DYNAMIC-CHAOS INFORMATION TECHNOLOGIES FOR DATA TRANSMISSION, STORAGE, AND PROTECTION

Yuri V. Gulyaev, Rostislav V. Belyaev, Georgy M. Vorontsov, Nikolay N. Zalogin, Valerii I. Kalinin, Erast V. Kal'yanov, Vladimir V. Kislov, Vladimir Ya. Kislov, Vladimir V. Kolesov, Evgeny A. Myasin, Evgeny P. Chigin

Kotelnikov Institute of Radioengineering and Electronics of RAS, http://www.cplire.ru
Moscow 125009, Russian Federation

gulyaev@cplire.ru, belyaev@cplire.ru, info@cplire.ru, zal.dunin@mail.ru, val.kalinin@mail.ru, kalianov@ms.ire.rssi.ru, info@cplire.ru, kvv@cplire.ru, eam168@ms.ire.rssi.ru, chigin@cplire.ru

Abstract. **Information technologies based on dynamic chaos are considered. Their promising applications in data transmission, processing, storage, and protection are reviewed. Wideband data transmission channels that use complex signals with a large processing gain produced by dynamic chaotic systems are described. Finitedimensional mathematical algorithms are proposed for calculation of chaotic signals by reconstructing nonlinear dynamics in dissipative systems with delay. It is shown that a digital data transmission system with spread spectrum and dynamic code escape exhibits high noise immunity and security, is electromagnetically compatible with other devices, and guarantees reliable and confidential data transmission in a complex electromagnetic environment. Schemes of data masking, protection, processing, and transmission are implemented in original chaotic algorithms.**

Keywords: **information technologies, dynamic chaos, broadband systems, algorithms for computing chaotic signals, dissipative systems with delay, noise immunity, security**

UDC 004.93, 621.391

Bibliography - 45 references *Received 16.06.2003* [1]

RENSIT, 2018, 10(2):279-312 **DOI: 10.17725/rensit.2018.10.279**

Content

1. INTRODUCTION

In classical radiophysics, noise was always attributed to thermal and shot fluctuations. The frequency spectrum of electromagnetic oscillations generated by an oscillator was believed to be enriched by harmonics or subharmonics of the fundamental frequency, and a finite width of the oscillator spectrum line was explained by the fluctuation effect. Therefore, noise oscillation generation discovered in the Institute of Radio Engineering and Electronics of the Russian Academy of Sciences (IREE RAS) could not have been expected by radio physicists [1]. The intensity and frequency band of noise produced by plasma and travelling-wave tube (TWT) electron devices could not be attributed to the fluctuation effect. The nature of generation of such intensive oscillations was successfully explained using the methods of nonlinear dynamics in self-oscillatory systems with delayed feedback. Virtually at the same time, using a substantially simplified model of convective instability of the Earth's atmosphere, Lorentz demonstrated the possibility of chaotic oscillation generation [2].

Development of mathematical concepts describing possible emergence of complex nonperiodic motions in dynamic systems was begun long ago by Poincare, who introduced the notion of homoclinic paths as applied to the problem of motion of three interacting bodies [3].

Later studies showed that complex irregular motions are no less typical of a wide class of dynamic systems than classical regular processes. It was striking that such motions were possible in dynamic systems with a small number of degrees of freedom. It had intuitively been assumed that a complex chaotic motion could emerge in systems with an infinite or very large number of degrees of freedom. This was the assumption involved in the model of hydrodynamic system turbulent motion developed by Landau in 1944 [4]. Revealing the complex chaotic character of motion of a dynamic system with a small dimension seemed to be a nontrivial problem.

Since the early 1960s, researchers of IREE RAS conducted investigations on designing microwave oscillators with direct noise modulation to facilitate solving problems of electronic warfare. At that time, the original idea of a noise generator based on a ring self-oscillatory system consisting of an O or M microwave amplifier and a special nonlinear element providing for stochastization of generated oscillations. (This generator is referred to as a shumotron.) Such devices were implemented using TWTs or plasma, and, later, the idea was realized in semiconductor transistor and diode oscillators [5-12].

In the late 1970s, numerous studies aimed at revealing chaotic motion in various structures and media were published, which resulted in classifying scenarios of monochromatic oscillation conversion into chaos in various dynamic systems. Within the expanded research area, the concepts developed were generalized and the laws that govern the emergence of chaotic motion were revealed. Finally, the concept of strange attractor as the representation of dynamic system motion in its phase space was originated. At present, the notion of dynamic chaos is identified with the notion of strange attractor, introduced by Ruell and Takens [13]. A specific feature of dynamic system motion on a strange attractor is that, in the phase space of a system, its trajectories are attracted to a stable Cantor set with a fractal dimension rather than to a limit cycle or torus, which have integer-valued dimensions [14]. Earlier, complex dynamics in conservative systems was reported by Zaslavskii and Chirikov [15].

In the subsequent studies, increasingly wide classes of dynamic systems (natural systems, representing natural phenomena; mathematical models; and technological systems) exhibiting dynamic chaos effects were discovered. The laws that govern transitions to chaos and conditions providing for chaotic motion were established [16].

Chaotic motion of dynamic systems exhibits certain specific features. Realizations of this motion are characterized by a continuous power spectrum in a frequency band, an exponentially decreasing autocorrelation function, and the Gaussian probability distribution. At the same time, dynamic chaotic systems exhibit pure dynamic properties, such as an extremely high sensitivity to initial conditions and, associated with it, exponential divergence of close trajectories.

Previously, mechanisms of forming dynamic system chaotic motions were analyzed using radiophysical and radio-electronic systems. These results showed that chaotic properties of dynamic systems could find applications. A topical line of investigations is searching new technologies that employ specific features of dynamic systems operating in the dynamic chaos state. Studies in this research area have initiated a number of novel investigations in various fields, including informatics, biophysics, chemistry, medicine, and dynamics of natural phenomena (e.g., earthquakes) [16].

A promising direction is research aimed at developing novel telecommunications systems based on chaotic dynamics. Chaotic dynamics of systems provides for the possibility of producing complex oscillations by devices of a simple structure, generation of a large number of various chaotic modes by a single device, a high information capacity, a wide variety of methods for introducing an information signal into a chaotic one, transmitter-receiver synchronization, and data security. This diversity of chaotic properties of dynamic systems has initiated various applications of chaotic modes of dynamic systems to support communications services [17]. Development of new classes of algorithms based on chaotic dynamics and used to form sequences that behave like random processes is of considerable importance [18-21]. These algorithms offer promise in developing novel information technologies and applications of chaotic signals to data transmission, processing, storage, and protection.

2. DATA CARRIERS BASED ON CHAOTIC ALGORITHMS

The search for information carriers (processes and signals) with an increased information capacity and mathematical algorithms that generate such processes is the most urgent task in the development of new information technologies. The basic concept in the field of information technology is "information coding", usually interpreted as a synonym for "information representation". Such carriers of information can be graphics (pictures), texts, musical notations, numbers, sequences of electromagnetic, optical or other signals.

The term "information systems" includes all devices that provide the receipt, processing, transmission and storage of information. These are various sensors that transform external influences (sound, image in the form of a light field of various local intensity, pressure, temperature, chemical composition of the environment, etc.) into electrical signals, electronic systems for converting and processing signals based on computer technology and this means of radio communication and telecommunications . The information in these systems is recorded either in the form of a continuous electrical signal - an analog form of information coding, or as a sequence of electrical pulses - a digital encoding form. With analog coding, the necessary information is transmitted by the corresponding amplitude or frequency of oscillations of the continuous electrical signal. In digital form, information is expressed in the form of a binary code specified by an electrical pulse, for which, for example, the logical state "0" corresponds to the absence of an electrical voltage (or current), and the state "1" is its presence. Digital codes due to good protection from errors and interference, high processing speeds in computer systems and high transmission density over communication channels are prevalent in modern information systems.

A. Discrete Generating Algorithms of Chaotic Signals Forming

It is well known in the information theory that stochastic signals generated by random processes are characterized by the highest information capacity. The main problem involved in the development of data carriers in digital telecommunications channels is to generate random binary sequences using a short driving key. Mathematical algorithms forming pseudorandom number sequences using a key must exhibit the following properties.

(i) The nonperiodic segment of a pseudorandom sequence obtained may have an arbitrarily large length.

(ii) A number sequence must be statistically similar to a purely random sample.

(iii) A random number generator could be implemented using soft hardware so as to be applied in a communications channel with the corresponding operation speed.

Despite the fact that there are numerous algorithms of pseudorandom sequence (PRS) generation, binary PRSs are actually produced using a recurrent algorithm. According to this algorithm, a recurrence relationship and certain initial conditions are employed to construct an infinite sequence each of whose terms is determined from the previous ones. Binary sequences obtained from recurrence relationships are simple to program and implement by hardware using high-speed multibit binary shift registers.

Attempted adaptation of operations with real numbers for digital algorithms has failed, because the statistics of a sequence obtained is severely changed upon the replacement of a real number by its approximation. Rounding off results in an unpredictable perturbation of a generating algorithm, so that the sequence obtained becomes no longer statistically independent and, hence, random.

At present, the most widespread method of constructing PRSs is formation of M sequences (sequences with the maximum period) using shift registers, when the number value at a given instant is determined by linear relationships weighted (with a code) with respect to the previous terms of the sequence. The weighting factors are selected so as to provide a rapid decrease of the correlation function to values of about $1/\sqrt{N}$, where N is the period length of an M sequence. The most substantial drawback of this method is the absence of mathematical tools for constructing algebraic polynomials of arbitrarily high degrees that generate sequences with the maximum period. Moreover, information on high-degree polynomials suitable for antinoise coding is extremely confidential.

Well-known classes of PRSs, both linear (*M*, Hadamard, Gold, Kasami, etc., sequences) and nonlinear (Legendre, bent, etc., sequences) have certain drawbacks and do not meet some of the requirements mentioned above. The solution of the problem can be facilitated by using noiselike signals (NLSs) formed by nonlinear dynamic chaotic systems. Exhibiting correlation properties no worse than those of *M* sequences, such NLSs have virtually arbitrary lengths, can form ensembles of signals with large information content, and are nonlinear, which impedes their recognition necessary for subsequent signal reconstruction.

All known dynamic systems with a small number of degrees of freedom that exhibit dynamic chaos (a strange attractor), such as the Lorentz and Rossler attractors, Chua systems, and ring systems with delay and pure amplitude nonlinearity, do not ensure correlation functions with necessary parameters either.

Efficient statistical properties are typical of dynamic systems with the dissipative (amplitude) and reactive (phase) kinds of nonlinearity observed simultaneously. Due to the presence of a nonlinear phase in self-oscillatory systems with phase nonlinearity, the phase balance and mode synchronization are disturbed. During oscillation chaotization, intraspectrum couplings become weaker and correlations in the generated signal are split more rapidly than in other self-stochastic systems. Signals with efficient correlation properties can be produced in nonlinear ring systems with delay that simultaneously exhibit the active (amplitude) and reactive (phase) kinds of nonlinearity. A block diagram of such a system can be represented by a ring consisting of three blocks (**Fig. 1**).

The self-oscillation process in this system is described by the complex integral equation taking into account the effect of all functional blocks:

$$\hat{x}(t) = \int_{-\infty}^{t} g(t-\tau)\hat{F}(\tau - T)d\tau, \qquad (1)$$

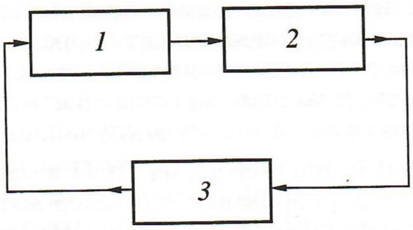

Fig. 1. *Model dynamic chaotic system: 1 - nonlinear amplifier; 2 - delay line; 3 - filter.*

Introducing rectangular signal filtering and expanding functions g and $\hat{F}$ in the orthogonal Kotel' nikov series, Eq. (1) can be modified to the discrete form:

$$\hat{x}_k = (1-\exp(-h))\hat{F}_{k-N_z} + \exp(-h)\hat{x}_{k-1}, \qquad (2)$$

after some algebra. Here, $\hat{x}$ = $a$exp (iφ), $\hat{F}_k$ = $F(a_k)$exp[φ_k + $\Phi(a_k)$], N_z is the delay parameter, and h is the sampling interval determined according to the Kotel'nikov-Shannon theorem [22]. Nonlinear functions $F(x)$ and $\Phi(x)$ responsible for the amplitude and phase transformations govern the oscillation stochastization process in the dynamic system considered. They may appear rather complex depending on the type of nonlinear amplifier. A steep slope of the phase characteristic with respect to the signal value at the nonlinear element input guarantees necessary statistical properties of the signal. Simulations have yielded the system parameters that provide for developed chaos of selfoscillations and a rapidly dropping signal autocorrelation function (ACF).

Calculations of the cross-correlation function (CCF) have shown that the CCF and ACF exhibit similar behavior, and the most pronounced spikes decrease as the sample duration increases as $\alpha / \sqrt{N}$.

There are two possibilities of producing binary signals in the process of realizing the new class of signals used in digital communications, which is mainly based on binary coding. One method involves clipping multilevel signals that are calculated. Simulations have shown that quantization of a multilevel signal does not deteriorate its correlation properties.

