1. Introduction

The phenomenon of chaos, which is arising of noise-like oscillations in deterministic low-dimensional nonlinear systems, should be treated from two different points of view. First, this effect can lead to a threat to stability of many practical systems, and it is important to know conditions for chaos to arise, and to develop methods for suppression of chaotic instabilities. Second, chaotic oscillations can be used for the development of various advanced devices and systems, like noise oscillators, random number generators, secure communication systems, noise radars, and so on. Such applications call for a detailed investigation of properties of chaotic oscillations and for the development of methods for their control. These both topical directions of the chaos theory and applications are addressed in this thesis.

1.1 Chaotic instabilities

There are a number of theoretical and experimental investigations which clearly indicate that chaotic oscillations are typical for physical, chemical, biological, economical, and other systems [1 – 5]. Such oscillations have been repeatedly observed in many practical electronic, microwave, and optical circuits and devices [6 – 18]. The main threat for the stability of practical systems comes from the chaos onset under the condition of weak nonlinearity. At the early stages of the chaos study, it was common opinion that chaotic states are typical only for strongly nonlinear systems. However, it was confirmed later that any degree of nonlinearity, however small, may cause the chaos onset [19 – 22]. There are a lot of typical situations where chaotic states manifest themselves under such conditions, including various types of oscillators with external and parametric forcing [23 – 25], multimode autonomous and nonautonomous systems [26 – 29], distributed systems [30 – 32], and etc. The obtained results indicate, for example, that conventional analysis of the stability of amplifiers with a harmonic input signal is not sufficient. It is necessary to take into account that real signals have multi frequency spectrum. Amplifiers being stable with a harmonic input signal, lose their stability when a multi frequency signal is applied. It was predicted theoretically and proved experimentally [33, 34] that parametric amplifiers have the lowest threshold in terms of the degree of nonlinearity for the chaos onset as compared to other types of amplifiers.

An electron beam can introduce a large enough degree of nonlinearity into a slow-wave structure or in an open resonator for chaotic states to arise. Chaotic oscillations have been observed practically in all types of electron tubes, including klystrons [35], travelling-wave tubes [36], backward-wave oscillators [37], gyrotrons [38, 39], free-electron lasers [40, 41], and orotron-type oscillators [42]. It should be noted that the high Q-factor of the oscillatory system of some of the above tubes (gyrotron, free-electron laser, and orotron) does not prevent the chaos onset. Moreover, it was shown that the threshold for chaos is proportional to $1/Q$.

There are many other physical reasons which can contribute essentially to the development of chaotic instabilities. For example, when studying microwave generators, it was shown that a parasitic low-intensity component in the spectrum of the synchronizing signal [43], or a low-frequency hindrance in a supply circuit [44, 45] initiate the chaos onset and destruction of regular oscillations. Multimode interactions in microwave and optical devices create a variety of additional ways for the transition to chaos. Chaotic instabilities arise as a result of the interaction of only two active modes [46]. It was determined that a passive mode can also essentially change dynamics of microwave generators [47]. However, not only the resonant modes interaction leads to a chaotic state arising, but a nonresonant interaction of two modes can also have a dramatic effect on the system dynamics [47, 48].

The above examples indicate that many classical results of the stability of electronic, microwave, and optical circuits should be revised from the point-of-view of chaotic instabilities arising. Such investigations have already been mainly performed with respect to generation and transformation of harmonic and quasiharmonic signals. In its turn, chaotic instabilities, which may arise during generation and transformation of pulse sequences used in digital communication lines and systems, have not been studied in detail until recent time. During the transfer of pulses via nonlinear circuits, various mechanisms of their destruction can take place, which should be investigated in order to develop methods for the suppression of such instabilities. Results of such investigation are presented in the first part of this thesis.

1.2 Applications of chaotic oscillations

There are several promising directions of the application of chaotic oscillations, which are aimed on the development and implementation of the following devices and systems:

- Noise generators,
- Data processing, compression and storage systems,
- Secure communication systems,
- Cryptographic systems.

