MATHEMATICAL AND COMPUTER MODELING

UDC 004.056.55

STEPAN BILAN,
ANDRII DEMASH

HIGH PERFORMANCE ENCRYPTION TOOLS OF VISUAL INFORMATION BASED ON CELLULAR AUTOMATA

This article describes a method of encryption of visual information, based on the use of cellular automata. This method allows you to solve problems with noise errors in deciphering information, low-speed, low resistance to cracking, as well as move away from the use of generators of noise signals in the known methods of encryption of visual information. Analyzed modern encryption methods of visual information, as well as problems encountered in their implementation and use in the communication channels. The article also presents the structure of the device that implements - encryption is the visual information based on cellular automata, programs, texts, diagrams and results of the encryption method, the basic characteristics of the used field-programmable gate array. The essence of the method is to encrypt the visual information by overlaying additional transformations besides the usual encryption. The first additional conversion is carried out by the chosen method of encoding and digitizing images. The second transformation is to select the sequence of bit layers and their principles scan each block. Data conversions in the form of numerical values are used as additional fields to the key. In addition, the key is not given as a ready-bit sequence, but as the operation code, the units form a key sequence. Options propagation path of the excitation signal and a three-dimensional map of a cellular automaton states belong to the key sequence. The formation of pseudo-random key range increases reliability and protection to burglary resistance. Due to the three-dimensional image coding, the use of technologies of programmable integrated circuits and cellular automata increases speed encryption. The method allows you to create a key range implicitly, that reduces the probability of selecting an opponent. Encryption tools are implemented on cheap field-programmable gate array with high performance in speed, allowing you to encrypt visual information in real time during its transfer via communication channels.

Keywords: visual information, encryption, video, cellular automata, Field-Programmable Gate Array.

Introduction. Today, video transmission in modern computer networks, mainly in the Internet is one of the most important components in the structure of data transmission. In this case part of this component increases with throughput and expansion of the Internet in the world. Today, video transmission is used in different systems for monitoring, surveillance, video telephony, recording and transmitting large amounts of video data in a personalized television and many other systems. Statistics of reputable organizations engaged in research on the Internet, said that most of the global traffic today is one or the other the video information. Data exchange of this kind is sufficient demanding to technical characteristics of data channel, such as channel bandwidth, transmission delay and the amount of information that is lost in the process of transmitting. Communication channels with the so-called “guaranteed quality of service” are quite expensive, so we meet rare with them. Data networks usually have a heterogeneous structure, which also negatively affects the final results.

Furthermore, when exchanging sensitive information to compromise by public channels, it shows in its entirety a need to protect data from unauthorized access, while ensuring the availability and integrity [1].

Statement of the Problem. Today, there are many methods and means for encrypting video information that represent the image as a sequence of binary bits. The corresponding sequence is divided into blocks, which then by known methods are encrypted. However, images forming by large arrays of bits, and wherein the length of the keys is limited, which could potentially allow to crack

encrypted numerical sequence. Improve the quality of encryption allows the use of the special features and additional tools are based on the original form the key sequence key. In addition, the constant change of key sequence in time lowers the degree of cracking algorithm. To achieve a constant functional change in key sequence is use of cellular automata (CA).

Review of existing methods and tools for video encryption. At the moment, for the protection of visual information used a number of methods [2-4], which is to transform the image based on unitary mathematical transformations. Image is subject to a unitary mathematical transformation (Fourier transform), and the resulting transform coefficients are encrypted by adding a mask – a key that has a random phase response.

Also known methods employ digitizing of images that simplifies the implementation of such encryption techniques.

The main problems of these methods have a weak protection of information when deciphering since noise errors reduce the quality of recovery. Furthermore, the methods are characterized by low speed if realized through the use of image transformations. In the considered methods there is a possibility to define probable combinations by consecutive search and decryption of images. The problem is, the use of the Fourier transform, and additional transformation of digital images, as well as the additional transformation, module and phase signals encryption.

At the site [5] is detailed information of a digital encoder that implements operations encryption / decryption full-PAL / NTSC-video in real-time by row permutation. The video with the audio is digitized and are recorded in video memory device. The first 22 row of each television fields are used for the transmission of audio and proprietary information. The rows are permutated randomly in the half frames. To the video codec output the encrypted audio and video information are receives. The law of permutation of rows and pixels in each half frame is changed. Long-term key length of 256 bits used, which can be stored for a long time in a memory or be generated by the operator. For this purpose are used a generator that provides an infinite sequence of key bits.

In this coder device is also the problem with the formation of a key sequence as for encryption and decryption at the receiving side. Such a generator gives a key bit sequence, but does not carry out its function of indirect form. Since the generators are linked to the generation of noise signals, there exists the need for coordination of key signals at the transmitting and receiving sides.

In [6] discusses possible approaches to pre-encryption and encryption with compression. The main focus is on the encryption of the compressed data. Thus, encryption performed by the known algorithms with known methods of forming of the key gamma.

It is also known strip – image encryption method [7, 8], which is a video signal for cutting the strip and forming a signal sequence bit of chopped strips. From these strips can be formed by the matrix, which are subjected to the application of matrix operators. Matrix processing used to delete noises and masking image encryption method [9-11].

These methods are needed to be improved in terms of the representation of the image and the formation of a key sequence, adapted to its dimensions.

Necessary tools and initial data for the implementation of encryption video method. For a description of encryption method of video data based on the CA, we introduce the basic definitions of the input data and means of preparation of the initial states.

As an input data are used: input image, means of forming the encryption key and decryption.

The input image is represented as an array of numbers, which encodes each point of the image (color and halftone).

$$I_{in} = \{a_{i,j}\}; \left(i = \overline{1,n}; j = \overline{1,m}\right). \quad (1)$$

The array of numbers is determined by the dimension which depends on the values of n and m.

Means of formation of key consist of a binary array of numbers and binary states maps.