The other method represents direct construction of discrete self-oscillatory systems. Thus, in a discrete self-oscillatory system, an algorithm of obtainino 0 a binary signal can be described by the relationship

$$x_k = \mathrm{sgn}[F(x_{k-N})] + x_{k-1}, \qquad (3)$$

which follows from Eq. (2).

Based on the mathematical model of a rino selfoscillatory system with pronounced amplitude-phase nonlinearity, filtering, and delay, a discrete algorithm generating a chaotic signal is developed and investigated. This algorithm is classified as a recurrent-parametrical algorithm with delay. Generally, this algorithm can be represented as the discrete functional transformation (mapping):

$$x_n = f(x_{n-1}, x_{n-2}, ..., x_{n-N_\zeta}), \qquad (4)$$

where x_n and x_{n-1} are the PRS term being calculated at the nth step and the previous term calculated at the $(n - l)$th step, respectively; N_ζ is the delay parameter equal to the number of the sequence terms on the delay interval $(x_{n-1}, x_{n-2}, ... , x_{n-N\zeta})$, which completely determine new value x_n and must be specified as the initial condition at the first step; and function $f(x)$ describes amplitude and phase transformations in the generatino ring self-oscillatory system operating in the chaos mode. Defined on set M of natural integers belonoino to a closed number interval $[M_1, M_2]$, where $M_2 > M_1$ and $M = M_2 – M_1 + 1$, the algorithm forms a virtually uncorrelated PRS of integers with a probability distribution that is close to uniform and correlation characteristics satisfying the requirements of coding signals.

The mapping specified by an algorithm with time delay may bring new value x_n out of domain of the algorithm $[M_1, M_2]$. Therefore, formula of the algorithm (4) must be completed with a special operation that returns value x_n of each calculated term of the sequence to a given number interval when this value falls beyond the interval limits. These self-mappings of a numerical set (e.g., the baker's transformation [14]) are well known. Other transformations are also possible. However, the transformations that do not substantially change the distribution of generated numbers must be emphasized.

B. Reconstruction of nonlinear dynamics for a system with delay

According to the theorems on nonlinear dynamics reconstruction in the space of embeddings [23], there is a one-to-one finite-dimensional mapping for an original infinite-dimensional system with delay. However, the theorems on nonlinear dynamics reconstruction do not provide for a general method that can be applied to construct finite-dimensional diffeomorphic mappings. Using the method of nonlinear dynamics reconstruction, one can determine the minimum dimension of a new dynamic system, which may exceed the fractal dimension of an original chaotic attractor by a factor greater than two.

To develop discrete mathematical algorithms (based on self-oscillatory systems with delay) for forming wideband chaotic signals, one has to find a finite-dimensional representation of strongly unbalanced nonlinear dynamics. We consider dissipative dynamic systems such that their initial volume in the phase space is contracted. An important feature of dissipative systems with delay is the convergence of bounded trajectories to finite-dimensional manifolds in the original phase space with a quadratic metric [25].

In infinite-dimensional dynamic systems with delay, chaotic attractors have a finite fractal dimension [26]. The method of nonlinear dynamics reconstruction provides for finite-dimensional description of finite trajectories on an original chaotic attractor [24].

The behavior of numerous dynamic systems with delay is determined by the general first-order differential equation:

$$dx(t)/dt = \Phi[x(t); x(t – T); \mu], \qquad (5)$$

where Φ is a nonlinear operator, T is the delay time, and μ is the control parameter. Each state of dynamic system (5) is specified by continuous trajectory $x_k(\tau)$ on the kth time interval, $t = kT + \tau(0<\tau\leq T)$, of lenght T. The set of all chaotic trajectories x_k of length T represents attractor $M(T) = \{x_k\}$ in infinite-dimensional phase space L^2 (T) of the original system (5).

In space of continuous functions $L^2(T)$, let us introduce a root-mean-square (rms) metric and define the distance between arbitrary functions as

$$\rho(x_k, x_m) = \left\| x_k - x_m \right\|. \tag{6}$$

The norm of each function is assumed to be bounded.

An important feature of a dissipative system with delay is the convergence of bounded trajectories to finite-dimensional manifolds in original phase space $L^2(T)$ with a quadratic metric.

Let compact manifold M^D of an integer dimension (D_C) contain chaotic attractor $M(T) = \{x_k\}$ with fractal dimension $D \geq D_C$. Then, according to the embedding theorem, chaotic attractor $M(T) = \{x_k\}$ can be projected onto subspace M^N with the embedding dimension $N \geq 2D + 1$ by a one-to-one mapping [27].

In a finite-dimensional form, motions on a chaotic attractor can be described in reconstruction space M^{2D+1} using $N = 2D+1$ new dynamic variables. To find these variables, we employ the well-known procedure of orthogonally projecting continuous functions onto finite-dimensional subspaces [28].

If basis $\{\varphi_i(\tau);\ i = 1, 2, ..., N\}$ consisting of orthonormal functions (for example, weighting functions with a shift on a finite time interval T) is chosen in $L^2(T)$, the time shift for neighboring basis functions is determined by the ratio of the delay time in the system to the embedding dimension:

$$\Delta\tau = T/(2D + 1) \tag{7}$$

Let us construct linear functional subspace M^{2D+1} spanned over system of basis functions $\{\varphi_i\}$. Orthogonal projection of chaotic functions $\{x_k(\tau)\}$ belonging to $L^2(T)$ onto subspace M^{2D+1} yields:

$$\tilde{x}_k(\tau) = \sum_{i=1}^{2D+1} x_k(i)\varphi_i(\tau). \tag{8}$$

Here, numerical coordinates $x_k(i)$ of function $\tilde{x}_k(\tau)$ developed in system of basis functions $\{\varphi_i(\tau);\ i = 1, 2, ..., N\}$ are represented as the scalar product:

$$x_k(i) = (x_k, \varphi_i) = \int_0^T x_k(\tau)\varphi_i(\tau)d\tau. \tag{9}$$

According to the Takens theorem on nonlinear dynamics reconstruction [24], representative function . $\tilde{x}_k(\tau)$ is a one-to-one projection in space M^{2D+1} for original chaotic function $x_k(\tau)$.

Set of numerical coordinates $\{x_k(1), x_k(2), x_k(2D + 1)\}$ determines $(2D + 1)$-dimensional vector X_k in reconstruction space $\Re^{2D+1}$.

Being specified by scalar product (9) with weighting functions $\{\varphi_i\}$, the coordinates of vector $X_k = \{x_k(i)\}$ generally differ from samples of a chaotic trajectory. Numerical coordinates (9) can be calculated using orthogonal development (8) in basis functions $\{\varphi_i\}$ defined on a finite time interval T, which requires considerable computational effort. However, dimension $(2D + 1)$ of reconstruction space $\Re^{2D+1}$ is the minimum one according to the Takens reconstruction theorem [24].

The coordinates of vector $X_k = \{x_k(i)\}$ are determined at discretization interval (7) equal to the ratio of delay time T in dynamic system (5) to the embedding dimension $(2D + 1)$. Expression (7) specifies the maximum discretization interval involved in the finitedimensional representation of original trajectories $x_k(\tau)$. Here, D is the dimension of a compact set containing the original chaotic attractor for dynamic system (5).

Thus, lower boundary N of the embedding dimension is found using the reconstruction methods of nonlinear dynamics:

$$N = 2D + 1. \tag{10}$$

This boundary is greater than double fractal dimension D,. of the chaotic attractor [29]. The value of the manifold dimension ($D \geq D_C$) is the nearest integer-valued complement for fractal dimension D_C of the chaotic attractor. Maximum discretization interval $\Delta\tau$ is determined by the lower boundary $N = 2D + 1$ for embedding dimension according to formula (7). This result is of practical importance for constructing discrete mathematical models. Finite-dimensional nonlinear algorithms provide for one-to-one description of chaotic infinite-dimensional dynamic system with delay (5) if their dimension is greater than the double fractal dimension of the original chaotic attractor.

C. Synthesis of a chaotic code set

Identifying transmitted messages by a native chaotic code formed of m initial conditions for the chaotic trajectory

$$X_0 = \{x_0(h), x_0(2h), \ldots, x_0(mh)\}^T \tag{11}$$

enables one to realize code division and code addressing for all users in a telecommunications network.

The processing gain of a chaotic signal is the number of discrete samples n used to transmit one bit of useful information. During data transmission, chaotic signal processing gain n may have an arbitrary value relative to embedding dimension m. Actually, the chaotic signal processing gain is specified by the data transmission rate and duration h of a single elementary symbol contained in a chaotic code. Chaotic signal processing gain n is an important parameter. It determines the actual information content of a chaotic signal system and characterizes the noise immunity of a spread-spectrum communications system.

A large ensemble of chaotic binary codes is formed using the following simple mathematical algorithm

$$\begin{aligned} y_k &= sign[F(x_k)], \\ x_k &= (1-\exp(-h))sign[F(x_{k-m})] + \exp(-h)x_{k-1}, \end{aligned} \tag{12}$$

which enables one to calculate chaotic processes in a highly unbalanced system with delay [19].

Here, parameter h denotes the sampling step in the Kotelnikov-Shannon theorem and integer m determines the number of samples on the delay interval in system (12), which represents the embedding dimension for a set of chaotic codes according to the Takens theorem on nonlinear dynamics reconstruction [24].

In a wide sense, coding is considered to mean data representation in a form suitable for transmission over a communication channel. The coding procedure involves one-to-one representation of transmitted data by n-dimensional signals of n-dimensional redundant set M_n. The power of set M_n, or the number of code sequences of duration n, is determined by the quantity $C = b^n$, where b is the code base.

Chaotic code sequences are formed using the nonlinear algorithm with retarded argument described by (12). In a given domain of control parameters, generating algorithm (12) exhibits strongly unbalanced chaotic dynamics. Each message is transmitted via a unique chaotic code combination of n binary symbols, which is never repeated.

In original space M_n, the distance between arbitrary binary codes $Y_k = (y_{1k}, y_{2k}, \ldots, y_{nk})$ and $Y_l = (y_{1l}, y_{2l}, \ldots, y_{nl})$ is specified by Hamming metric $d(Y_k, Y_l)$, indicating the number of symbol mismatch positions for a fixed pair of codes. Synthesis of a system of optimum chaotic codes involves choosing subset U_n out of entire set of chaotic codes M_n. The number

$$D = \min d(Y_k, Y_l), \tag{13}$$

where function $d(Y_k, Y_l)$ is minimized over distances between the codes of subset U_n, is referred to as the code distance of subset U_n.

The code distance of subset U_n is the distance between the two closest code sequences.

Chaotic codes $Y_k = (y_{1k}, y_{2k}, ... , y_{nk})$ of large length n are not replicated. The analysis of a chaotic code set shows that the code distance of the entire set increases with the code length and approaches half its value [30].

Long chaotic codes are distributed over the Hamming space so that they are virtually equally spaced by half a code length. Mutual dispersion of chaotic codes is caused by local instability and subsequent mixing of chaotic trajectories in an original dynamic system with delay whose behavior is described by (5). Quasi-equidistant distribution of long chaotic codes indicates that the code group properties approach the properties that are optimum in terms of the Hamming metric [30].

Chaotic code y_k is completely reproduced in a receiver when m initial sample values are exactly specified to start generating algorithm (12). Even a small error in specified initial sample values results in the exponential divergence of perturbed and specified trajectories. After a short time interval, the perturbed code becomes entirely different from the specified one and, therefore, cannot be used to recover transmitted data. The set of m initial samples exactly specified deter-mines the subscriber's identifier and represents a key to confidential data recovery.

Thus, theoretical investigations and simulation of systems with chaotic dynamics can facilitate development of novel information technologies providing for information resource security. Chaotic algorithms can be simulated to construct a large system of complex NLSs, characterized by a high processing gain, or chaotic key codes. Dynamically varying chaotic codes make it impossible to disclose information resources of open telecommunications systems in real time. Development of discrete mathematical models can also provide for a fundamentally new technology of cryptographic closing of information resources.

3. WIDEBAND TELECOMMUNICATIONS SYSTEMS BASED ON DISCRETE CHAOTIC ALGORITHMS

Telecommunications systems of the new generation, employing wideband signals (WBSs) with a large information capacity, ensure an increase in the information rate and exhibit enhanced performance stability in the presence of disturbances [31, 32]. Information transmission over multichannel code-division systems, wireless spread-spectrum communications systems, etc., use WBSs. Radiation of NLSs that are temporally continuous and have an extremely low spectral density enables one to receive information at a signal-to-noise ratio much less than unity, provides for multipath mitigation, reduces the effect of numerous types of interferences, and guarantees high-level communication security and electromagnetic compatibility with other electronic devices.

Designing of narrowband digital communications channels is impeded by the necessity of compromising between contradictory requirements. Multiuser communications systems must provide for a necessary spectrum efficiency measured in bits per second for one hertz. High-quality data transmission necessitates applying high-speed coders and a coding method that guarantees error detection and correction. These requirements imply that redundant information must be introduced into transmitted data, which even increases the channel bandwidth.

Currently, development of alternative wideband and ultrawideband personal wireless channel is in progress. A spread spectrum is obtained with nonsinusoidal signals, such as noiselike carriers, ultrashort video pulses, etc.