The development of noise generators was probably the first practical application of chaos, when it became clear that chaotic oscillations can be relatively easy excited in electronic and microwave circuits. First of such oscillators have been developed on the bases of traveling-wave tubes with a feedback loop with delay [36] and backward-wave oscillators [37]. Late on, it was shown that even simple semiconductor devices and circuits can be used for the development of noise generators. The main advantages of such generators are related with a high output power level of the chaotic oscillations and the possibility to control the output spectrum shape. The same device can be used either as a harmonic oscillator or a noise oscillator depending on the selection of some control parameter value. The main drawbacks of such generators are related with a relatively narrow noise spectrum bandwidth and a sensitivity of the generator output characteristics on the generator internal parameters. It is also a problem to realize the spectrum “flatness” over a wider frequency bandwidth what is typically required in most applications.

The idea of using of chaos for data processing, compression, and storage systems comes from the fact that many nonlinear dynamical systems balance at the border of order and chaos. The transition from one type of motion to another and vice versa can be realized by changing control parameters of the system by very low energy consumption. Based on this, methods of chaotic dynamics have been developed allowing to create devices of principally new types, which can be used for storing, encoding, and processing of large volumes of information [49]. The main approach to the solution of this problem is based on the fact that chaotic attractors contain an infinite number of unstable cycles. Due to this, unlimited number of words can be encoded by such cycles, and the recorded information will be hidden because unstable cycles are unobservable. However, the dynamical system can be disturbed in such a way that the required unstable cycles will become stable and easy observable. This allows to extract the encoded information. Reliable methods allowing to stabilize these cycles or to generate new ones have been proposed for various types of dynamical systems with chaotic behavior.

There is another interesting approach related to the usage of deterministic chaos for recording, storing, and extracting information. The property of the unpredictability of chaotic trajectories for large time intervals is employed. During such motion, the system produces information, and the rate of the information production is increased with increasing the randomness of the system. In this case, information can be memorized and stored as trajectories of the dynamic system. Today, several methods and the corresponding mathematical models exist, which provide the possibility to process the information in described above way [49].

During the past decades, we also observe growing research and application activities focused on using the phenomenon of chaos for the purpose of the development secure communication systems. These activities have been stimulated by the necessity of the development of reliable and convenient tools for signal and message protection from an unauthorized access. This problem is becoming increasingly important because of the extended introduction of electronic systems with wide public access for distribution of documents, banking via the Internet, and so on. These systems require providing confidentiality of transferred information with retaining the possibility of a wide access.

Several approaches have been proposed to build encoding and decoding devices for secure communication systems. In particular, the ability to the self-synchronisation of several coupled chaotic oscillators has been employed [55 – 58]. In this case, the communication line includes a transmitter with a chaotic oscillator producing a chaotic oscillation. The transmitting signal is a sum of the chaotic oscillation and an information signal. On the receiver end, this transmitted signal is used to synchronize an identical chaotic oscillator. The decoded signal is just a difference between the transmitted and the synchronized signal.

The described approach has several drawbacks. The information signal may destroy the synchronous state of the receiver chaotic oscillator, and this leads to the destruction of the signal transfer. Next, the exact extraction of information is not possible, and in order to increase the accuracy, the signal intensity should be rather small, what leads to decreasing the signal to noise ratio.

There is another approach to the realization of the coding and decoding devices, according to which an information signal is directly applied to the chaotic oscillator in the transmitter of a communication line [58]. The transmitted signal becomes a complicated nonlinear function of the chaotic components of the oscillator and the information signal. This transmitted signal, as in the previous case, is used to synchronize the receiver chaotic oscillator. This approach allows potentially for an exact extraction of the transmitted information, even if the signal intensity is large. The drawbacks here are related with the necessity to have the identical signal amplitudes at the transmitter and the receiver ends. Besides, the synchronism of the transmitter and the receiver may be destroyed due to noises and parasitic components in the communication channel.

A radically new solution to the problem of the development of secure communication lines has been proposed in [59, 60]. This solution does not involve the synchronization principle. It is based on the fact that all chaotic trajectories of a dynamical system are placed in the phase space on some integral manifold determined by the governing system of differential equations, for example, by the Lorenz system

[68], or another system with chaotic behavior. Then, an information signal is introduced in the system as an external perturbation, which does not destroy the chaotic regime. The peculiarity of this solution for the realization of secure communication consists in the method of the information decoding. The decoding is realized via an inversion of the equations of the governing dynamical system. The main advantage of the approach consists in the possibility to illuminate the above described drawbacks typical for traditional chaotic masking schemes based on the phenomena of synchronisation of chaotic oscillators.

