## 5. Conclusion

The algorithm of determination the hydrogen ions saturation level makes possible to standardize the assessment methods of the soil pH level and soil resistivity, to simplify and speed up the preparation of the device to measurement, and to reduce the subjective factors influence on the measurement conducted.

Wide application of these methods in the devices for estimation of the soil corrosion activity and the effectiveness of the cathodic protection equipment will reduce labour and material costs on the diagnosis and maintenance of the pipelines, identify areas of the corrosion risk and develop recommendations for additional preventive measures to protect the pipelines.

*References*

1. Дамаскин Б.Б. Электрохимия / Б.Б. Дамаскин, О.А. Петрий, Г.А. Цирлиа. 2е изд., испр. и перераб. М.: Химия, КолосС, 2006. 672 с.
2. Иванов Ю.А. Аспекты развития и применения электроаналитических систем // Материалы симпозиума с международным участием «Теория и практика электроаналитической химии» (Томск, 13-17 сентября 2010 г.). Томск, 2010. 185 с.
3. Васильев В.П. Аналитическая химия. В 2 кн. Кн. 2. Физико-химические методы анализа: Учеб. для студ. вузов, обучающихся по химико-технол. спец. 2-е изд., перераб. и доп. М.: Дрофа, 2002. 384 с., ил. С. 179-181.
4. Хижняков В.И. Противокоррозионная защита объектов трубопроводного транспорта нефти и газа. Томск: Изд. ТПУ, 2005. 151 с.

*Scientific adviser: V.V. Korobochkin, Professor of TPU; linguistic adviser: T.S. Mylnikova, senior teacher of TPU.*

*D.S. Kozhevnikov, N.P. Shatilov*
*Tomsk Polytechnic University*

## Hardware and software implementation of telecommunication systems components

Hardware implementation of telecommunication systems components is currently considered to be of great interest for researchers and developers since this implementation can be faster than software implementation. Nevertheless, software implementation sometimes can be more flexible and easily debugged. Note that numerous telecommunication components are implemented in the form of "hard" logic, and hardware implementation of high level telecommunication protocols is being investigated. Therefore, clear criteria to evaluate the effectiveness of hardware implementation versus software one. In this paper, the criteria selected are time and speed of input data processing. The preliminary results of evaluating the effectiveness of hardware implementation as the components of the telecommunication system are shown.

In particular, since security of information transmitted over communication channels is of current importance in today's world, the paper examines the possibility of hardware encryption. U.S. Standard DES is chosen as an encryption algorithm.

In 1972, the National Bureau of Standards (National Bureau of Standards, NBS) initiated a program for protection of communication lines and computer data. One of the goals of the program was to develop a single, standard cryptographic algorithm. To develop the product the following basic requirements were to be met: the algorithm must be tested and certified, easily accessible, and various cryptographic devices using the algorithm must interact. Thus, the encryption algorithm DES (Data Encryption Standard) was designed.

DES is a block cipher that transforms the plaintext data by 64-bit blocks. The 64-bit plaintext block is applied to the algorithm input and the output is removed from a 64-bit block of ciphertext. Note that DES is a symmetric algorithm, i.e. the same algorithm and key are used for data encryption and decryption (except for small differences in the use of the key).

The key length is 56 bits. The key is typically represented by a 64-bit number, however, every eighth bit is used for parity checking and it is ignored. The parity bits are the least significant bits of the key bytes. According to DES, the key, which may be any 56-bit number, can be changed any time. Nevertheless, several key numbers are known to be weak in terms of stability of the cipher key as the initial value in the encryption algorithm is split into two halves, and each of the halves moves independently. The vector one half of which consists of ones and the second half of zeroes may serve as an example. In this case, the same key is used for all stages of the algorithm. The main operations in the algorithm are permutation and diffusion. Figure 1 shows a diagram of DES algorithm.

The key length is 56 bits. The key is typically represented by a 64-bit number, however, every eighth bit is used for parity checking and it is ignored. The parity bits are the least significant bits of the key bytes. According to DES, the key, which may be any 56-bit number, can be changed any time. Nevertheless, several key numbers are known to be weak in terms of stability of the cipher key as the initial value in the encryption algorithm is split into two halves, and each of the halves moves independently. The vector one half of which consists of ones and the second half of zeroes may serve as an example. In this case, the same key is used for all stages of the algorithm. The main operations in the algorithm are permutation and diffusion. Figure 1 shows a diagram of DES algorithm.