A binary array of numbers describes the trajectory of the signal forming of key encryption and decryption in the field commensurate with the input image. This array is represented by the following model

$$V = \{v_{i,j}\}; v \in \{0,1\}; \left(i = \overline{1,n}; j = \overline{1,m}\right). \quad (2)$$

Array V presents by the CA, each cell has a neighborhood of cells formed by the Moore neighborhood. Moore neighborhood represented an array of cells

$$B_{i,j} = \{b_{i,j,l}\}; l = \overline{1,8}; (i = \overline{1,n}; j = \overline{1,m}), B \subset V, \quad (3)$$

Map of binary states of the spacecraft is an array of cells of the same dimension in which the cell can be in a state of logical "0" or "1"

$$C = \{c_{i,j}\}; c \in \{\overline{0,1}\}; (i = \overline{1,n}; j = \overline{1,m}). \quad (4)$$

Encryption model in a general form represented as

$$S_{en} = f(I_{in}, K_{en}), \quad (5)$$

where K_{en} – the key bit sequence that is used to encrypt.

Such a model is presented in a general form. For a detailed description of encryption method array the image is divided into sub-arrays, which are binary sections of the original array

$$I_{in} = \{D_{\alpha}\}; (\alpha = \overline{0,p}), \quad (6)$$

where p – the number of bits of binary code that encodes the value of brightness and color of each cell of the input image. Each binary array is a set of cells with a logic "0" and "1".

$$D_{\alpha} = \{d_{\alpha,i,j}\}. \quad (7)$$

The resulting binary arrays are divided into blocks of predetermined length. Usually, each block represents one string of length n of cell array.

For convenience of in each encryption block is 8 bits and selected as Moore neighborhood, which is composed of 8 cells. By choosing the smallest unit that is involved in the encryption, the encryption process can be represented by the following model

$$S_{en,z} = f(I_{\alpha,z}, K_{en,z}), \left(z = \overline{1, \frac{n \cdot m}{z}}\right), K_{en,z} = B_{i,j} = f(V, C), K_{en,z} = B_{i,j} = f(V, C). \quad (8)$$

The model is valid for the one elementary unit. A logical function XOR is used as a mixing function. Image is served encrypted bit sequence which is transmitted to the addressee. The method is characterized by the formation of an indirect key bit sequence

$$K_{en} = g(CA_{tr}, CA_{st}), \quad (9)$$

where CA_{tr}, CA_{st} – set of states of the trajectory CA and state CA.

Such formation of the key bit sequence it improves resistance of the algorithm to cracking. To improve the quality encryption it also allows change the map of states over time, which is described by the model

$$K_{en}(t) = g[CA_{tr}, CA_{st}(t)]. \quad (10)$$

Parameter time t indicates a change in state of states maps at each time step of encrypting.

Software implementation of the algorithm requires a lot of time spent on the result of the encryption that in real-time systems the desired characteristics do not produce. Therefore, to reduce the amount of time the hardware implementation allows. From these positions it is effective to use an FPGA.

Description of the encryption method of the video data, based on CA. On the algorithmic and structural level the image data encryption method based CA is described in [12].

According to this method, the initial image is digitized and represented as an array of numbers that are presented of binary codes arrays. Each point represents a binary code. The resulting numeric array is divided into a binary array of layers, each of which contains the values of bits of codes with corresponding weights. An example of this separation is shown in the fig. 1.

Each resulting binary array is divided into blocks, which can be of different lengths. Typically, each block has a block length that is equal to the length of the row. For our example, the first binary array is divided into blocks, as shown in fig. 2.

To encrypt the blocks is used a key sequence that is formed by using the trajectory signal the forming CA of the key bits and CA initial condition. Examples of these CA are presented in fig. 3.

The principle of forming the key bit sequence is the following.

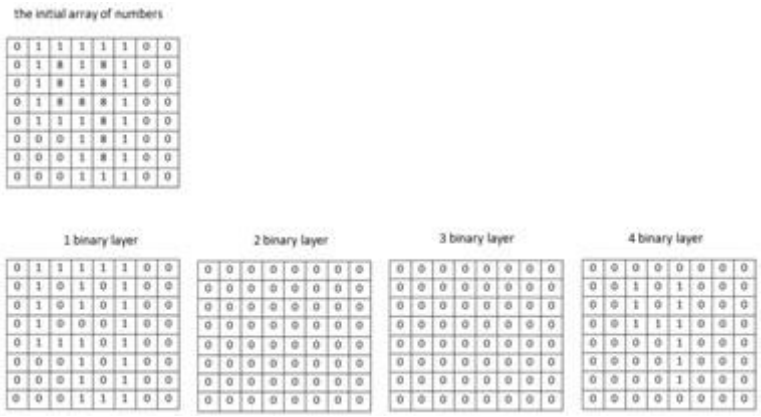

Figure 1 – An example of splitting of the numerical array of the digitized images into the binary layers

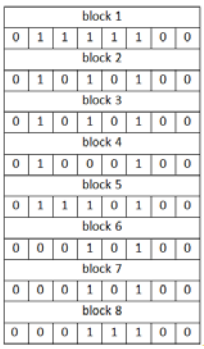

Figure 2 – An example of splitting of the binary array into the blocks

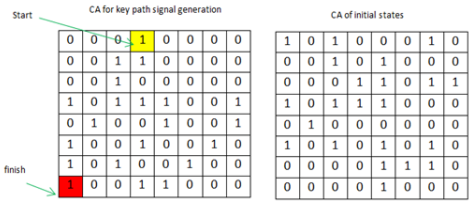

Figure 3 – An example of the initial states of trajectory and conditions CA's

Starting with an initial trajectory cells (cell yellow in fig. 3) the signal on every cycle time moves towards neighboring cells that set to logic "1" on the field CA. Each of trajectory CA cell is combined with the corresponding cell of initial states CA. If cell of CA trajectory is exciting on the setting cycle time, then a single signal is arriving from the output of a corresponding cell to an input of the cell of CA states. This cell has a neighborhood of cells organized on a Moore neighborhood. The states of the cells neighborhood this cell are form the corresponding 8-bit key sequence (see fig. 4).