Because of the current explosion of multichannel autonomous communications and code-division data transmission systems, the problem of producing NLS systems still is extremely urgent. A set of signal determined by a single construction rule (algorithm) is referred to as a signal system. The number of signals in system *L* is called the system size, which is typically compared to NLS processing gain *B,* equal to the band-width-duration product: $B = \Delta fT$, where Δf and *T* are the signal bandwidth and duration, respectively. At $L << B$, $L \approx B$, and $L >> B$, the system is referred to as a small, normal, or large signal system, respectively. Construction of large systems of phase-modulated (FM) NLSs with good correlation properties is a challenging task [32].)

The most widespread modem method of producing NLSs involves the formation of *M* sequences based on shift registers with linear feedbacks.

It is well known that NLS communications systems are efficient when they employ signals exhibiting certain features summarized below.

(i) The signal must be wideband; i.e., $B = \Delta fT >> 1$.

(ii) The noise spectral density must be uniform over the communications channel bandwidth.

(iii) The signal ACF must have a single narrow peak and low side spikes.

(iv) The signal must form code sequences satisfying the following criteria for randomness:

(a) the code must be balanced; i.e., the numbers + 1 and -1 must coincide;

(b) the probability of a block consisting of *k* identical symbols must be close to $1/2^k$ (for a binary code). This criterion resembles the requirement for the absence of excess with respect to the Gaussian distribution in a multilevel signal.

(v) The signal must the reproduced at the receiving terminal of a communications system.

(vi) The signal system must consist of signals having (a) equal energies and equal bandwidths and exhibiting (b) low cross correlation.

In addition, some more requirements can be formulated. Thus, the Hamming distance must have the maximum value in the signal space, and the algorithm must be simple enough to reduce computational effort.

This traditional set of nontrivial requirements, for brevity, referred to as good statistical and correlation properties, is implemented in part in current NLS systems.

A. Formation of a Noiselike Carrier in Spread-Spectrum Communications Systems

In recent years, interest in wideband and ultrawide-band data transmission methods has substantially increased. Having a structure suitable for discrete sig-nal transmission, wideband communications channels are digital systems. Wideband wireless considerably differs from traditional communications systems in properties and technological implementation, since it employs signals having a bandwidth much greater than the bandwidth of a transmitted message and uses data reception techniques based on signals of various shapes matched with the shape of a transmitted signal. With these systems, all users employ a single frequency band, which is wider than that with traditional narrow-band frequency-time-division communications systems. In each local loop, its own identification code or code sequence is applied to distinguish between users. In a specified frequency band, a desired signal arrives at an individual user's receiver simultaneously with stan-dard natural interferences and disturbing signals radi-ated by transmitters of other subscribers as well as reflected signals due to multipath propagation effects. Complex electromagnetic environment within the cov-erage of telecommunications systems imposes additional severe requirements on the system of pseudoran-dom signals involved in coding and data transmission over communications channels. The ensemble of code sequences used by various systems or a single multi-channel system must exhibit good cross-correlation and group properties [32].

In designing code division multiple access (CDMA) systems, it is important to properly choose mathemati-cal algorithms generating a large ensemble of PRSs that exhibit necessary statistical and spectral properties and good auto- and cross-correlation characteristics. Spe-cial demands for size must be met by the ensemble of orthogonal PRSs to provide for stable and simultaneous multiuser service within the common spatial coverage. Mathematical algorithms must generate a variety of long statistically independent pseudorandom codes of an extremely intricate structure to guarantee data trans-mission security.

The use of WBSs in data transmission systems offers the following important advantages.

(i) Highly reliable signal reception is ensured at an interference power considerably exceeding the signal power within the signal bandwidth.

(ii) Interference immunity to certain kinds of jam-ming and pulse and narrowband interferences is enhanced.

(iii) Signal resolution is enhanced, and, hence, the efficiency of a communications system is increased in the presence of the multipath propagation effect.

(iv) The possibility of developing asynchronous multiaddress CDMA systems for subscribers using a common frequency band is provided.

(v) The possibility of developing data transmission systems such that direction finding and radiation source tracking are impeded is provided.

As a rule, WBSs are formed by expanding the infor-mation signal bandwidth and (or) spreading the carrier spectrum. The signal bandwidth is usually expanded through carrier modulation so that the bandwidth of the modulated signal is wider than that of the modulating function. A frequency-modulated signal with a large modulation index is a typical example of an expanded-bandwidth signal.

Digital signals with additional antinoise coding also have expanded bandwidths, since the presence of redundant symbols introduced at a fixed information rate necessitates reducing the duration of each symbol. In this situation, the bandwidth of a transmitted coded signal is expanded. Note that simple binary redundant coding complicates the structure of an information sig-nal (especially in the case of highly redundant codes) but does not substantially expand an occupied band-width.

A significant drawback of systems with bandwidths simply expanded via analog carrier modulation (when an information signal is modulated on a carrier) is that they are efficient only at a high signal-to-noise ratio observed across the bandwidths of transmitted and received signals.

This is not the case for spread-spectrum signals. Such signals are formed through modulating a special function on the transmitted oscillation. This function spreads the spectrum and is independent of a transmitted message. As a rule, complex spread-spectrum signals occupy a bandwidth that is wider than the bandwidth expanded using the information signal. A complex spread-spectrum signal can be obtained via amplitude, phase, or carrier frequency modulation. Spectrum-spreading function must be the same for the transmitter and receiver to ensure the inverse transfor-mation (convolution) of the spectrum.

During this procedure, the received signal is demodulated and filtered over the message bandwidth.

An efficient spectrum-spreading function must satisfy certain requirements imposed on the signal bandwidth, receiver structure, and data transmission technique. The spectrum-spreading function must be deterministic. It must have a wide uniform noiselike spectrum (large processing gain) and, hence, a relatively large duration and narrow ACF with low side spikes. The ensemble of various spectrum-spreading functions employed by various systems or a single multichannel system must exhibit good cross-correlation properties.

A spectrum-spreading function may be analog or discrete. However, digital (level- and time-quantized) spectrum-spreading functions are most promising for forming WBSs. These functions are obtained using digital code sequences. Sometimes, the spectrum and signal bandwidth can be expanded simultaneously, for example, when a spectrum-spreading function is combined with digital antinoise coding of messages by restoring codes.

Spread-spectrum signals are divided into coherent and incoherent ones. For example, an amplitude-modulated radio pulse burst represents an incoherent spreadspectrum signal. In this case, information is transferred by the amplitude, and the pulse sequence spreads the spectrum. Another example is a signal with pseudorandom frequency hopping (random frequency hopping from one frequency channel to another). Complex incoherent signals are characterized by the ratio of the signal bandwidth to the information bandwidth (or the information rate). This ratio serves as an equivalent of the processing gain for incoherent signals and determines the gain in noise immunity when WBSs are detected in the presence of noise.

Complex coherent signals are superior to incoherent spread-spectrum signals in most characteristics. However, incoherent signals are simpler for designing both receivers and transmitters (modulators). During reception and processing of a coherent WBS in the optimum receiver, a signal with the processing gain $B >> 1$ is compressed to a simple information signal with the processing gain $B \approx 1$. Time- and frequency- compressed signals are applied. As a rule, the limiting time- and frequency-compression ratios coincide, being equal to the signal processing gain. Physically, a signal is compressed by summing all of the signal spectral components and compensating the differences between their phase shifts, i.e., by coherent summation of all the signal spectral components. After compression, a complex signals is transformed to a simple one (with the processing gain $B \approx 1$) whose bandwidth is about that of the message transferred by this signal. The limiting compression ratio is obtained only in the optimum receiver perfectly matched with the signal.

The basic properties of a complex spread-spectrum signal are determined by the properties of the modulating (spectrum-spreading) oscillation rather than the method of carrier modulation. The ACF of the spectrum-spreading oscillation governs the final bandwidth of a complex signal and uniformity of its spectral density across the bandwidth.

High occupation of the radio frequency band and the necessity of secure and antinoise communications have stimulated development of novel communications systems involving pseudorandom WBS coding. With these systems, all subscribers employ a single frequency band, which is much wider than that employed with traditional frequency-division communications systems, but each subscriber uses his own identification code or code sequence. Standard interferences and fluctuation noise arrive at the input of an individual subscriber's receiver along with the signals of other subscribers and signals due to multipath effects. This circumstance necessitates imposing additional requirements on signal systems involved in information coding and transmission over these code-division communication channels.

It should be emphasized that extremely long nonperiodic PRSs are preferred in coding, which enhances transmitted data security and impedes decoding [31, 32]. The choice of the form of PRSs is of considerable importance for developing a CDMA system. The PRSs employed must exhibit good statistical and correlation characteristics and a wide variety of lengths providing for ensembles of signals transferring a large information content. In addition, their structure must be extremely intricate, ensuring high security of transmitted information.

At present, all of the requirements mentioned above are most completely satisfied by chaotic algorithms describing the behavior of dynamic systems. These algorithms, based on nonlinear procedures with delay, offer the following advantages. They are simple to implement in soft hardware. Only a limited set of initial data uniquely determining the algorithm start is necessary for synchronization. The use of noiselike chaotic signals (NCSs) in wireless communications systems enhances noise immunity and reliability of data transmission in the presence of interferences and distortions and enables one to develop a new approach to the solution of problems of electromagnetic compatibility of various radio facilities.

Operation in the presence of interferences produced by other code groups in the same frequency band is typical of CDMA systems. Therefore, designing of CDMA communications systems necessitates the development of generating algorithms that enable one to construct large signal systems and investigation of statistical and correlation properties of these signals.

B. Formation of a Noiselike Carrier

A noiselike-carrier wireless channel can be formed when, at the transmitting terminal, a spectrum-spreading chaotic pulse sequence generated by a chaotic algorithm is modulated on a microwave sinusoidal signal and then demodulated at the receiving terminal. Phase modulation is the most efficient method of spectrum spreading. It is realized by a phase modulator (a device that changes the phase shift of a transmitted signal). Phase modulators can be classified as follows: according to the principle of operation, into continuous (analog) and discrete (digital); according to the type of connection to the external circuit, into reflective and transmissive (with time delay); and into passive (without signal amplification) and active (with signal amplification). Phase modulators applied in wideband communications systems must ensure a necessary phase shift at minimum loss; a high performance speed; low extraneous modulation; oscillation phase modulation at an admissible power level across a necessary bandwidth; good matching with the microwave section; and stable parameters at a variable input power, microwave section characteristics, and control signal voltages. In addition, these phase modulators must be of a small size and mass.

In digital communications channels, a wide bandwidth is most efficiently provided by a biphase modulator, which realizes two states corresponding to the absence of a phase shift (zero shift) and the π phase shift (a π modulator). Standard microwave phase modulators use a discrete variation of the length of the transmission line between the modulator input and output caused by a control pulse. Thus, if the input pulse changes the line length by λ/2 (λ is the wavelength in the line), the output oscillation phase changes by π (the phase modulation index is Φ = π/2). Discrete variation of the line length is obtained using switching elements, such as most frequently applied *p-i-n* diodes. An advantage of these circuits is that they do not necessitate employing circulators and bridge networks, which are difficult to manufacture and tune.

It is known that the spectral distribution of FM oscillations is much more intricate than that of amplitude modulated (AM) oscillations. For the sinusoidal modulation, FM oscillations are described by the formula

$$X(t) = A\sum_{-\infty}^{+\infty} J_n(\varphi)\sin(\omega + n\Omega)t. \tag{14}$$

It is seen that the FM oscillation spectrum consists of a carrier component at frequency ω(*n* = 0) with amplitude AJ_0(φ) and an infinite number of side components located symmetrically with respect to the carrier on both sides of it at frequencies (ω ± *n*Ω) with amplitudes AJ_n(φ). However, the only noticeable contributors are components with amplitudes comparable to AJ_0(φ). Since Bessel functions rapidly decrease as n increases at given argument φ, in most cases of practical importance, the truncated series with only the first terms retained can be used. However, for signals with a high modulation index, the series terms with the numbers as large as *n* = 10 are substantial contributors, because the amplitude distribution does not allow their neglect.

When a nonsinusoidal and nonperiodic signal is modulated on the carrier, the spectral distribution becomes much more complicated.

An FM signal with sinusoidal carrier at frequency fo and step phase variation can be represented in the form

$$X(t) = \sum_{k=1}^{N} A\sin 2\pi f_0[t + k\Delta T(-1)^{j_k}]; \quad 0 \le t \le \Delta T, \tag{15}$$

where *A* is the amplitude, f_0 is the carrier frequency, Δ*T* is the duration of the modulated sinusoid section equal to an integer number of sinusoidal signal halfperiods, and parameter j_k takes on the value of zero or unity according to the code sequence which determines the step (±π) variation of the carrier phase.

With the modulation described above, the operating bandwidth is substantially expanded. In the vicinity of the main maximum, the form of the FM signal resembles the sinusoid half-period with the maximum at carrier frequency f_0. The spectrum width is determined by duration of the modulated sinusoid section Δ*T* and equals f_0/n, where n is the number of carrier oscillation periods in interval Δ*T*.

With the periodic function modulation, signals have line spectra. With the discrete noiselike signal modulation, the signal has a continuous spectrum whose width is determined by the maximum (clock) frequency.

The inverse transformation of the FM signal to the pulse form is performed through calculating the CCF of the recorded signal and *X*(*t*). In the absence of frequency and phase distortions of the recorded signal, the correlation transformation yields an FM signal whose form coincides with the ACF of the transmitted signal.