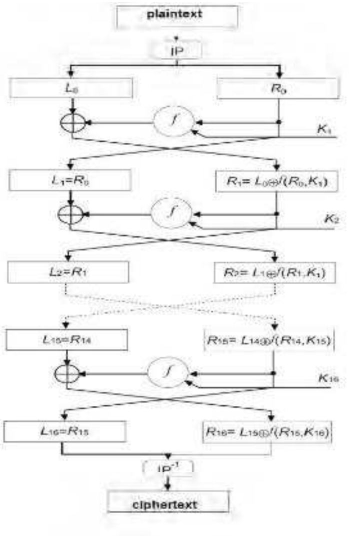
plaintext
IP
$L_0$
$R_0$
$f$
$K_1$
$L_1=R_0$
$R_1= L_0\oplus f(R_0,K_1)$
$f$
$K_2$
$L_2=R_1$
$R_2= L_1\oplus f(R_1,K_1)$
$L_{15}=R_{14}$
$R_{15}= L_{14}\oplus f(R_{14},K_{15})$
$f$
$K_{16}$
$L_{16}=R_{15}$
$R_{16}= L_{15}\oplus f(R_{15},K_{16})$
$IP^{-1}$
ciphertext

Fig. 1. DES algorithm

The DES algorithm was implemented with the hardware on the FPGA Cyclone II Starter Development Board of Altera (Fig. 2).

Fig. 2. Exterior of the Cyclone II Starter Development Board

FPGA technology is widely used and based on the multiplication-summation blocks (in particular, signal processing and DSP), and logic gates (usually based on truth tables of corresponding functions), and their switching units [2]. The FPGA technology is commonly used for signal processing and its architecture is more flexible than that of CPLD, as an example. Program for FPGA is stored in shared memory which can be made both on the basis of volatile SRAM cells (the program is not retained if the power supply of the chip fails), and on the basis of non-volatile memory cells of Flash-jumpers or antifuse (the program is saved when the power supply fails). If the program is stored in volatile memory, every time the circuit is switched on it is to be reconfigured with a bootloader, which can be embedded in the board based on FPGA. Slower digital signal processors can be used as alternative FPGA, however, research in the use of such processors with hardware encryption are beyond the scope of this paper.

In addition to hardware implementation, software implementation of the DES encryption has been developed. The corresponding program was written in C + + using the integrated environment of Microsoft Visual Studio 2013 Express Edition.
A 64-bit vector (plaintext block) and a randomly generated key of the same dimension are processed by the program. The output is a 64-bit block cipher. Note that the software implementation uses the PLO and for treatment of Boolean vectors greater than 32 bits "Long Boolean vector class" was implemented.

The implementation acts were compared, and the time spent on encryption using hardware and software implementations was chosen as one of the evaluation criteria. In particular, a plurality of sequences is experimentally determined for each of the implementations, and the total time of the input data processing was compared.

To achieve a maximum encryption speed the fastest way to read information for encryption is required. The optimal solution in this case is to read the data from SD-card or business data interface, which will insure speedy transfer of the data to the FPGA. USB or Ethernet is an example of this type of interface. Note that the solution of this problem, namely, the choice of a suitable interface for calculation of the "net" time hardware encryption is of interest for further research, and currently, the memory is realized in the FPGA chip. This fact allows use of the 64-bit memory from which 64 bits of a plaintext can be read simultaneously. The experiments to estimate the time of the encryption are being performed by the authors.

Note that in addition to the speed and time data processing, there are other criteria to evaluate the two implementations. In the future we plan to evaluate other implementations to compare the efficiency, reliability, quality and other parameters. The issue of testing is a special problem in the design of the hardware, and in the future the authors propose to use software implementation for hardware testing.

These tasks offer prospects for further research.

The research is supported by the Ministry of Science and Education of the Russian Federation, Project No 5.1307.2014.

*References*

1. Schneier B. Applied Cryptography. Protocols, Algorithms and Source Code in C. Second Edition B. Schneier. Wiley. 1995. Pp. 226-256

2. Steshenko V.P. FPGA ALTERA company: designing signal processing devices. M.: DODAKA, 2000. p. 128.

*Scientific adviser: S.N. Torgaev, docent of TPU; linguistic adviser: T.S. Mylnikova, senior lecturer of TPU.*