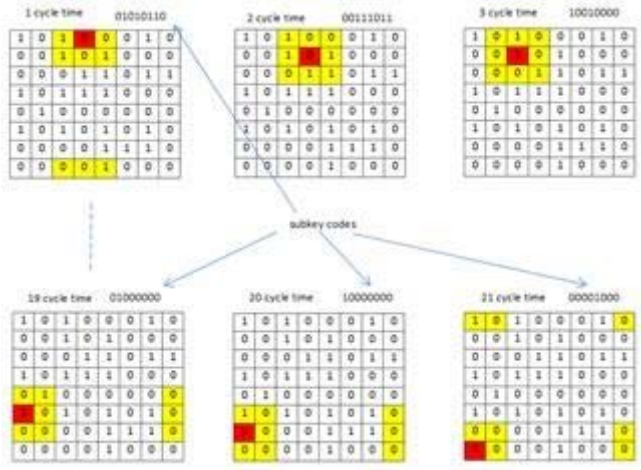

Figure 4 – An example of the initial states of trajectory and conditions CA's

Key bits are participating in obtaining cryptogram that is supplied to the receiving side. In this method, the key sequence is represented in an implicit form that improves the quality of the encryption.

To decrypt the received cryptogram subkeys codes formed similarly as the encryption codes from a cells state, that are located in corresponding positions of all discrete image elements. It is forming the cell codes, matrix field, the number of which is determined by the number of bits of the code discrete value of image. Matrix field is scanned for each block consistently.

The hardware implementation of the method. To implement an encryption method of visual information based on CA was selected Cyclone II FPGA chip (EP2C35F672C6) Altera Corporation, which belongs to the family of inexpensive entry-level FPGA. The main IC characteristics are shown in tabl. 1.

Table 1 – Main characteristics of the chip EP2C35F672C6

Parameters	Value
Number of cells	33216
Number of memory units M4K (4 kb)	105
Number of IC Pins, which are available to the user	475
Cost	approximately 150$

In the terminology of Altera FPGA cell called logic elements (logic elements, LE). Each logic element of chip Cyclone II includes the following main components (see fig. 5):

– transformation table (look-up table, LUT) with 4 outputs, which allow the implementation of an arbitrary Boolean function of four arguments;

– programmable trigger, which can operate in mode D, T, JK or RS;

– programmable internal connections.

When programming the FPGA transformation table are set value corresponding to each of the 24 sets the value of its pins. Multiplexers allow the use or transformation table, or trigger, or a serial connection. It is also are set when programming the internal connection between cells on-chip FPGA.

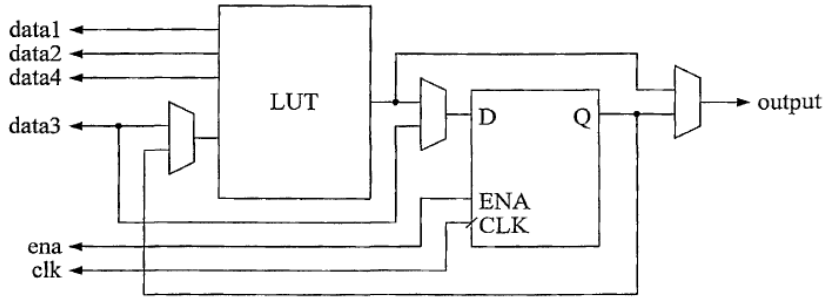

Figure 5 – The structure of the logic element of Altera Cyclone II FPGA

Altera Quartus II software was used as a tool of the development, and as the main way of the description of the circuit - the AHDL language [13, 14].

Fig. 6 shows a block diagram of device implementing the visual information encryption method, where IDU – image digitization unit, SCGU – sub keys codes generating unit, BEU – block encryption unit, CL – communication line, BDU – block decryption unit, DIRU – digital image reproduction unit.

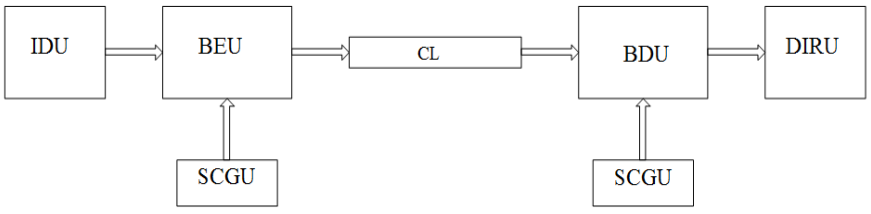

Figure 6 – Block diagram of device implementing the encryption method of visual information

In fig. 7 shows the functional block diagram of the project that implements the IDU, SCGU and DIRU. To implement BEU and BDU can use algorithms block encryption (DES, AES, IDEA and others) [13, 15].