C. Chaotic Algorithms Producing Spectrum-Spreading Functions

It has been shown that an NCS produced by a discrete chaotic algorithm meets all of the following requirements necessitated by spectrum spreading and formation of a noiselike carrier: this signal is wideband; it has a large processing gain and uniform spectral density over the transmission channel bandwidth; its ACF has a single narrow peak and low side spikes; and the signal can be completely recovered in the receiving device, which is needed for correlation processing. In addition, code sequences of NCSs satisfy the criteria of randomness. The ACF characteristics of both a binary and transformed binary signals fit the correlation properties of binary sequences.

The statistical characteristics of NCSs resemble those of a Gaussian process, which is an important qualitative factor ensuring structure hiding of a desired signal in the presence of noise often having the normal distribution. This circumstance guarantees high noise immunity. The structure of an *M* sequence is usually recovered using its difference from a normal random process.

Evaluation of the size of a signal system shows that NCSs offer promise in constructing large signal systems guaranteeing extremely efficient energy and structure hiding. Dynamically variable chaotic codes make it impossible to disclose information resources of open telecommunications systems in real time, thus ensuring high-level security and noise immunity.

D. A Spread-Spectrum Communications System Based on Chaotic Binary Codes

A microwave model radio terminal for a wideband spread-spectrum communications system is developed and experimentally investigated. The model incorporates a bridge phase shifter producing the fixed phase shift φ = π. The properties of the communications channel were investigated using an elementary model double-terminal wideband communications channel with a noiselike carrier. The model included a digital generator forming a chaotic pulse sequence, a microwave microstrip phase modulator-demodulator, and horn antennas. The channel was assumed to consist of transmitting (a phase modulator ensuring spectrum spreading) and receiving (a demodulator, which is a convolving device applied to recover the carrier) units. Special interferences were not introduced into the channel, and it was assumed that a microwave signal is transferred from the transmitter to receiver during a time interval much shorter than the pulse duration.

The block diagram of the model noiselike-carrier communications channel (**Fig. 2**) contains a microwave sinusoidal signal oscillator (1), digital generator of a chaotic coding sequence (2), phase modulator (3), phase demodulator (4), spectrum analyzer (5) connected to various points of the circuit, discrete delay unit (6), and horn antennas (7).

The digital generator produced a chaotic code sequence modulated on a microwave signal. The experiments on demodulation of this microwave signal were performed in the coherent mode; i.e., the modulator and demodulator were assumed to be completely synchronized. This situation was actually provided by modulating signals simultaneously applied to the modulator and demodulator units.

The spectrum of the communications channel was spread using a wideband phase modulator based on a microwave bridge phase shifter producing a fixed phase shift equal to φ = π/2, π/4, π/8, or π/l6. The phase-shifting sections of the microstrip line were switched by high-frequency *p-i-n* diodes with a small relaxation time (no more than 5 *ns*). The range of the modem operating frequency exceeds

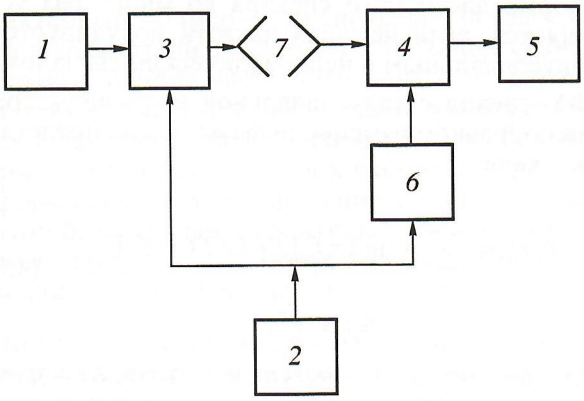

Fig. 2. *Block diagram of a model noiselike-carrier communications channel: (1) microwave sinusoidal signal oscillator, (2) digital generator of a chaotic coding signal, (3) transmitting terminal phase modulator, (4) receiving terminal phase demodulator, (5) spectrum analyzer, (6) discrete delay unit, (7) horn antennas.*

an octave. In the phase shifter, *p-i-n* diodes are controlled by chaotic binary codes that are formed by a programmable digital processor according to a developed mathematical algorithm. For each subscriber, his own chaotic code is programmed by choosing an *N*-dimensional vector of initial samples. The multidimensional digital array specifying the vector of initial samples is the subscriber's identification parameter. A programmable coder forming individual chaotic codes is developed using high-speed programmable logic matrix (PLM) technology.

Transmitted digital information can be introduced into a communications channel via either frequency modulation of the microwave carrier or variation in the phase of a coding signal. The spectrum of an FM signal transferring information is spread at the signal carrier frequency by the phase modulator incorporated in the transmitted modem circuit. The signal that contains an information component and is radiated by the transmitter has a continuous noise spectrum (**Fig. 3**a). Most of its energy corresponds to the part of the spectrum lying in the bandwidth $\Delta f = 2F_T$. Clock frequency F_T of chaotic binary codes is governed by the frequency synthesizer incorporated in the modem. In the experiment, F_T = 1 MHz. The information message is a sequence of binary symbols represented by current pulses at a clock frequency of 20 kHz.

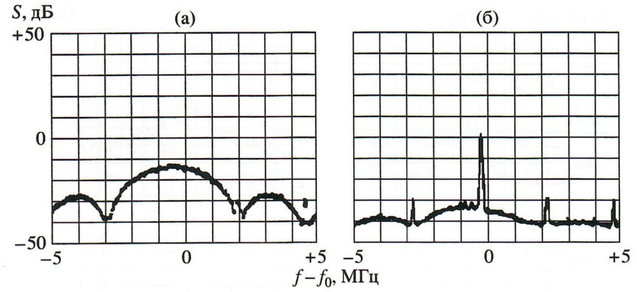

Fig. 3. *(a) Code signal spectrum spreading in the transmitter and (b) signal coherent frequency compression in the receiver f_0 = 2600MHz.*

Dimension *N* of the number identifier or vector of initial samples is *N* > 7. This important requirement of the generating algorithm ensures stable multimode chaos providing for good correlation and statistical properties of the codes formed. The transmitted WBS with an information component has a continuous noise spectrum, and its structure virtually coincides with that of a random process with the same bandwidth.

The coder digital processor can operate in the cyclic and aperiodic modes. In the cyclic mode, chaotic codes are replicated at a given period. In the aperiodic mode, the digital processor generates a continuous sequence of unreplicated chaotic symbols. This method can be applied to realize dynamic code escape during the entire time interval of data transmission. According to Shannon's results [31], the developed system of data transmission based on dynamic code escape makes it impossible to cryptographically disclose messages.

In the receiver, information is recovered after the relative delay of the received and reference codes is eliminated and the WBS is frequency-compressed. In the experiment, data are transmitted via continuous generation of nonperiodic sequences with dynamic code escape. In the receiver, the chaotic binary code is replicated by the digital processor according to the generating algorithm, the *N*-dimensional number identifier (or vector of initial samples) being specified exactly. The inverse transformation of the received FM signal is performed by the phase demodulator, which recovers the signal phase using a chaotic code replica as a reference signal. The received signal can be frequency-compressed only when the delay of the received and reference codes is within the duration of a single clock cycle. The efficiency of this procedure is illustrated by power spectra of the decoded signal (**Figs. 4***a*, 4*c*-4*f*). Fig. 4*c* represents the signal spectrum at

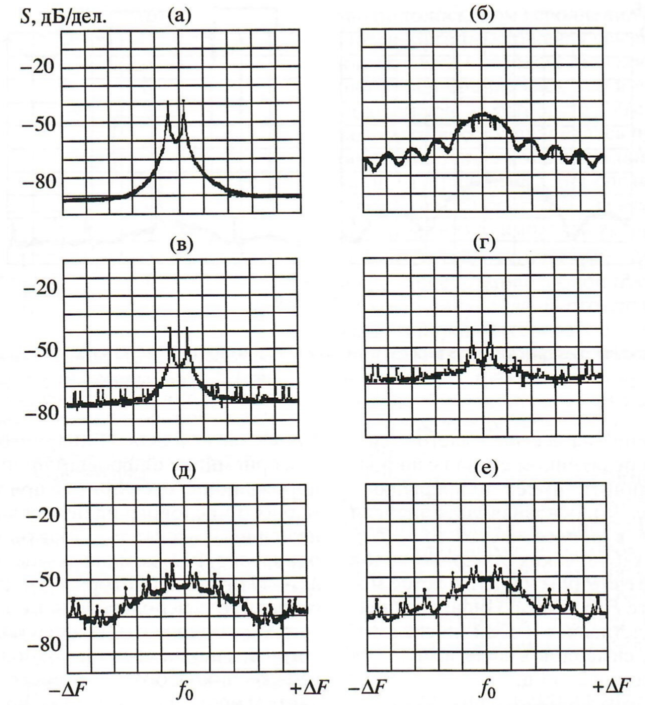

Fig. 4. *Signal spectrum transformation during transmission over a communications channel: (a) information FM signal spectrum; (b) the spectrum of a transmitted signal with a code-spread spectrum and an information component; (c) the recovered signal spectrum upon demodulation under complete synchronization; (d) spectra of the recovered signal with an information component obtained at the reference chaotic code delay τ= 0.1T, (e) 0.3T, and (f) 0.5T, where T is pulse repetition interval of the coding sequence.*

the demodulator output for the synchronized received and reference codes in the absence of code delay, $\tau = 0$. The recovered signal spectrum contains an information component similar to the FM signal spectrum at the output of the information modulator incorporated in the transmitter (Fig. 4*b*). In the absence of active interferences, the intensity of information components exceeds the receiver noise and incidental components with the clock frequency $F_T = 1$ MHz by almost 40 and 35 dB, respectively.

At the duration of a single symbol $T = 1/F_T = 1$ μs, reference code delay τ equal to only $0.1T$ reduces the information spectral component by 14 dB down to 26 dB with respect to the noise pedestal (Fig. 4*d*). At the reference code delay $\tau = 0.5T$ (Fig. 4*f*), the information component virtually vanishes. As delay τ increases, the levels of the noise pedestal and incidental spectral components at frequencies that are multiples of F_T increase because of the incompletely convolved received signal. When the reference code delay exceeds the duration of a single clock cycle, $\tau > T$, the information component cannot be detected against the background noise and it is impossible to recover transmitted information. Our experiment of data transmission with dynamic chaotic code escape has shown that useful information can be efficiently recovered only at a small delay of the reference code, $\tau < 0.5T$. The experiment on data transmission in a communications system with spread spectrum and dynamic code escape has revealed the necessity of exact synchronization of the reference code in the receiver.

We experimentally investigated the noise immunity of a model noiselike-carrier radio terminal. In the model, information was transferred by binary chaotic signals. The schematic of the experimental setup is presented in **Fig. 5**, where 1 and 2 are microwave signal and interference oscillators, respectively; 3, 4, and 5 are phase modulators PM$_1$, PM$_2$, and PM$_3$; 6 and 7 are coders; 8 is a microwave summator; 9 is a variable delay line; 10 and 11 are microwave transmitting and receiving antennas; and 12 is a spectrum analyzer. The coders produced chaotic signals of the class described above according to one of the possible algorithms.

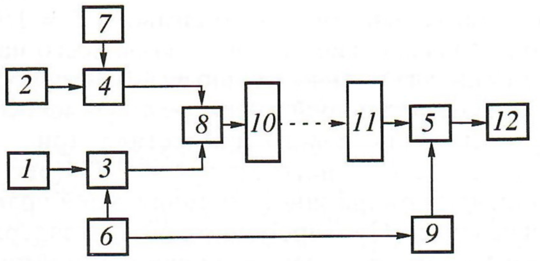

Fig. 5. *Block diagram applied to investigate noise immunity of a model noiselike carrier terminal: (1) and (2) signal and interference microwave oscillators; (3), (4), and (5) phase modulators; (6) and (7) coders, (8) microwave summator; (9) variable delay line; (10) and (11) transmitting and receiving antennas; and (12) spectrum analyzer.*

The spectrum of the signal transmitted from microwave oscillator 1 was spread using microwave modem PM_1 (3). A microwave signal at center frequency F_c arrived at the input of the modem, which was controlled by a binary chaotic pulse sequence produced by coder 6. As a result, a noise signal with a continuous spectrum was observed at the PM_1 (3) output.

In the experimental determination of noise immunity, two kinds of interferences were employed: a sinusoidal interference whose frequency was close to the transmitted microwave signal and a wideband interference which was spectrum-matched with the transmitted signal. The wideband interference was produced by microwave modem PM_2 (4). Modem 4 was controlled by independent coder 7 having the same clock frequency as coder 6 of the transmitter. The coding sequences of coders 6 and 7 are time-uncorrelated. The experiment was performed with synchronized coding sequences of the transmitter and receiver modems. Synchronization was provided by variable delay line 9. Backward coherent frequency compression of the received signal was performed by modem 5 incorporated in the receiver.

The excess of the convolved signal at the output of receiver 12 over the background noise, depending on the receiver input signal-to-noise ratio, served as a criterion of noise immunity.

In the presence of a narrowband interference, the total spectrum of the signal and interference at the receiver input coincides with the wideband noise spectrum that is continuous across a certain bandwidth and corresponds to the received spread-spectrum signal whose level is below that of the sinusoidal interference. Decoder PM_3 convolves and detects the useful signal. With decoding, the narrowband interference is smeared over the entire spectrum bandwidth being transformed into a noise pedestal lying below the convolved information signal.

