=50, r_0=30$, что соответствует оперативно-тактической глубине проведения боевой операции.

Проведем расчет бюджета радиолинии для дальности связи 30 км между командным пунктом и БПЛА. Оценим затухание радиосигнала на трассе [14]:

$$L = 20 \log_{10} \left(\frac{4\pi D}{\lambda} \right), \quad (3)$$

где L – потери на распространение в свободном пространстве, дБ; D – расстояние между приемником и передатчиком, м; λ – длина волны, м. Для $\lambda=0,1$ (диапазон 3 ГГц), $D=3 \cdot 10^4, L=131$.

Для расчета бюджета радиолинии также необходимо учитывать дополнительные параметры, такие как мощность передатчика, чувствительность приемника, усиление антенны и т.д., значение которых примем равными усредненным параметрам "классических" авиационных бортовых и наземных радиостанций, таких как Р-832, Р-833, Р-845 и т.д.

С целью анализа бюджета радиолинии сведем полученные данные в табл. 1.

Таблица 1. Анализ бюджета радиолинии

Параметр	Усиление / ослабление (дБ)	Σ
Дальность связи	30 км	–
Диапазон	3 ГГц	–
Мощность передатчика КП	30	–
Потери в фидере	-1,5	28,5
Усиление антенны	24	52,5
Затухание радиосигнала	-132	-79,5
Усиление антенны БПЛА	2	-77,5
Потери в фидере БПЛА	-1,5	-79
Чувствительность приемника БПЛА	-90	11
Бюджет радиолинии	–	11

Из анализа табл. 1 следует:

- радиолиния имеет запас бюджета связи +11 дБ, что позволяет увеличить дальность связи;
- для организации связи между КП и БПЛА необходимо иметь наземную антенну с большим коэффициентом усиления;
- для обеспечения скрытности функционирования радиолинии (работе "под шум") необходимо адаптивно понижать выходную мощность передатчика и повышать чувствительность приемника.

Следует также отметить, что при расчете бюджета радиолинии не учитывались такие важные факторы, как шум канала связи и радиоэлектронное противодействие противника.

Выводы

Применение хаотических сигналов в качестве несущей позволяет обеспечить скрытие факта передачи информации за счет схожести их статистических и динамических характеристик с аналогичными характеристиками шума наблюдения. Что в свою очередь позволяет применять хаотические сигналы для повышения скрытности функционирования систем передачи информации. Для решения задачи разделения абонентов (обеспечения многоканальности по виду сигнала) и обеспечения высокой скорости передачи данных (что особенно актуально при обмене информацией в режиме реального времени) целесообразно применять ММО-технологии.

Идея использования хаотических сигналов и ММО-технологии теоретически позволяет синтезировать стеганографическую сеть передачи данных. Стеганографическая сеть передачи данных на уровне формирования и обработки сигнала должна быть реализована как программно-определяемая радиосистема, что позволяет в зависимости от условий прохождения сигнала на трассе адаптивно изменять виды модуляции, выходную мощность передатчика, виды канального кодирования сигнала, параметры

расширения спектра сигнала, скорость передачи данных, соотношение времени передачи и приема для каналов связи, параметры шифрования передаваемых данных.

Изложенный подход может быть реализован при создании единого информационно-коммуникационного пространства в системе скрытого управления войсками, организованной по сетевому принципу. Такая сеть создает в пространстве шумовое поле, сформированное множеством хаотических несущих, что значительно затрудняет при радиоразведке правильную классификацию источников излучения.

Список литературы:

1. Васюта К. С. Особенности построения стеганографических систем радиосвязи [Электронный ресурс] / К.С. Васюта, С.В. Озеров, А.Н. Королюк // Проблемы телекомунікацій. – 2012. – № 3 (8). – С. 94 – 104. – Режим доступа до журн.: http://pt.journal.kh.ua/2012/3/1/123_vasuta_sten.pdf.
2. Основы комп'ютерної стеганографії: Навчальний посібник для студентів і аспірантів / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця: ВДТУ, 2003 – 143 с.
3. Грибунин В.Г. Цифровая стеганография/ В.Г. Грибунин, В.Н. Оков, И.В. Туринцев. – М.: Солон-пресс, 2002. – 272 с.
4. Васюта К.С. Анализ эвристических моделей информационных систем на хаотической несущей // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2009. – № 156. – С. 17-22.
5. Васюта К.С., Малышев А.А., Зоц Ф.Ф. Анализ корреляционных свойств хаотических радиоимпульсов // Системи обробки інформації. – 2012. – Вып. 3 (101), т.2. – С. 22-25.
6. Костенко П.Ю., Васюта К.С., Барсуков А.Н. Использование BDS-статистики для оценки скрытности сигнала, полученного перемешиванием хаотической несущей // Известия вузов. Радиоэлектроника. – 2010. – № 5 (53). – С. 41-45.
7. Васюта К.С., Озеров С.В., Малышев А.А. Повышение скрытности передачи бинарного сообщения в прямохаотической системе радиосвязи за счет фильтрации хаотической несущей // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2013. – Вып. 2(35). – С. 78 – 81.
8. Васюта К. С. Метод повышения пропускной способности и скрытности системы радиосвязи путем применения ММО-технологии на хаотических несущих / К.С. Васюта, С.В. Озеров, Ф.Ф. Зоц, Н.А. Глуценко // Системи управління, навігації і зв'язку. – К.: "ДП" ЦНДІ Н і У, 2012. – Вып. 3(23). – С. 223–227.
9. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. – С.Пб.: Питер, 2013. – 944 с.
10. Gershman A.B. Space-Time Processing for MIMO Communications. – Wiley&Sons, 2005. – 370 p.
11. Paylraj A., Nabar R., Gore D. Introduction to Space-Time Wireless Communications. – Cambridge University Press, 2003. – 277 p.
12. Васюта К.С. Повышение скрытности хаотического сигнала путем применения MSK-модуляции / К.С. Васюта, С.В. Озеров, А.М. Королюк // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУПС, 2013. – Вып. 3(12). – С. 115 – 117.
13. Долуханов М.П. Распространение радиоволн. – М.: Связь, 1972. – 336 с.
14. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Издательский дом Вильямс, 2003. – 1104 с.