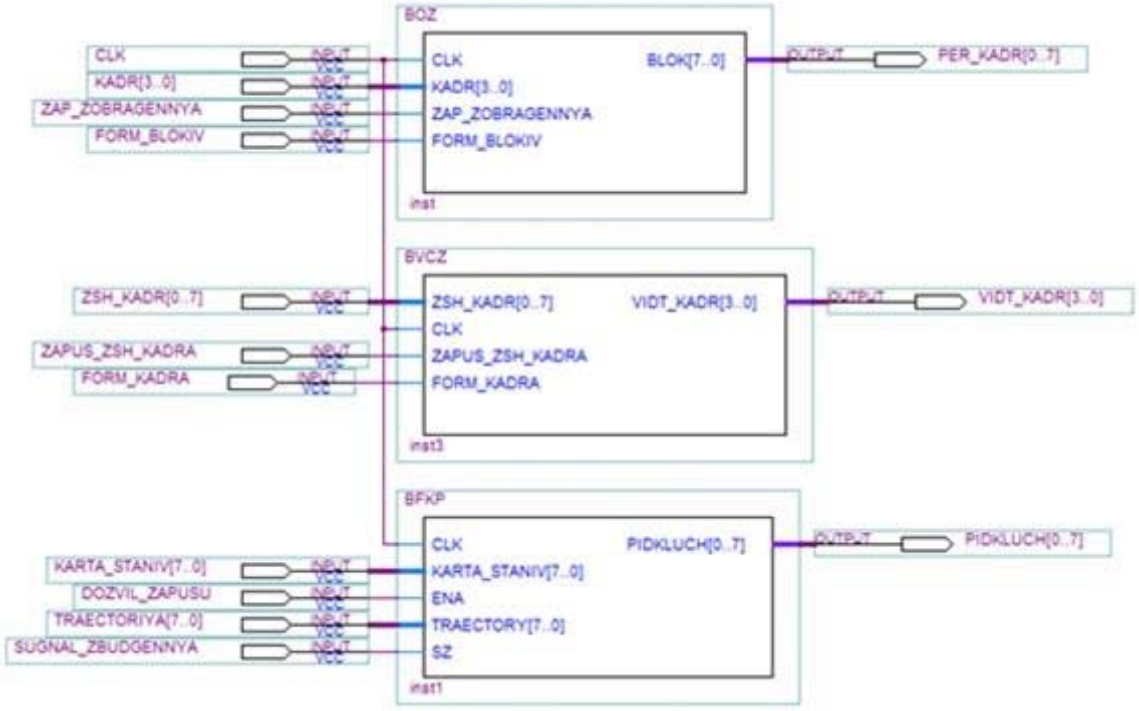

Figure 7 – The project Functional diagram of the IDU, the SCGU and the DIRU

The image that you want to encrypt, digitize by the way of transformation into a discrete form. Digitizing raster image is done on a matrix uniform cell structure. Each cell has its own input optical aperture, the geometric shape and size of which depends on the level of images discretization. Each cell makes the conversion the corresponding discrete of single field of the input image in the code that encodes the color and intensity of light, this forms a single discrete image. Thus, the digitized image given by the set of codes which are stored in the cells of the matrix cell of a homogeneous environment.

This environment is also divided into horizontal layers of the matrix consisting of the corresponding bits of all cells. For example, the first matrix layer (bit-section) is formed in the first bits of cell codes, and so on (see fig. 1).

With help of this cellular environment the analog image is supplied by a three-dimensional structure which formed its three-dimensional code.

To carry out its encryption is performed sequentially scan each matrix cell layer in a predetermined sequence. Scanning is carried out in parallel and parallel to each block is read and sent to encryption unit. The unit is a predetermined group of bits, which can be fed to row or other form (see fig. 2).

Thus, the image sending to the input of the encryption is carried out in a distorted form. Such form is due to given law of scanning, which belongs to the key data.

The above described transformations the IDU implements the described in VHDL-code (see fig. 8).

Figure 8 – Digitizing image unit

Operations of transformation by matrix cell homogeneous environment are performed on the rising edge of the clock signal CLK. Through the 4-bit input KADR [3..0] with a positive edge of the signal ZAP_ZOBRAGENNYA to IDU (Register CC [255..0]) loaded the numeric equivalent of the digitized image and carried it into horizontal separation on matrix layers.

```
IF ZAP_ZOBRAGENNYA THEN
   CC[].ENA=VCC;
   CC[63..0].D=(KADR[0],CC[63..1]);
   CC[127..64].D=(KADR[1],CC[127..65]);
   CC[191..128].D=(KADR[2],CC[191..129]);
   CC[255..192].D=(KADR[3],CC[255..193]);
 ELSE
    CC[].ENA=GND;
 END IF;
```

On the positive edge the signal FORM BLOKIV carries out formation of 8-bit units, which further through the 8-bit output BLOK [7..0] come in BEU. Register DD [7..0] is used for alignment wavefront.

```
IF FORM_BLOKIV THEN
   CC[].ENA=VCC;
   DD[].ENA=VCC;
   CC[]=(0,0,0,0,0,0,0,0,CC[255..8]);
   DD[]=CC[7..0];
   BLOK[]=DD[];
ELSE
    BLOK[]=GND;
    CC[].ENA=GND;
    DD[].ENA=GND;
 END IF;
```

The diagrams which are describe the behavior of the device, shown in fig. 9, 10.