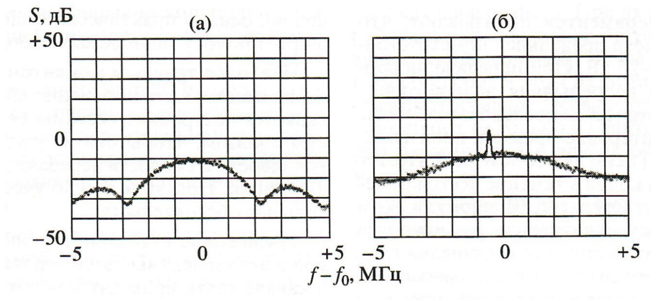

Fig. 6. *The total spectrum of a signal and wideband interference at the receiver (a) input and (b) output.*

A wideband interference is formed when the signal of oscillator 2 is transmitted through PM_2. At the receiver input, its spectrum resembles the noise spectrum of the information signal at the PM_1 output. The total spectrum of the signal and wideband interference at the receiver input, shown in **Fig.** 6*a*, coincides with the wideband noise spectrum that is continuous across a certain bandwidth. Figure 6*b* represents the receiver output spectrum obtained via convolution in PM_3 at an input signal-to-noise ratio of 10 dB.

Fig. 7 shows the measured signal-to-noise ratio at the receiver output (S_s/S_{int}) versus the ratio of the interference and information signal levels at the receiver input (S_{int}/S_s) for the narrowband (1) and wideband

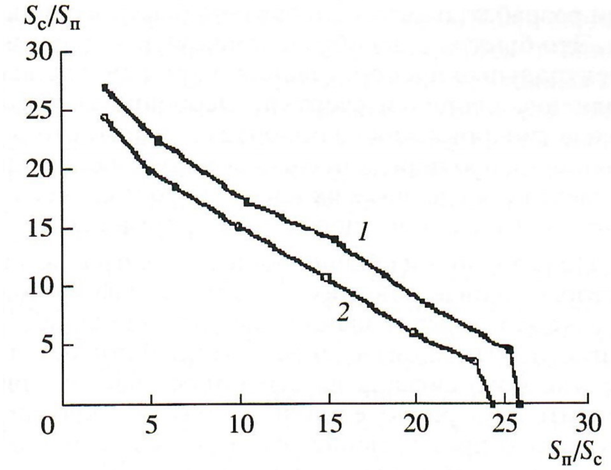

Fig. 7. *Signal-to-interference ratio Ss/Sint at the receiver output vs. quantity Sint/Ss determined at the receiver input: (1) narrowband and (2) wideband interferences.*

(2) interferences. For a spread-spectrum communications system, the ultimate noise immunity is determined by the receiver input signal-to-noise ratio such that transmitted information cannot be recovered at a given averaging time.

The experiments have shown that the ultimate noise immunity is about 25 dB for both interference types. Information is transferred using a continuous nonperiodic chaotic coding sequence of an arbitrary duration. Thus, dynamic code escape is ensured during the entire time of data transmission. According to Shannon's theory, in this case, a message virtually cannot be cryptographically disclosed [31]. This result indicates that the chaotic-code spread-spectrum system under study offers much promise for high-security multistation mobile communications systems.

Formation and time synchronization of complex signals is the main problem arising when complex signals are involved in data transmission. The enumerative technique can be applied for searching suitable signals. In this technique, the correlation integral, where correlation is determined with respect to a shifted reference signal, is calculated. The time shift maximizing this correlation serves as an estimate of the time instant of a received signal. However, when the region of *a priori* uncertainty of a signal delay is big and the signal processing gain is large, which guarantees high noise immunity, the hardware implementation of this method results in a long search time interval and, with parallel processing performed by several correlators, overcomplicates communications equipment. The software implementation necessitates large-capacity RAM and high-speed processors.

Quick search algorithms are developed to reduce the search and synchronization time intervals. They include the fast Fourier transform and other spectral transformations which simplify the convolution procedure. In the synchronization algorithm, the main goal of signal transmission over a communications channel is the determination of the time position of a signal and information transfer is an auxiliary goal.

Signals whose bandwidth-duration product substantially exceeds unity are typically referred to as complex signals. It is known that, for any pulse, its bandwidth-duration product is close to unity. Therefore, special algorithms spreading the signal spectrum have to be applied to increase this product to values exceeding unity.

Note that simple binary redundant coding complicates the structure of an information signal (especially for highly redundant codes) but does not considerably expand the bandwidth.

In designing complex-signal communications systems, the most difficult task is to develop a synchronization system that does not deteriorate noise immunity and reduce the main information rate. The following additional circumstances should be taken into account.

(i) Reduced stability of reference oscillators and equivalent frequency fluctuations in the communications channel necessitate a substantial increase in the synchroinformation rate and, hence, result in reduced noise immunity.

(ii) The structure of signals transferring synchroinformation may differ from that of signals transferring basic information; i.e., the former signals may be nonoptimal.

(iii) Simple clock synchronization of complex compound signals can be performed using the entire complex form of a compound signal, which necessitates synchronization over the period of the total signal.

With the direct convolution performed at the receiver input, synchronization and data transmission can be realized using virtually identical methods. In this case, the functional circuit of a radio terminal may contain only standard components.

Synchronization involves the following successive procedures:

(i) search, i.e., smooth scanning over the phase of either directly the clock frequency signal or the code combination of a specific subscriber;

(ii) lock-in and synchronization of the clock frequency, subscriber identification, reporting synchronization with the subscriber, reporting the information sending start, and NLS generator start;

(iii) periodic control of the synchrosignal parameters.

Thus, in order to enhance the noise immunity of the synchrochannel, it should transmit information not only at the beginning of a communication session but during the entire cycle of receiver-transmitter data exchange.

When the signal is directly convolved at the input, the information channel and synchrochannel can employ a common bandwidth, but these channels should be structurally separated in the receiver and transmitter (the highest spectrum-spreading signal frequency is the clock frequency of the reference oscillator). Then, information on the phase of the clock frequency of the reference oscillator and the subscriber's identification code go through the synchrochannel. The presence of synchrochannel communications is uninterruptedly controlled at both the receiving and transmitting terminals.

When the synchrochannel is stable at both terminals, the NLS generator is started. It produces a nonperiodic random sequence, which is used for data bit coding and decoding.

The results obtained indicate that pseudorandom signal systems formed by chaotic algorithms may serve as coding sequences for wideband CDMA transmission systems. A digital spread-spectrum communications system with dynamic chaotic code escape exhibits high noise immunity and ensures highly secure data transmission in complex electromagnetic environment in the presence of intense interferences and multipath effects. High-speed digital processors based on finite-dimensional algorithms with nonlinear dynamics produce a wide variety of binary chaotic codes, which provides for code division of a large number of subscribers. Data transmission with dynamic chaotic code escape impedes cryptographic disclosure of confidential messages.

E. Digital Chaotic Code Generator

During information coding, a coding sequence is superimposed over an information sequence according to a certain algorithm. In the information theory, it is known that the best coding function is a random process (the white noise). When information is coded in digital communications channels, the most difficult task is to generate binary random sequences.

Analog noise generators, which were intensively developed in past decades, find specific applications. Thus, they are employed to produce an artificial interference and calibrate various measuring instruments and devices [33]. Physical modeling involving such phenomena as radioactive emission, shot noise observed under electron thermal emission, or avalanche breakdown in a stabilitron does not yield real random processes. Therefore, random sequences are formed using various mathematical algorithms rather than physical processes. Progress in computational mathematics initiated development of special software techniques for generation of random number sequences. Using these algorithms, special statistical computational methods, such as the Monte Carlo method, were developed

[34] to meet, in particular, the needs of cryptography. Pseudorandom process generators are applied not only in cryptography but also in the theory of complexity and other branches of discrete mathematics.

Random number sequences are generated using the following two approaches: a technique involving digitization of analog physical processes and computational methods for generating flows of numbers that exhibit statistical properties of random numbers but, being produced by deterministic algorithms, are referred to as pseudorandom numbers.

Based on the generating algorithm developed for forming a discrete chaotic sequence [35], a digital data transmission channel is modeled. The main element of this model is a digital chaotic sequence generator, implementing the algorithm mentioned above.

Discrete algorithms forming chaotic sequences and resembling those described in [19] are simple to realize using high-speed digital technology. Theoretically, such a digital successive computational algorithm can be implemented using a high-speed microprocessor package like a DSP [36]. However, the matrix technique of chaotic sequence generation, which is rather simple and cheap, provides for efficient operation in real time. With this technique, a data table formed from a precalculated data array is stored in the high-speed RAM address space. For each complete set of the input data from this table, current values of a chaotic sequence are sampled. In this procedure, standard digital pipes of any capacity (8-, 16-, or 32-bit pipes) can be employed.

The emergence of open telecommunications networks has initiated intensive development of methods for information protection during data transmission, processing, and storage. This line is necessitated by the needs of digital information coding and novel telecommunications technologies employing wideband communications channels based on systems of complex pseudorandom signals [32].

In spite of the fact that there are a large number of algorithms for generating pseudorandom processes, their statistical properties are usually far from those of a random signal. Therefore, binary pseudorandom sequences are actually generated by the following recurrent algorithm: using a linear recurrent relation and certain initial values, a continuous sequence is constructed so that each subsequent term is found from the preceding ones. Attempts to adapt real-number operations for digital algorithms have failed, since replacing a real number by its approximation badly changes the statistics of a sequence obtained. A round-off operation unpredictably disturbs a generating algorithm, and a sequence obtained becomes statistically dependent and, hence, nonrandom.

In practical development of multistation CDMA radio systems, an important problem is choosing the form of coding sequences that exhibit not only good statistical and correlation properties but also enable one to form large signal ensembles, which guarantees high structural complexity and security of data transmission [32].

A discrete algorithm based on nonlinear dynamic systems is developed for producing a sequence of integer numbers on the segment [0, 255]. This form of the algorithm is chosen because it allows hardware implementation with a standard eight-bit microprocessor series having a sufficiently high clock frequency (as high as 100 MHz and higher). The delay parameter is chosen to be equal to 16. The initial conditions of the algorithm are specified by a specific combination of 16 eight-bit binary numbers so that the initial point of the dynamic system in the phase space belongs to a strange attractor and completely determines the further behavior of the system. This enables one to uniquely reproduce a replica of a formed chaotic signal at any point and instant.

The parameters of the dynamic system and initial conditions govern, within a wide range, the system behavior and the properties of a generated chaotic signal. A possible large variety of signals that can be obtained depending on initial data for the same algorithm indicates that this method can be applied to produce big systems of chaotic signals with specified goal statistical properties.

The investigation of the generating algorithm involved thorough experimental tests for the absence of regions where the sequence formed was regular and contained correlated terms. The theoretical estimate of the generated signal maximum period, which is limited due to a finite element set for the algorithm under consideration, is about 10^{38} symbols. Increasing the delay or the number of binary number digits, the probability of periodicity emerging in the generated chaotic process can be still reduced.

Investigation of the algorithm parameter effect on the statistical characteristics of the generated signal have revealed the parameter domains where the chaotic sequence produced by the algorithm exhibits the same statistical properties as a δ-correlated random process and has a uniform signal probability density function over the entire interval of admissible values.

We have analyzed the frequency at which groups consisting of k identical symbols occur in a binary sequence formed by the algorithm under study and clipped afterwards. Comparison of the dependence of this frequency on k with the law $1/2^k$ for an ideal random process shows that they virtually coincide.

Investigation of the initial condition effect has shown that even the minimum (one bit) variation in the initial conditions completely changes the formed sequence in a number of steps of about the delay value but retains the statistical characteristics; i.e., a new sequence belongs to the same ensemble of the signal system.

In order to evaluate the size of the chaotic signal system, we selected the segments of binary sequences that were produced by the algorithm and satisfied specified correlation properties. The analysis has shown that the ensemble formed is large; i.e., its size exceeds the signal processing gain. The ensemble size is several times as large as the size of the signal system of an M sequence, which is currently a typical coding signal.

Based on the generating chaotic algorithm for forming discrete sequences, a model digital random number generator is developed and investigated.

Discrete algorithms forming chaotic sequences similar to those described in [19] can be easily implemented using high-speed digital technology. Theoretically, recurrent digital computational algorithm can be realized using a high-speed microprocessor package like a DSP [36]. However, the matrix technique of chaotic sequence generation, which is rather simple and cheap, provides for efficient operation in real time. With this technique, a data table formed from a precalculated data array is stored in the high-speed RAM address space. For each complete set of the input data (address) from this table, current values of a chaotic sequence are sampled. This technique enables one to intentionally change the chaotic algorithm by writing in ROM another table data array. In this procedure, standard digital pipes of any capacity (8-, 16-, or 32-bit pipes) can be employed.

The block diagram of a digital chaotic signal generator realizing one of the chaotic algorithms is displayed in **Fig. 8**. A number sequence of eight-bit binary numbers is formed in a parallel code in the generator output bus. The chaotic algorithm can be started when the set of initial conditions (whose various variants are stored in the ROM) is specified. Under loading various sets of initial conditions, various random sequences are formed in the generator, which may be used for realizing dynamic key escape during information coding.