Another direction of using chaos is related to the development of generators of random sequences to be used in classical cryptographic schemes. As it is well known, the availability of reliable sources of such sequences is of principal importance for secure operation of these schemes.

At the present time, various methods of the generation of random and pseudorandom sequences are used in practice [50 – 52]. One of the approaches is the introduction of a certain random parameter into a deterministic process to generate random sequences. Such generator, for example, is based on reading a deterministic counter state at some random instants of time. In order to obtain truly random sequences in this case, a multiple overflow of the counter in time intervals between the readings should take place.

Another example of a random generator that has become popular is a system based on reading of the timer state of a personal computer. The reading is organized at the moments of pressing arbitrary keys on the keyboard. For example, in order to get a random number of 512 bits in length, it is required to press 32 keys. Such method of generation can be realized at software level, and it does not require any additional hardware.

Hardware generators of random sequences are based on various microscopic or macroscopic phenomena. Examples of microscopic phenomena include:

- Thermal noise,
- Short noise,
- Avalanche noise,
- Photoelectric effect,

- Radioactive decay,
- Radiation of particles.

Methods for the realization of hardware generators on the basis of macroscopic phenomena are:

- Throwing dice,
- Coin flipping,
- Roulette wheeling,
- Reading the frequency of an oscillator,
- Measurements of air turbulence or other atmospheric phenomena,
- Measurements of microphone sound intensity,
- Measurements of fluctuations of expectation time for reading of a computer disk sector.

The list of the phenomena can be further extended. The hardware generators can produce truly random sequences with the absence of correlation in the bits of a generated sequence and with the impossibility of reconstruction of the sequence by using analytical methods. This is their main advantage of the hardware generators over the pseudo-random software generators. The disadvantage is related with a complexity of their practical realizations. Typically, such generators contain a transducer to transform the measured physical value into an electrical signal, an amplifier to increase the signal amplitude, an ADC, and the corresponding software. In addition, when developing such generators, it is needed to take into account the sensitivity of generator to the environmental conditions (temperature, humidity, pressure), and the dependence from the hardware platform on which the device should work.

The usage of the principle of pseudorandom generation allows to get rid of the above problems. There are a great variety of methods for the development of pseudorandom generators [54]. Such generators have a high operational speed, acceptable statistical properties, but unsatisfactory characteristics from the point of view of the structural security.

The increasing requirements to the development of reliable and convenient tools for information protection call for using alternative approaches to the random number generation. One of such approaches is based on using dynamical chaos [52, 61]. From the general standpoint, it seems that deterministic systems with chaotic behavior can be used as generators of random sequences combining the advantages of software pseudorandom generators and physical noise sources [61]. Really, such generators can be realized as software application, and, therefore, they are convenient for a wide practical usage. Chaos based generators, like the hardware generators, can produce truly random sequences of an arbitrary length. In addition, such generators provide reproducible random sequences and can provide a high rate of the bit generations. The above indicated potential advantages have been the main motivation for our investigation of generators of random sequences on the bases of deterministic systems with chaotic behavior. The results obtained in this direction are presented in the second part of the thesis.

1.3 Goals and outline of the thesis

1.3.1 Goals

The first goal of this thesis was to determine mechanisms and conditions for chaotic instabilities arising during transition of trains of pulses via nonlinear circuits. In order to achieve this goal, several issues were addressed:

- Development of the corresponding mathematical model and elaboration of methods for its study,
- Analytical and numerical studies of the conditions for chaos onset,
- Investigation of properties of chaotic oscillations,
- Experimental investigation of the destruction of trains of pulses in a nonlinear circuit, and
- Comparison of theoretical and experimental results.

The studied oscillator is described by a generalized Duffing equation, which is an adequate model to describe stability of a number of electronic, microwave, and optical devices. The simplest physical oscillator, which is described by such equation, is a RLC circuit with a nonlinear capacitor, or a microwave or optical cavity with nonlinear element or media.