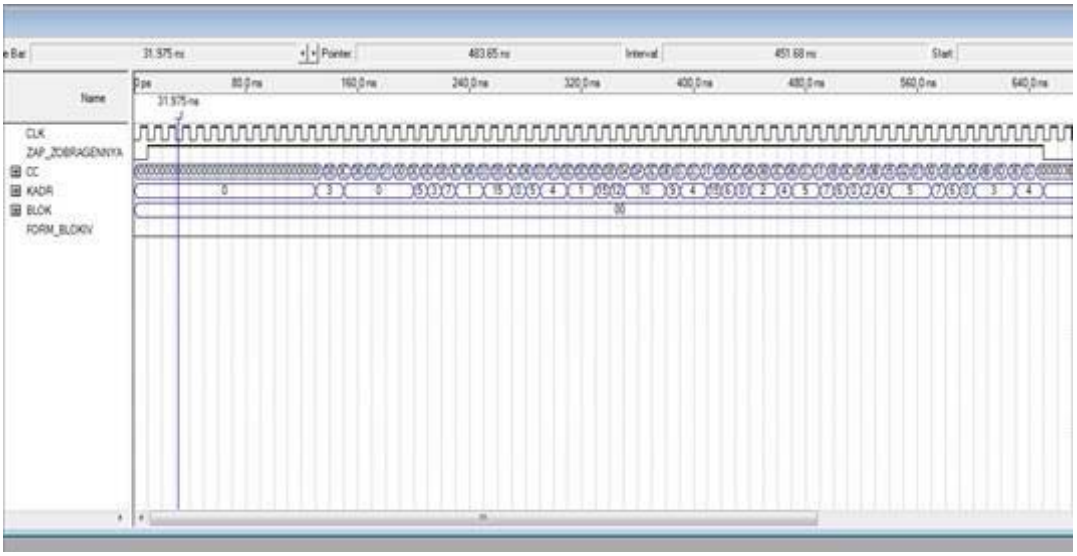

Figure 9 – Writing of the numerical equivalent of images in IDU

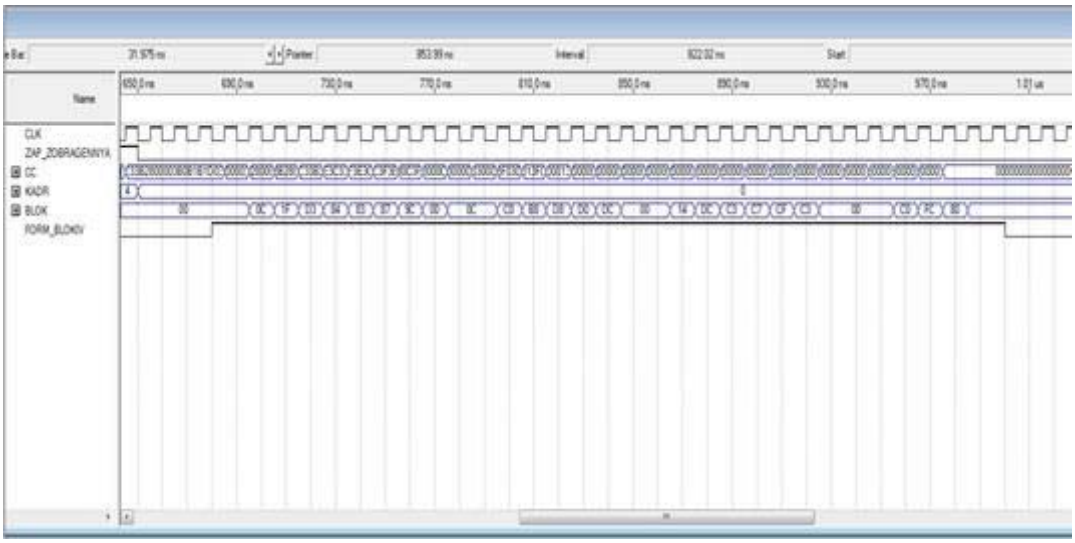

Figure 10 – Formation of blocks for BEU

For the formation of subkeys codes that come to BEU used CA on which the unit trajectory is stored and the map of states (see fig. 3). By projected trajectory from cell to cell is transmitted the drive signal that sets the cell to the excited state (see fig. 4). On each step of signal transmission the formation of a code excitation is carried out forming subkey.

The above-described transformation implements the SCGU that described by AHDL-code (see fig. 11).

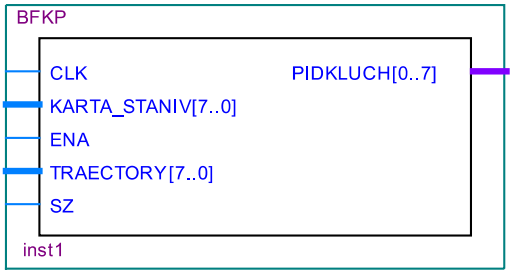

Figure 11 – Block of formation of the subkeys codes

Operation of subkeys codes forming are performed on a rising edge of synchronization signal CLK. Across8-bit input KARTA STANIV [7..0] with positive edge signal ENA to SCGU (Register DD [0..7] [0..7]) is loaded the states map of CA. With a positive edge of the signal SZ SCGU through an 8-bit input TRAECTORY [7..0], reads the propagation path of the excitation signal of CA and generates codes of subkeys that come in BEU through the an 8-bit output PIDKLUCH [0..7] (see fig. 12).

```
DD[][].D=(DD[1..7][],KARTA_STANIV[]);
IF SZ THEN
   CASE TRAECTORY[] IS
   WHEN 1 =>
         PIDKLUCH[0]=DD[7][0];
         PIDKLUCH[1]=DD[7][1];
         PIDKLUCH[2]=DD[0][1];
         PIDKLUCH[3]=DD[1][1];
         PIDKLUCH[4]=DD[1][0];
         PIDKLUCH[5]=DD[1][7];
         PIDKLUCH[6]=DD[0][7];
         PIDKLUCH[7]=DD[7][7];
```

```
WHEN 64 =>
        PIDKLUCH[0]=DD[6][7];
        PIDKLUCH[1]=DD[6][0];
        PIDKLUCH[2]=DD[7][0];
        PIDKLUCH[3]=DD[0][0];
        PIDKLUCH[4]=DD[0][7];
        PIDKLUCH[5]=DD[0][6];
        PIDKLUCH[6]=DD[7][6];
        PIDKLUCH[7]=DD[6][6];
WHEN OTHERS =>
        DD[][]=GND;
 END CASE;
```

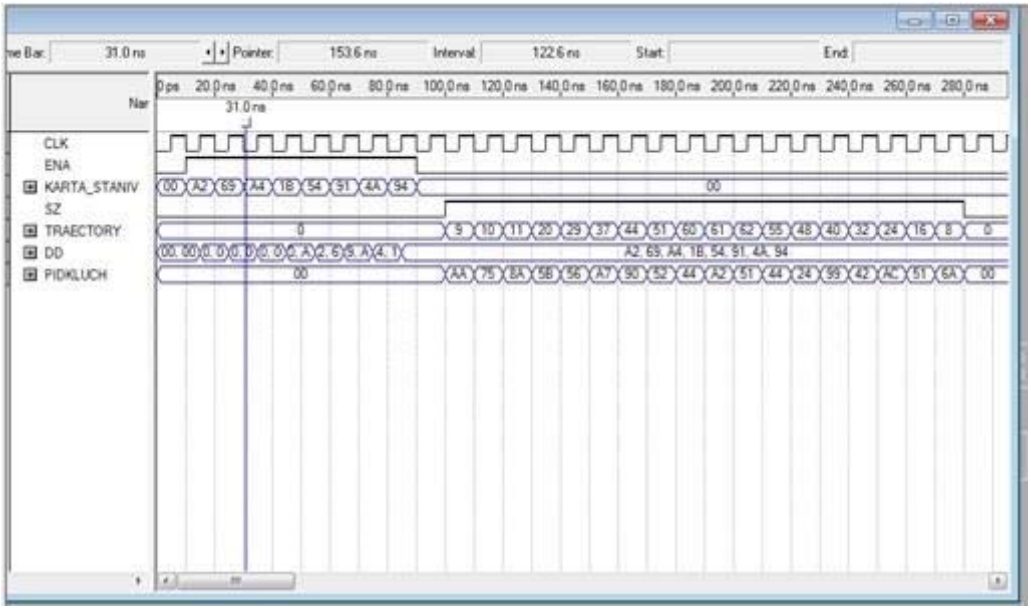

Figure 12 – The work of SCGU

BEU performs data encryption of sequence and describes the image, using the existing code of subkeys. The resulting cryptogram is sent to the communication line. On the receiving side is decoding is performed.