A prototype digital chaotic signal generator consists of the following functional components: a device per- . forming number sampling from an array; ring stack 2; device specifying initial conditions 1; and clock frequency grid former, represented in the block diagram by units 7-9. The prototype design contains an eight-bit data bus, which means that a discrete chaotic algorithm is produced using a set of 256 eight-bit binary numbers.

The device performing number sampling from an array is built around ROM 3. Since ROM is applied to realize sampling of discrete values of a chaotic sequence, one can use tabular calculations when the number of possible discrete numbers is finite and a deterministic algorithm is known. Therefore, a one-toone correspondence can be established between a finite number of discrete values and the ROM address space of a number array employed. This technique enables one to intentionally change the chaotic algorithm by writing in the ROM a different table data array.

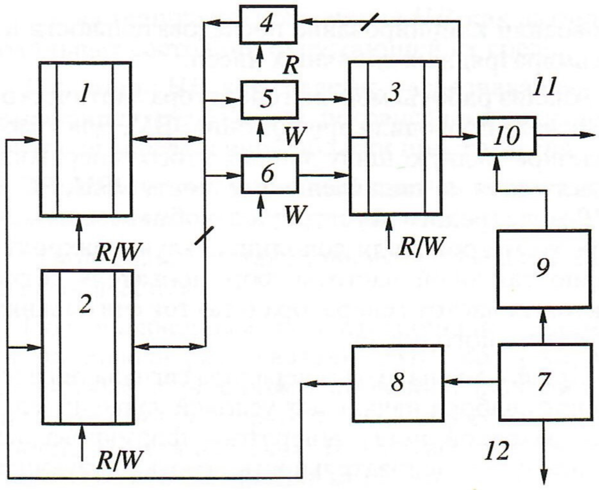

Fig. 8. *Block diagram of a digital chaotic signal generator realizing the chaotic algorithm: (1) ROM for initial condition storing, (2) an RAM-based ring stack, (3) ROM for data array storing, (4)-(6) latch, (7)-(9) clock frequency grid former, (10) signal-clipping buffer register, (11) one-bit output bus, and (12) clock oscillator. Control signals are designated by R/W A short transverse line section marks an eightbit data bus.*

Ring stack 1 represents a set of shift registers applied to store in the RAM data necessary for performing number sampling from an array. The ring stack is based on the RAM combined with a control unit. The device specifying initial conditions is implemented using the ROM, where the sets of initial conditions are stored. These sets provide for loading the ring stack at the initial instant. Various sets of initial conditions provide for various random process realizations produced by the digital chaotic signal generator. This circumstance ensures the controlled dynamic key escape during digital information coding. The available number of all possible keys is limited only by the capacity of a specific ROM.

Clock frequency grid former 7-9 is intended for synchronization of the processes in the eight-bit data bus in various generator units. The mode of the random number generator is controlled by the corresponding enabling signal. This signal is used to load initial conditions (or the law of dynamic key escape). After that, the generator starts forming a random sequence; i.e., the operating mode of the generator is initiated.

In order to obtain a one-bit binary sequence that can be used, in particular, in phase modulation, a sequence of eight-bit binary numbers was clipped.

The operation of the model chaotic signal generator was analyzed on a computer. To this end, the eight-bit data bus of this generator was connected to the IBM PC parallel port in the EPP mode (the two-way data exchange mode). In addition, the clock frequency of the generator clock frequency grid former was synchronized with the read time of the parallel port.

When a signal of a certain set of initial data arrived at the generator input, a binary sequence corresponding to the chaotic sequence produced by the generator under specified initial conditions was formed in the generator parallel output bus. Segments of temporal realizations of the discrete random process were downloaded in separate files. After that, correlation analysis of the obtained signal system was performed using a computer.

The experiments have verified the identity of the software and hardware implementations of the chaotic algorithm. The actual operation speed of the generator was limited by the time of information reading from the ROM. The analysis of the obtained segments has confirmed a high quality of signals formed from realizations of a digital chaotic sequence at the generator output.

The digital generator of random numbers based on the discrete chaotic algorithm is developed as a codingdecoding device (codec) for radio terminals of a wideband digital communications channel, as well as an information coding device for cryptographic encrypting systems. The chaotic algorithm enables one to produce a large system of codes, which is a substantial advantage over pseudorandom sequences currently applied, and guarantees high interchannel noise immunity in multistation CDMA systems. The experiments have verified the identity of the software and hardware implementations of the chaotic algorithm. The actual operation speed of the generator is limited by the time of information reading from the ROM.

4. NOISE RADAR AND RADIO-WAVE IMAGING

Informativeness, accuracy, and resolution of modem radar measurements can be substantially enhanced using ultrawideband noise signals [37, 38]. At a bandwidth of probing signals (PSs) exceeding 3 GHz, spatial resolution is better than 5 cm for an individual reflector. With this high resolution, complex targets are recognized and informative radar images are constructed using microwave and millimeter-wave noise radars with optimum processing of ultrawideband signals.

In the radar station (RS) receiver, noise signals treated by correlation or double-spectral processing methods are coherently time- or frequency-compressed, respectively [39]. Coherent compression and long-term accumulation of probing noise signals ensure high (no less than 60 dB) noise immunity in the presence of active and passive interferences. Since noise radars continuously radiate electromagnetic waves (EMWs) with a low power spectral density over a very wide frequency band, they ensure secure noise radiation and exhibit electromagnetic compatibility with other equipment in service, including traditional and narrowband systems.

Ultrawideband PSs can penetrate plant or ground covers and artificial obstacles such as walls of buildings, concrete constructions, etc. Ultrawideband radars ensure high-resolution detection of military objects hidden in high forest vegetation and detection and identification of antipersonnel mines and minefields from electromagnetic fields scattered in various (including backward) directions [40]. Noise signal probing followed by coherent processing and accumulation of energy of useful scattered signals enables one to detect hardly noticeable remote objects covered by radio wave absorbing materials owing to an increase in their radar cross section caused by bandwidth expansion.

A topical problem arising in noise radar is the creation of ultra wideband noise signals sources with a sufficient radiation power and development of optimum processing methods for these signals. Progress in the theory and applications of dynamic chaotic systems offers the possibility of developing solid-state and electron-wave self-excited oscillators for producing ultrawideband noise signals with a specified power and controlled spectrum [41]. Modem coherent convolution devices for noise and noiselike signals, such as analog and digital correlators, convolvers, and code-controlled phase demodulators, successfully perform correlation processing of PSs over a bandwidth of tens and hundreds of megahertz. Recent investigations in the field of spectral interferometry carried out by researchers of the IRE RAS have shown that noise signals at frequencies ranging up to several gigahertz (and even tens of gigahertz) can provide high-accuracy radar measurements. Spatial resolution of noise radars that use the spectral interferometry methods combined with ultrawideband noise signal cepstral processing may reach fractions of a centimeter, which can substantially enhance informativeness of radar measurements and offer the possibility of constructing detailed radio images of complex and extended objects.

A. Nonlinear Scattering of Radio Waves and Nonlinear Radar

Novel technologies used in radar engineering that employ nonlinear electromagnetic radiation scattering from various objects provide for a considerable increase in the body of information on the environment. Physically, these technologies are based on nonlinear scattering of EMW s and the fact that the field scattered by an object contains spectral components that are absent in the incident field spectrum. Nonlinear scattering effects enable one to detect various objects in the presence of reflection from surroundings of the object through probing the medium by EMWs. Sometimes, remote information on dynamic processes evolving in an object and its surroundings can be obtained. Nonlinear scattering is caused by the fact that objects contain nonlinear elements (NEs) with nonlinear properties (imperfect electrical contacts of metal constructions, semiconductor elements of electronics, etc.) [42].

At present, nonlinear effects are mainly used in two areas: remote detection of objects that are nonlinear wave scatterers, such as mine or shot firing devices and camouflaged vehicles and armament equipment, and design and investigation of artificial nonlinear scatterers (NSs), including markers for designation and remote search of objects and people [43l

Active interest in the following novel research lines has emerged:

(i) remote analysis of system dynamics;

(ii) design of elementary NSs serving as sensors of the local state of their surroundings;

(iii) development of systems of NSs for recognizing moving objects, signal retranslation, and control of a fixed space area;

(iv) development of systems for remote diagnostics of engineering objects and constructions;

(v) development of remote search systems for rock analysis.

A passive EMW scatterer containing NEs, whose electric parameters σ, μ, and ε depend on the current flowing through this element, is conventionally ref erred to as a nonlinear object. Due the aforementioned properties, the signal scattered by a nonlinear object may contain components that are absent in the incident field.

The secondary (scattered) field may be caused by various mechanisms. This can be illustrated by the following example of quasi-monochromatic PS scattering from an NS.

(a) A distorting NS contains an NE with the current nonlinearly depending on the applied voltage, which results in the emergence of higher harmonics in the frequency spectrum, i.e., in distortions of the spectrum.

(b) a subharmonic NS contains power-consuming NEs, whose presence (under certain conditions) initiates a parametric resonance and induces subharmonic currents in the scatterer.

(c) Specially synthesized NSs contain NEs producing a secondary field due to a d.c. field component induced in an NS affected by a PS. After that, the set of NEs incorporated in the NS form an arbitrary specified NS response to a PS.

Common features of these interaction mechanisms are remote reception of the EMW source energy and the presence of the antenna part (which is usually linear), an NE, and a secondary field with spread spectrum induced by the NE-PS interaction. Nonradiating systems that contain active elements providing for the internal dynamics of these systems also may serve as NSs.

Research into nonlinear scattering from mechanical systems, electronics, and its components aimed at developing methods of their detection is the area most thoroughly studied and technically coped with. Nonlinear radar is a conventional term used in this area. At present, the concept of an NS has been developed in which an NS is interpreted as an electrodynamic structure containing a finite number of discrete nonlinear elements. The dependence of the scattered signal intensity on the depth of NS embedding in the soil, the soil humidity, and the NS angular position has been analyzed. Studies of the properties exhibited by NEs (numerous metal-oxide-metal structures) in the time and frequency domains and their dependence on various factors are now in progress. Most investigations involve the analysis of amplitude, frequency, and polarization properties of NSs. In particular, it has been found that NS amplitude characteristics may be discontinuous functions and there is no one-to-one relationship between the polarizations of the incident field and the field scattered from an NS. This relationship is determined by not only the configuration of the NS linear part and its angular position with respect to the PS field but also the direction of conductivity of NEs incorporated in an NS.

The statement that, with nonlinear radar, the received signal intensity decreases with distance as $1/R^6$ has to be corrected for second-order nonlinear fields (NFs) in free space.

Generally, NS amplitude characteristics have quadratic, linear, and saturation sections (and may even break). Therefore, the received field vector flux may be proportional to $1/R^2$, $1/R^4$ (as with linear radar) or l/R^6 and even increase with R.

Passive scatterers are the most widely manufactured NSs. The first markers were half-wave diode-loaded vibrators and could be used, for example, to find survivors. The information content of their response was equal to one bit. An infinitely long service life, low cost, and good mass-size characteristics of these scatterers stimulated their production.

Generally, a marker contains an antenna, a transmitter, receiver, and memory unit. A marker usually weighs no more than tens of grams. Marker operating bandwidths range from hundreds of kilohertz to 5 GHz. In low-frequency markers, their built-in antennas represent windings. A marker may respond at the NF or PS frequency or at its own (PS-independent) frequency. In the latter case, the d.c. field component induced in the marker NE is used to feed the modulator or the marker high-frequency oscillator. A PS may carry an address query. The information content read from marks may amount to hundreds of bits. Admissible speeds of objects that are supplied with marks and move near readers may be as high as 300 km/h. One can readily see that, at a limited duration of a contact with a mark, the identification range depends on the read information content, which determines the reader receiver bandwidth. The energy portions corresponding to the information contents of an address query and a mark response, a carrier chosen, and the mark location on a marked object are of much importance for identification.

Using the technology described above, environment state sensors involved in remote control can be developed in the form of NSs. The presence of discontinuities in amplitude characteristics of certain NSs and their small sizes ensure nondestructive testing of EMW field distribution. These simple artificial NSs provide for remote recording of weak perturbations of the incident stationary EMW field that are caused by variable surroundings, for example, by moving objects or living beings. Linear objects can be recognized when they move along an NS array. Studies have been performed on detection of living beings and remote measurements of their physiological parameters. The method is based on the analysis of NFs scattered from de-energized electronics surrounding these beings. The EMW irradiating them must have an intensity sufficient for NF reception.

It has been found that a system of subharmonic scatterers (SHSs) may exhibit collective effects manifesting themselves in a certain hierarchy; i.e., as the PS wavefront approaches, scatterers that were earlier excited may impose their scattered field phases on other SHSs included in the system. The conditions imposed on PSs and relative SHS position that provide for transformation of a generally stochastic system response into a deterministic one have been established. In this case, the flickering backward scattering pattern of the system acquires a fixed form, which enables one to control the propagation speed of the excitation and synchronization processes in the system [44].

We should mention the following research problems arising in the fields described above and calling for special studies:

(i) NS recognition;

(ii) determination of NS coordinates;

(iii) development of processing methods;

(iv) increasing the efficiency of synthesized NSs;

(v) investigation of scattering from NSs and possibilities of its application at higher frequencies, which can provide for more efficient spatial NS selection and facilitate formation of denser EMW fluxes.

The use of complex WBSs in nonlinear radar can substantially increase the radar signal informativeness.

4. CHAOTIC ALGORITHMS APPLIED FOR INFORMATION PROTECTION, PROCESSING, AND TRANSMISSION

A. Information Masking by Multimode Chaos Applied to Batch Transmission

Chaotic masking is of interest for batch communications, which are increasingly being widely expanded at present. For example, the digital WAP protocol being introduced into the GSM standard, used in cellular communications, implies multimedia support, including real-time video signal transmission. Application of novel telecommunications technologies of packet data transmission, conventionally referred to as General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE) will increase the data rate up to 171.2 and 384 kbit/s, respectively.

However, the universal communications system of the third generation, referred to as Universal Mobile Telecommunications System, requires a rate no lower than 2.048 Mbit/s. Today, the GPRS technology provides for a gradual transition from current cellular communications to wideband strategy systems of the third generation. Development of alternative packet data transmission methods is a topical problem. In particular, it is expedient to apply delay chaotic systems with multimode chaos. An application of such a system is illustrated in **Fig. 9**, displaying the block diagram which contains transmitter consisting of elements 1-8 (Fig. 9a) and receiver consisting of elements 9-16 (Fig. 9b) [45].

Oscillator 1 produces a driving pulse $f(t)$ (pilot signal). After oscillations pass through splitter 2, oscillatory process $\gamma_1 f(t)$, where γ_1 is the output capacity of the transmitter, is induced at the first output of the splitter. This output is connected to delay line 3. The process $1 - \gamma_1 f(t)$ is realized at the second output. At the output of the delay line, $\varphi_1(\tau) = \gamma_1 f(\tau)$, where $\tau = t - T_1$ and T_1 is the signal delay in line 3. Signal $\varphi_1(\tau)$ arrives at driven oscillator 4 (a chaotic generator with hard excitation), producing oscillatory process $x_1(t)$. If transmitted message $s(t)$ is modulated on oscillations x in device 6, signal $z_1(t)$ produced by summator 5 can be represented as $z_1 = x_1(t) + x(t) + (1 - \gamma_1)f(t)$, and the signal at the amplifier 7 output is $G z_1(t)$, where G is the amplifier gain. This signal is radiated by antenna 8.

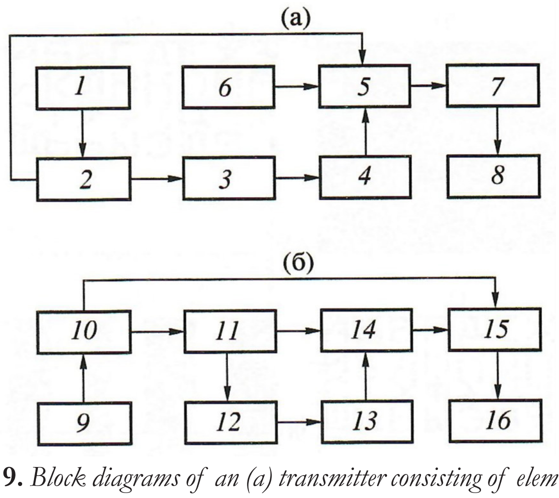

Fig. 9. *Block diagrams of an (a) transmitter consisting of elements (1)-(8) and (b) receiver consisting of elements (9)-(16).*

In the receiver, oscillations come from antenna 9 to splitter 10. From its first output, the received oscillations arrive at electron switch 11, which having transmitted the pilot signal, is locked, so that driven oscillator 13 (which is similar to oscillator 4) is affected only by the radio pulse that has passed along delay line 12 and chaotic oscillation produced by the transmitter are cut off. When the radio pulse is split into two equal parts, splitting loss is compensated in switch 11, so that radio pulse oscillations at either output coincide with those at the switch input. The oscillatory process at the splitter 10 input is determined by the quantity $G\ z_1(t)$ (with compensated loss in the transmitting channel). At the first splitter output (at the switch 11 input), oscillations $G\gamma_2 z_1(t)$, where γ_2 is the output capacity of the receiver, are produced. At its second output, the signal $(1 - \gamma_2)G z_1(t)$ appears. Being transmitted through the switch, the signal takes the form $G\gamma_2(l - \gamma_1)f(t)$. The T_2 delay in line 12 yields the signal $\varphi_2(\tau) = G\gamma_2(1 - \gamma_1)f(\tau)$ if $T_2 = T_1$. This signal excites oscillator 13. Its oscillation $x_2(t)$ are applied to one of the summator 14 inputs. The signal $(1 - \gamma_1)\gamma_2 Gf(t)$ arrives at the other input. The total oscillatory process, determined by the expression $z_2(t) = x_2(\tau) + (1 - \gamma_1)\gamma_2 Gf(t)$, comes to one output of subtractor 15. The oscillation $G(l - \gamma_2)z(t)$ (coming from the splitter 10 output) are applied to its other input. The difference oscillation $z(t) = G(l - \gamma_2)z_1(t) - z_2(t)$ affect detector 16. Having been nonlinearly transformed, integrated, and filtered, the output signal is picked off detector 16.

Fig. 10 shows typical power spectra obtained with data transmission. Fig. 10*a* displays power spectrum S_1 at the device 6 output and spectrum S_3 at the receiver output.

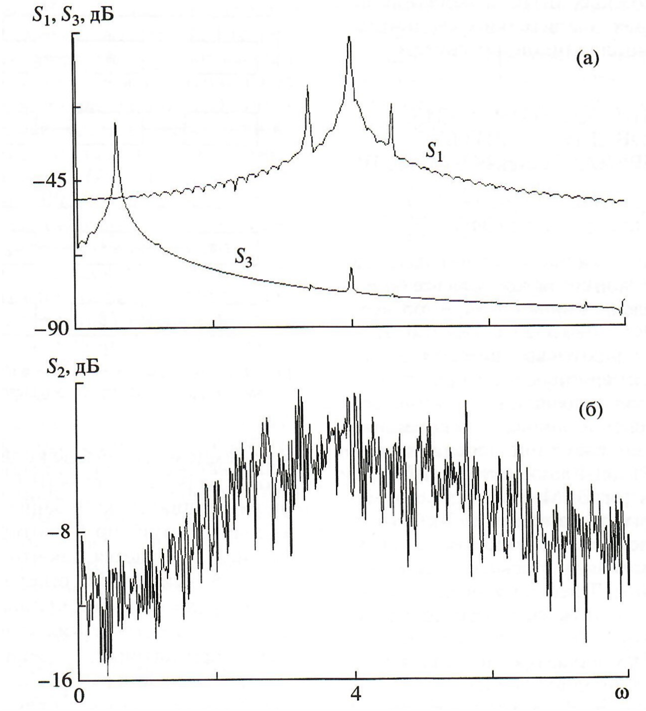

Fig. 10. *Power spectra of the transferring information according to diagrams presented in Fig. 9: (a) spectra S_1 at the transmitter device 6 output and S_3 at the receiver device 16 output and (b) spectrum S_2 at the transmitter amplifier 7 output.*

Fig. 10*b* represents power spectrum S_2 at the amplifier 7 output. In the simulations, oscillators 4 and 13 are described by nonlinear differential equations with retarded argument when the NE characteristic provides for hard excitation. For simplicity and clearness, transmitted signal *s*(*t*) is specified in the form of a periodic function.

One can see in Fig. 10*b* that the power spectrum at the receiver output represents the chaotic character of oscillations. The transmitted regular signal is reliably masked. In the receiver, the transmitted signal is distinctly detected (curve S_3 in Fig. 9a).

B. Pseudoholographic Information Coding

Emergence of novel telecommunications technologies and development of methods of transmitting and storing large bodies of digital information necessitate solving the problem of efficient information recovery at unavoidable transmission, archiving, and long-term storage losses as well as providing for a high data rate and the possibility of fast access. Pulse noise in a channel observed during transmission, write and read faults (faults of the latter kind occur when information is read from magnetic and optical media), imperfect technology, and various damage of a magnetic coating occurring during storage result in losses of both isolated bits and whole, sometimes considerable, information blocks. The use and storage of information in the electronic form find increasingly wide applications in the modern world. Almost all big libraries and depositories transfer their archival stocks to digital media. Therefore, development of special coding methods that are necessary for information transmission, processing, and storage and ensure efficient recovery of lost information is an urgent problem.

In this context, the physical principle of optical holography (this term originates from the Greek words *holos* and *grapho* meaning entire or whole and write, respectively). Optical holography represents a technique of recording the phase pattern of wave fields scattered by objects on a photocarrier (hologram). The phase pattern is recorded using a reference coherent wave. This technique is actually analog coding of object images. An important and useful feature of this coding technique is the fact that, owing to sphericity of scattered waves, information on each scattering point of an object is uniformly spread over the entire hologram, which provides for the possibility of valid recovery of an original image from a small fragment of a hologram using reference coherent radiation (key). Even an irretrievable loss of a considerable hologram section does not prevent one from recovering an integral image through decoding. A deteriorated quality of a recovered image manifests itself only in a certain decrease of brightness and contrast.

As with optical holography, the most demonstrative is digital image recovery.

Obviously, any text information can be represented in a graphical form.

The matrix consisting of zero and unity elements, which is an analog of a bitmap image, may serve as a physical model of a digital image that is to be coded. In this case, one can assume that a black (white) image element corresponds to unity (zero). Obviously, this representation of graphical information can be extended to a color image by superposing several matrices, as is done in color printing art or television. Depending on resolution, a single element of an image (pixel) may represent both a single point and a set of bitmap points.

When the bitmap matrix is transformed through renumbering (mixing) its terms so that any compact subset of elements is uniformly distributed over the entire matrix field, black and white bitmap elements are mixed and the image becomes uniformly gray. The inverse one-to-one transformation returns all elements to their original positions, and the image is recovered in the original form. This matrix transformation should ensure satisfactory reproduction of an image as a whole upon decoding even if a part of the transformed matrix is lost. Thus, the method of digital image coding is a direct analog of optical holography.

Note that an integral image can be recovered from a fragment of the coded one using various techniques, such as the well-known two-dimensional (*2D*) Fourier transform and other similar transformations. However, in this case, image elements are mixed rather nonuniformly. Coding methods that employ decomposition of image elements into spatial harmonic modes and take into account phase differences between them are analog methods even when a discrete analytical approach is applied.

A simple 256x256 matrix containing zero and unity elements arranged in the form of the letters of the Russian alphabet was chosen as a model image to be coded (**Fig. 11***a*) [46]. The matrix elements were mixed through double permutation according to a pseudorandom law. In order to ensure a uniform distribution and one-to-one coding transformation, a random-number generator produced for each matrix line a special mixing code which consisted of random permutations of the entire set of 256 integers belonging to the natural series. Thus, a coding matrix was composed: It contained 256 lines with various pseudorandom sequences of 256 integers from the number interval $\{1, 256\}$, which were randomly mixed. Using this matrix, the elements in the lines of the original image matrix were randomly renumbered according to the law specified by the corresponding line of the coding matrix.

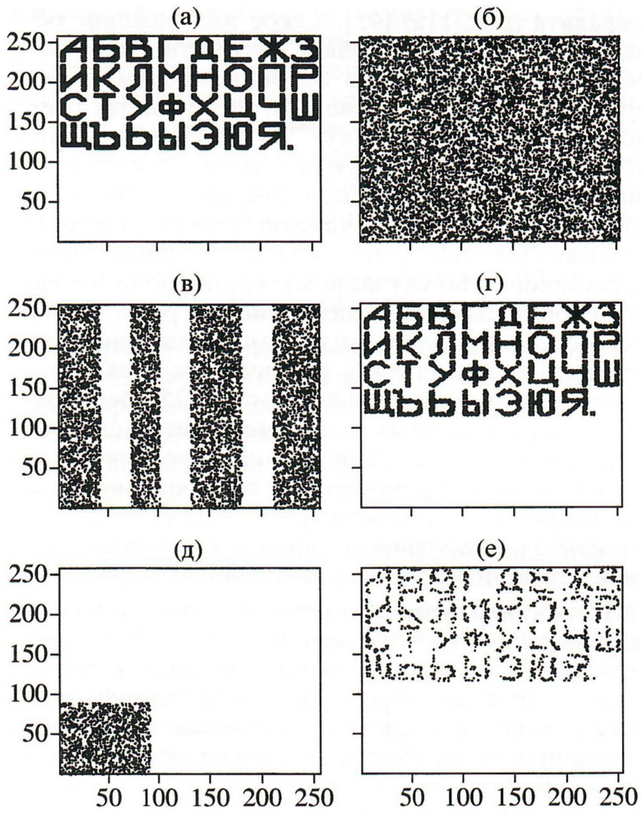

Fig. 11. *An example of pseudoholographic coding of graphic information: (a) original image of the Russian alphabet on a 256x256 matrix, (b) coded image obtained upon uniform pseudorandom mixing of elements over the entire matrix area, (c) a damaged coded image, (d) the image recovered from the corresponding truncated matrices, (e) a fragment of a coded image, and (f) the image recovered from its fragment.*

The image matrix thus renumbered was rotated through 90°. As a result, lines (columns) turned into columns (lines). After that, a new coding matrix was formed from pseudorandom sequences of 256 numbers belonging to the natural series $\{1, 256\}$ and the next mixing was performed. The second renumbering yielded a matrix consisting of the original matrix elements, which were completely mixed. The *ij*th element of the original matrix became the *lm*th element with the probability $1/256^2$; i.e., black and white elements of the image were rather uniformly distributed over the entire area of the transformed matrix. The image turned into a gray square (Fig. 11*b*).