To decrypt the received cryptogram the codes are forming the subkeys similar as well as for encrypt. Bit states codes are located in corresponding positions of all discrete image elements. They form the codes of cells, matrix field, the number of which is determined by the number of bits of the one discrete value image.

Formation of a single discrete value, images are performing by DIRU (see fig. 13).

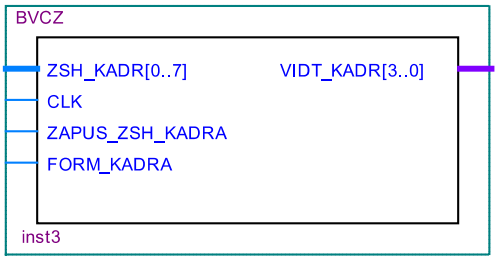

Figure 13 – A digital image reproduction unit

Forming operation of a single discrete value is performed on the rising edge of a synchronization signal CLK. Through 8-bit input ZSH KADR [0..7] with a positive edge of the signal to ZAPUS_ZSH_KADRA to DIRU (CC [255..0]) the blocs are recording of the image frame received from the BDU (see fig. 14).

```
IF ZAPUS_ZSH_KADRA THEN
    CC[].ENA=VCC;
    CC[].D=(ZSH_KADR[],CC[255..8]);
ELSE
    CC[].ENA=GND;
END IF;
```

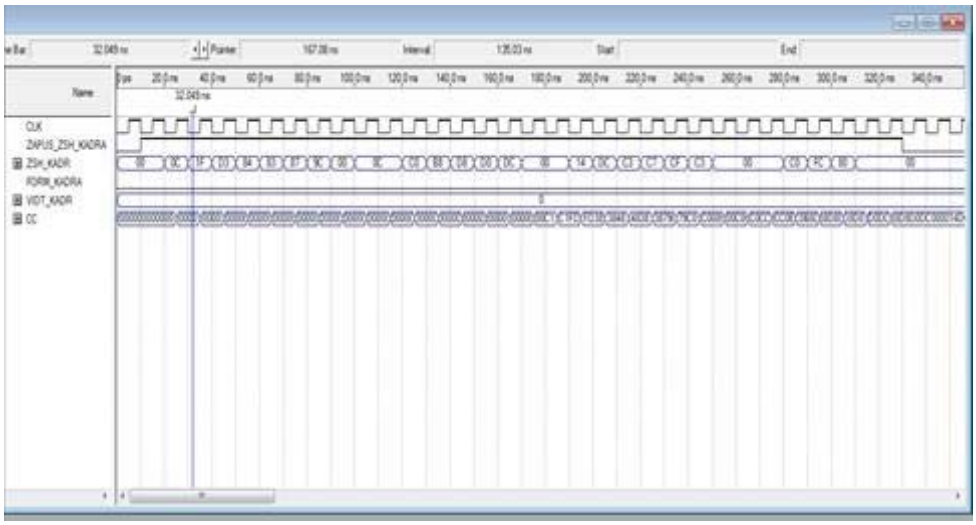

Figure 14 – Recording of blocks of image, received from BDU

On the positive edge the signal the FORM KADRA is performed formation and output via a 4-bit output VIDT_KADR [3..0] of the numerical equivalent of the image (see fig. 15).

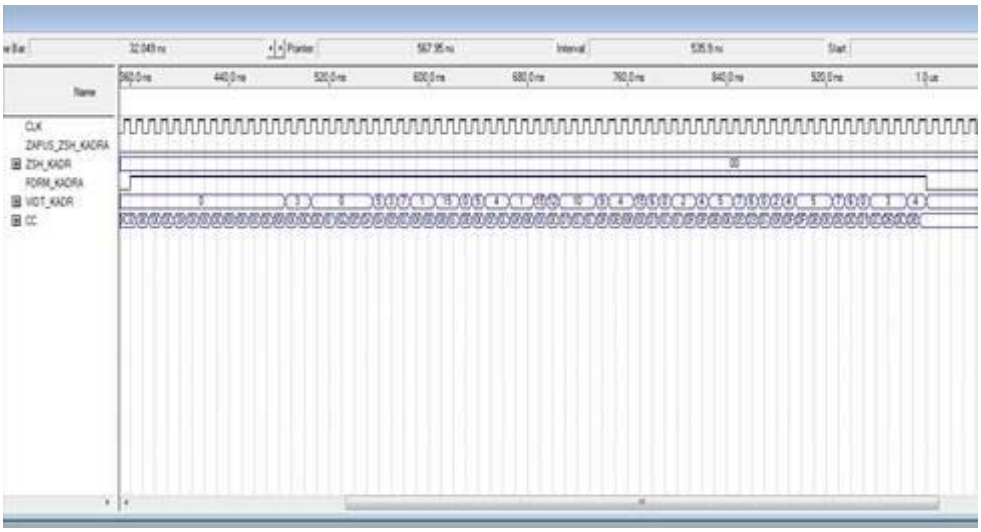

Fig. 15. Formation and output of a numerical equivalent of the image

Main characteristics of the implementation are shown in the tabl. 2.

Thus, the visual information is encrypted by overlaying additional transformations besides the usual encryption. The first additional transformation is carried out by the chosen method of encoding and digitizing images. The second transformation is to select the sequence of bit layers and their principles scan each block. These transformations in the form of numeric values are used as additional fields of the keys.