The inverse transformation can be performed using decoding matrices, i.e., matrices returning renumbered elements to their original positions. A lost part of a coded image can be imitated in various ways. In the matrix corresponding to a coded image, the elements of an arbitrary block may be replaced by zeros so that the original matrix dimension is retained. This operation resembles the whitening procedure. An original image is recovered from a fragment of the coded one irrespective of what section of the coded image is damaged. Figs 11*c* and 11*e* show a variant of the damaged coded image. One can see an array of whitened columns and a fragment representing a one sixteenth of the coded image. The original image recovered in the presence of these damages is displayed in Figs. 11*d* and 11*f*. It is distinctly seen that the original picture is rather satisfactorily recovered from undamaged fragments of the transformed matrix. Naturally, as the matrix area involved in recovery is reduced, the image becomes less distinct. The results obtained confirm the analogy between the proposed coding method and the principle of entire image recovery from a hologram fragment.

Using additional approximation methods for image recovering from a coded fragment, the recovery efficiency can be substantially enhanced. In this situation, *a priori* information on the image character enables one to choose the most efficient approximation method. In particular, gray-scale pictures are well recovered using a median spline and contour images (text, drawings, or diagrams) are adequately recovered using methods that improve the linear contrast [22].

Simulations show that the main requirement of a coding algorithm is uniform mixing of individual elements of an information block over the entire space. The second important requirement is one-to-one information block recovery, which means that, during decoding, the inverse transformation must not map different elements into a single point.

Coding matrices providing for image element mixing according to a pseudorandom law can be composed using both standard pseudorandom number generators and special programs for pseudorandom integer number generation, such as discrete chaotic algorithms [21]. Note that, as the body of information blocks increases, the efficiency of recovery from fragments strongly depends on the degree of uniformity of original information mixing. Therefore, using deterministic chaotic algorithms to this end may be extremely important.

During long-term storing of digital information in the electronic form on magnetic and optical media, as well as during its transmission over imperfect communications channels, rather large information blocks may be lost. The graphical information coding method proposed enables one to substantially reduce such losses since, during image recovering (decoding), large lost blocks are replaced by losses of isolated image points, which do not deteriorate the integral perception of the image as a whole. Note that information coded according to the algorithm proposed can be compressed using various methods that efficiently reduce information content.

An additional advantage of the method developed for digital information coding is cryptographic stability. The operation of matrix element mixing actually is key encryption, the key length being equal to the information array length. This means that, even when a coding technique is known, decoding of this image via simple key search is a problem whose solution necessitates resources exceeding those of modern computers. Indeed, the number of possible permutations is 256 ! ~ 10^{507} even for a small information block (with 256 elements in a line). A modern personal computer classifies this number of variants as infinity. Therefore, unauthorized decoding of such information can be performed only through revealing the algorithm of composing the matrix providing for image element mixing. Information coded using the method proposed can be stored in free-access archives· and transmitted over open information channels guaranteeing data security.

CONCLUSIONS

At present, progress in modem information-telecommunications systems and information technologies is primarily determined by development of software and algorithms ensuring data protection during transmission, processing, and storing in computer networks and by explosive expansion of personal wireless, rapid growth of the number of users, increased user mobility, and necessity of transmitting various kinds of information.

We have reviewed promising applications of information technologies based on dynamic chaos and aimed at information transmission, processing, storage, and protection. Finite-dimensional mathematical algorithms are proposed for calculating chaotic signals. They are based on the method of reconstructing non linear dynamics in dissipative systems with delay. A digital chaotic binary code generator involving high-speed digital devices is developed. It is suggested to apply discrete chaotic algorithms for protection, processing, and transmission of information including graphical information (in the latter case, it is suggested to use pseudoholographic coding). These algorithms are realized.

Applications of information technologies imply physical realization of a specific coding process during data transmission, processing, and storage in telecommunications systems and computer networks. Progress in this field is ensured by an increase in performance speed and noise immunity of information channels. This is necessitated by the demand for efficient channels of information exchange and control of distributed networks and automatic remote-control systems, where an error or a partial information loss may result in catastrophic consequences, even to the point of the loss of an entire system.

Using the example of a telecommunications radio terminal of a spread-spectrum wideband digital communications channel, we have experimentally investigated information technologies of a digital communications channel whose spectrum is spread by coding chaotic signals. It is shown that, during data transmission, this channel efficiently spreads the carrier spectrum by transforming the carrier into a noise signal in a wide frequency band. During data transmission, spectrum spreading guarantees energy security (necessary detectability), and the noiselike carrier formed ensures efficient structural security of the communication channel. The communications channel implemented using these concepts exhibits high security, since it is virtually impossible to recover a chaotic spectrum-spreading function and convolve a WBS at unauthorized reception. As chaotic codes are mutually orthogonal, WBSs can be statistically divided in the communications channel in the presence of multipath effects if the relative ray delay exceeds the duration of a single symbol of a chaotic code.

Global expansion of various open telecommunications systems and rapid growth of the number of subscribers necessitate information protection guaranteed not only at the level of state structures, special services, or business circles but also at the level of each individual user. In information networks, this problem is due to information loss caused by low noise immunity of various communications channels rather than to data closing from unauthorized access. The problem of enhancing communications channel noise immunity is the most urgent one in designing radio links.

Modern integrated circuitry enables one to realize a purely digital radio channel without analog microwave units when a microwave carrier, control signals, and digital information are formed with a unified frequency grid. This circumstance offers additional possibilities of overcoming technical restrictions due to the necessity of combining analog and digital units in modem computerized equipment of telecommunications channels.

The use of ultrawideband chaotic signals in modem radar provides for substantial enhancement of measurement informativeness, accuracy, and resolution, which enables one to obtain detailed radar images of complex and extended objects in the microwave and millimeterwave bands. Continuously radiating noise radars are characterized by high security and exhibit electromagnetic compatibility with other facilities in service, including traditional and narrowband systems.

Rapid progress in semiconductor microelectronics and its circuitry has already resulted in designing submicron elements. Further progress in this field will be possible upon creation new elements whose sizes are about tens of nanometers or a few nanometers. A promising line of the electronics progress is molecular nanoelectronics.

Molecular electronic devices can provide for extremely high integration of individual elements. The use of these elements as nanoelectronic circuitry will enable one to develop digital information technologies of a new generation with a new hardware infrastructure, create structurally developed neural and cell-automaton systems based on binary and multilevel logic, and design telecommunications systems of a new generation with high information capacity that involve chaotic signals with a high fractal dimension. Complex development of these systems could fundamentally contribute to solving the problem of artificial intelligence.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research, project nos. 03-07-90133, 01-07-90349, and 01-02-17529.

REFERENCES

1. Bogdanov EV, Kislov VYa, Myasin EA. *USSR Inventor's Certificate no. 1 125 735*, Byull. izobret., 1984, no. 43, p. 311.
2. Lorenz, EN. *J. Atmos. Sci.*, 1963, 20(2):130.
3. Puankare A. *0 krivykh, opredelyaemykh differentsial'nymi uravneniyami* [About Curves Determined by Differential Equations]. Moscow, Gostekhteorizdat Publ., 1947.
4. Landau LD. *Dokl. Akad. Nauk SSSR*, 1944, 44(2):339.
5. Kislov VYa., Zalogin NN, Myasin EA. *Radiotekhnika i elektronika*, 1979, 24(6):118.
6. Kislov VYa. *Radiotekhnika i elektronika*, 1980, 25(8):1683.
7. Kislov VYa, Zalogin NN, Myasin EA. *Radiotekhnika i elektronika*, 1980, 25(10):2161.
8. Kal'yanov EV, Ivanov VP, Lebedev MN. *Radiotekhnika i elektronika*, 1982, 27(5):982.
9. Kalinin VI, Zalogin NN, Kislov V.Ya. Radiotekhnika i elektronika, 1983, 28(10):2001.

10. Kalinin VI, Zalogin NN, Myasin EA. *Pis'ma Zh. Tekh. Fiz.,* 1984, 10(21):1311 (Sov. Tech. Phys. Lett., 10:554).
11. Anisimova YuV, Dmitriev AS, Zalogin NN. *Pis'ma Zh. Eksp. Teor. Fiz.*, 1983, 37(8):387 (JETP Lett., 37:458).
12. Dmitriev AS, Kislov VYa. *Stokhasticheskie kolebaniya v radiotekhnike i elektronike* (Stochastic Oscillations in Radio Engineering and Electronics), Moscow, Nauka Publ., 1989.
13. Ruell D, Takens F. *Commun Math. Phys.,* 1971, 20(3):167.
14. Schuster H. *Deterministic Chaos: An Introduction*. Weinheim, Physik, 1984.
15. Zaslavskii GM, Chirikov BV. *Usp. Fiz. Nauk,* 1971, 105(1):3.
16. Malinetskii GG, Potapov AB. Sovremennye problemy nelineinoi dinamiki (Contemporary Problems in Nonlinear Dynamics). Moscow, Editorial URSS Publ., 2000.
17. Dmitriev AS, Panas AI. *Dinamicheskii khaos. Novye nositeli informatsii dlya ststem svyazi* (Dynamical Chaos. New Information Media for Commumcations Systems). Moscow, Fizmatgiz Publ., 2002.
18. Gulyaev YuV, Kislov VYa, Kislov VV. *Dokl. Ross. Akad. Nauk*, 1998, 359(6):750.
19. Gulyaev YuV, Kislov VYa, Kislov VV. *Radiotekhnika*, 2002, 10:3.
20. Kislov VYa, Kalmykov VV, Belyaev RV, Vorontsov GM. *Radiotekhnika i elektronika*, 1997, 42(11):1342.
21. Belyaev RV, Vorontsov GM, Kolesov VV. *Radiotekhnika i elektronika*, 2000, 45(8):954.
22. Kotel'nikov VA. T*eoriya potentsial'noi pomekhoustoichivosti* (Theory of Potential Noise Immunity). Moscow, Radio i Svyaz' Publ., 1998.
23. Takens F. *Lecture Notes in Mathematics*, 1981, 898:366.
24. Ladyzhenskaya OA. *Dokl. Akad. Nauk SSSR*, 1972, 205(2):317.
25. Farmer JD. *Physica D,* 1982, 4(3):366.
26. Mane R. *Lecture Notes in Mathematics,* 1981, 898:230.
27. Kolmogorov AN, Fomin SV. *Elementy teorii funktsii i funktsional'nogo analiz*a (Elements of Function Theory and Functional Analysis). Moscow, Nauka Publ., 1972.
28. Kalinin VI. *Abstracts of Papers, 8th Int. Workshop ND&CS "Nonlinear Dynamics and Complex Systems*". Minsk, 2000, p. 7.
29. Belyaev RV, Vorontsov GM, Kalinin VI, Kolesov VV. *Abstracts of Papers, Tr. IV Mezhdunar. nauch.-tekhn. konf "Perspektivnye tekhnologii v sredstvakh peredachi infomiatsii"* (Proc. IV Int. Sci. Tech. Conf. on Perspective Technologies in Information Transmission Tools). Vladirnir-Suzdal', 2001, p. 212.
30. Shannon CE. *Bell System Techn. J.,* 1948, 27(3):379.
31. Varakin LE. *Sistemy svyazi s shumopodobnymi signalami* (Systems with Noise-Like Signals). Moscow, Radio i Svyaz' Publ., 1979.
32. Anisimova YuV, Vorontsov GM, Zalogin NN. et al. *Radiotekhnika,* 2000, 2:19.
33. Knuth D. *The Art of Computer Programming. Seminumerical Algorithms. Vol. 2.* Addison, Wesley, 1969.
34. Kolesov VV, Belyaev RV, Vorontsov GM. *Radiotekhnika i elektronika*, 2001, 46(11):1361.
35. Ushenin A, Reganov V, Nyrkov M. *Elektron. Komponenty*, 1998, 5(14):17.
36. Demin VP, Kupriyanov AI, Sakharov AV. *Radioelektronnaya razvedka i radiomaskirovka* (Electromc Reconnaissance and Masking). Moscow, MAI Publ., 1997.
37. Kalinin VI. *Abstracts of Papers, Proc. PIERS Workshop on Advances in Radar Methods,* Baveno, Italy, 1998, p. 222.
38. Aksenov VI, Zalogin N, Kirillin KL. *Proc. Int. Conf "Radar 87,"* London, 1987, p. 143.
39. Walton E. Abstracts of Papers, *Proc. PIERS Workshop on Advances in Radar Methods,* Baveno, Italy, 1998, p. 141.
40. Kal'yanov EV, Kalinin VI, Kislov V.Ya. *Radiotekhnika i elektronika*, 2002, 47(8):984.
41. Kuznetsov AS, Kutin GI. *Zarubezh. Radioelektron.*, 1985, 4:41.
42. Babanov NYu, Gorbachev AA, Lartsov SV et al. *Radiotekhnika i elektronika*, 2000, 45(6):676.
43. Gorbachev PA. *Radiotekhnika i elektronika*, 1995, 40(11):1606.
44. Kal'yanov EV. *Radiotekhnika i elektronika*, 2002, 47(4):469.
45. Kolesov VV, Vorontsov GM, Zalogin, N.N. *Radiotekhnika i elektronika*, 2002, 47(5):583.