Moreover, the key is given no ready bit sequence, and as codes of operations performed by SCGU. The key sequence has variants of the propagation path of the excitation signal and the two-dimensional map of states. The formation of a pseudo-random key range increases the reliability of protection and resistance to cracking.

Table 2 – Main characteristics of the implementation

Parameter	speed specifications
The nominal clock frequency	100 MHz
nominal speed	23,8 Gbit/s
The maximum clock frequency	420 MHz
the maximum speed	56,7 Gbit/s
the FPGA resources using	
The total number of logic elements	973 / 33 126 (3%)
The combined without trigger	385
Triggers are a part of a combination	588

Due to the three-dimensional image coding, the use of FPGA technology and the CA the speed of encryption are increased.

Conclusion. The proposed method allows us to form the key gamma in implicit form, which reduces the probability of selection by the opponent. Encryption tools are implemented on low-cost FPGAs with high parameters of speed that allows you to encrypt the video data in real time in the transmission of its channels.

Further research. In future the authors plan to implement the formation of a key range for the entire time video encryption on the basis of research. This will allow moving away from the stationary keys. In fact, the key will function of the initial settings and will be implemented in CA.

REFERENCES

[1] "Encryption methods of video transmitted over the Internet". [Online]. Available: http://eurocomplect.com/sposobyi-shifrovaniya-videoinformatsii-peredavaemoy-cherez-internet.php. Accessed on: Dec. 17, 2015.

[2] L. Finkelstein, J. Kosmach, and J. Smolinske. "Method and apparatus for providing cryptographic protection of a data stream in a communication system", *US Patent Appl. EP* 0671092 A1, Sept. 13, 1995.

[3] S.V. Valov, A.Ia. Olkhovskii, O.A. Pavlov, Iu.F. Pakhomov, and V.G. Starodubtsev, "Speech signals encoding and decoding device", *RU Patent Appl.* 2050698, Dec. 20, 1995.

[4] Yu.B. Rytsar, M.P. Kozlovskyi, M.V. Shovheniuk, S.V. Voloshynovskyi, and Z.D. Hrytskiv, "The method of visual information securing", *UA Patent Appl.* 22285, June 15, 2001.

[5] A. Volodin, V. Mitko, and E. Spinko, "Video Encryption-Developer Workshop". [Online]. Available: http://www.chipinfo.ru/literature/chipnews/200103/2.html. Accessed on: Dec. 17, 2015.

[6] A.V. Iakovenko, V.V. Larin, and R.V. Tarnopolov, "Approaches for protection vydeoynformatsyy based on Elimination of redundancy in ynfokommunykatsyyah", *Modern special equipment*, no. 2 (37), pp. 82-89, 2014.

[7] I.L. Erosh, A.M. Sergeev, and G.P. Filatov, "Protection of images during transfer via communication channels", *Information and Control Systems*, no. 5, pp. 20-22, 2007.

[8] L.A. Mironovskii, and V.A. Slaev, *Strip method of images and signals transformation*. Saint Petersburg, Russia: Politekhnika, SPb, 2006.

[9] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently", in *Proc. of the fourth ACM international conference on Multimedia*, Boston, USA, 1996, pp. 219-229. doi: 10.1145/244130.244209.

[10] H. Cheng, and X. Li, "On the Application of image Decomposition to Image Compression and Encryption", in *Proc. of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, 1996, pp. 116-127. doi: 10.1007/978-0-387-35083-7_11.

[11] T. Kunkelmann, and U. Horn, "Partial Video Encryption based on Scalable Coding", in *Proc. 5th International Workshop on Systems, Signals and Image Processing*, Zagreb, Croatia, 1998, pp. 215 – 218.

[12] V.V. Mokhor, S.M. Bilan, and A.A. Demash, "The method of securing visual information", *UA Patent Appl.* 99465, June. 10, 2015.
[13] A.P. Antonov, *AlteraHDL - Language of description digital devices. Practical course*. Moskow, Russia: IP Radio-Soft, 2001.
[14] V.B. Steshenko, *ALTERA's FPLD: developing of signal processing devices.*Moskow, Russia: Dodeka XXI, 2000.
[15] S.M. Bilan, *Information security in telecommunication systems*, Kyiv, Ukraine: DETUT, 2015.

The article was received 22.02.2016.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] "Способы шифрования видеоинформации передаваемой через интернет". [Электронный ресурс]. Доступно: http://eurocomplect.com/sposobyi-shifrovaniya-videoinformatsii-peredavaemoy-cherez-internet.php. Дата обращения: Дек. 17, 2015.
[2] L. Finkelstein, J. Kosmach, and J. Smolinske. "Method and apparatus for providing cryptographic protection of a data stream in a communication system", *EP* 0671092 A1, Sept. 13, 1995.
[3] С.В. Валов, А.Я. Ольховский, О.А. Павлов, Ю.Ф. Пахомов, и В.Г. Стародубцев, "Устройство кодирования и декодирования речевых сигналов", *Патент Российской Федерации* № 2050698, Дек. 20, 1995.
[4] Ю.Б. Рицар, М.П. Козловський, М.В. Шовгенюк, С.В. Волошиновський, та З.Д. Грицьків, "Спосіб засекречування візуальної інформації", *Патент України* № 22285, Черв. 15, 2001.
[5] А. Володин, В. Митько, и Е. Спинко, "Шифрование видеосигнала – практикум разработчика". [Электронный ресурс]. Доступно: http://www.chipinfo.ru/literature/chipnews/200103/2.html. Дата обращения: Дек. 17, 2015.
[6] А.В. Яковенко, В.В. Ларин, и Р.В. Тарнополов, "Подходы для защиты видеоинформации на основе устранения избыточности в инфокоммуникациях", *Сучасна спеціальна техніка*, № 2 (37), с. 82-89, 2014.
[7] И.Л. Ерош, А.М. Сергеев, и Г.П. Филатов, "О защите цифровых изображений при передаче по каналам связи", *Информационные управляющие системы*, № 5, с. 20-22, 2007.
[8] Л.А. Мироновский, и В.А. Слаев, *Стрип-метод преобразования изображений и сигналов*. Санкт-Петербург, Россия: Политехника, СПб., 2006.
[9] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently", in *Proc. of the fourth ACM international conference on Multimedia*, Boston, USA, 1996, pp. 219-229. doi: 10.1145/244130.244209.
[10] H. Cheng, and X. Li, "On the Application of image Decomposition to Image Compression and Encryption", in *Proc. of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, 1996, pp. 116-127. doi: 10.1007/978-0-387-35083-7_11.
[11] T. Kunkelmann, and U. Horn, "Partial Video Encryption based on Scalable Coding", in *Proc. 5th International Workshop on Systems, Signals and Image Processing*, Zagreb, Croatia, 1998, pp. 215 – 218.
[12] В.В. Мохор, С.М. Білан, А.А. Демаш, "Спосіб засекречування візуальної інформації", *Патент України* № 99465, Черв. 10, 2015.
[13] А.П. Антонов, *Язык описания цифровых устройств AlteraHDL. Практический курс*. Москва, Россия: ИП Радио-Софт, 2001.
[14] В.Б. Стешенко, *ПЛИС фирмы ALTERA: проектирование устройств обработки сигналов*. Москва, Россия: Додэка XXI, 2000.
[15] С.М. Білан, *Захист інформації в телекомунікаційних системах*, Київ, України: DETUT, 2015.

СТЕПАН БЕЛАН,
АНДРЕЙ ДЕМАШ

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ СРЕДСТВА ШИФРОВАНИЯ ВИЗУАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

В статье описан метод шифрования визуальной информации, основанный на использовании клеточных автоматов, по которому визуальная информация шифруется путем наложения дополнительных преобразований кроме обычного шифрования. Первое дополнительное преобразование осуществляется путем выбранного метода кодирования и оцифровки изображения. Второе преобразование заключается в выборе последовательности разрядных слоев и принципов их поблокового сканирования. Данные преобразования в виде числовых значений используются как дополнительные поля к ключу. Кроме того, ключ задается не как готовая битовая последовательность, а как коды операций. К ключевой последовательности принадлежат варианты траектории распространения сигнала возбуждения и двухмерная карта состояний клеточного автомата. Псевдослучайность формирования ключевой гаммы повышает надежность защиты и устойчивость к взлому. Метод позволяет формировать ключевую гамму в неявном виде, что снижает вероятность ее подбора оппонентом. Средства шифрования реализуются на дешевых программируемых интегральных схемах с высокими показателями по быстродействию, что позволяет зашифровывать визуальную информацию в реальном времени в процессе передачи ее по каналам связи.

Ключевые слова: шифрование, видеоинформация, клеточный автомат, программируемая логическая интегральная схема.

СТЕПАН БІЛАН,
АНДРІЙ ДЕМАШ

ВИСОКОПРОДУКТИВНІ ЗАСОБИ ШИФРУВАННЯ ВІЗУАЛЬНОЇ ІНФОРМАЦІЇ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

У статті описаний метод шифрування візуальної інформації, заснований на використанні клітинних автоматів, за яким візуальна інформація шифрується шляхом накладення додаткових перетворень крім звичайного шифрування. Перше додаткове перетворення здійснюється шляхом обраного методу кодування і оцифровки зображення. Друге перетворення полягає у виборі послідовності розрядних шарів і принципів їх поблокового сканування. Дані перетворення у вигляді числових значень використовуються як додаткові поля до ключа. Крім того, ключ задається не як готова бітова послідовність, а як коди операцій. До ключової послідовності належать варіанти траєкторії поширення сигналу збудження і двомірна карта станів клітинного автомата. Псевдовипадковість формування ключової гами підвищує надійність захисту та стійкість до злому. Метод дозволяє формувати ключову гаму в неявному вигляді, що знижує ймовірність її підбору опонентом. Засоби шифрування реалізуються на дешевих інтегральних схемах, що програмуються, з високими показниками по швидкодії, що дозволяє зашифровувати візуальну інформацію в реальному часі в процесі передачі її по каналах зв'язку.

Ключові слова: шифрування, відеоінформація, клітинний автомат, логічна інтегральна схема, що програмується.

Stepan Bilan, candidate of technical sciences, associate professor, associate professor of cybersecurity and application of information systems and technologies department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

E-mail: bstepan@ukr.net.

Andrii Demash, deputy head of research division, State research institute for special telecommunication and information protection, Kyiv, Ukraine.

E-mail: irlandec_lup@ukr.net.

Степан Николаевич Белан, кандидат технических наук, доцент, доцент кафедри кибербезопасности и использования автоматизированных информационных систем и технологий, Государственное учреждение “Институт специальной связи и защиты информации НТУУ “Киевский политехнический институт”, Киев, Украина.

Андрей Андреевич Демаш, заместитель начальника научно-исследовательского отдела, Государственный научно-исследовательский институт специальной связи и защиты информации, Киев, Украина.

Степан Миколайович Білан, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад “Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут”, Київ, Україна.

Андрій Андрійович Демаш, заступник начальника науково-дослідного відділу, Державний науково-дослідний інститут спеціального зв’язку та захисту інформації, Київ, Україна.

УДК 004.62

ІГОР СУБАЧ,
ОЛЕКСАНДР ЧАУЗОВ,
НІНА КУЧУК

МОДЕЛІ РОЗПОДІЛУ ІНФОРМАЦІЙНОГО РЕСУРСУ В АСУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У даній статті розглядаються принципи побудови математичних моделей, що дозволяють оптимально розподілити інформаційний ресурс системи у відповідності за обраним критерієм. Проведено аналіз особливостей планування розподілу інформаційного ресурсу в АСУ спеціального призначення. На основі проведеного аналізу сформульовано задачу розробки моделі, що базується на відповідній структурі системи планування, котра враховує обмеження, специфічні для АСУ, що розглядаються. Розроблено два варіанти математичної моделі розподілу інформаційних блоків по розподілених вузлах базової інформаційно-телекомунікаційній мережі АСУ спеціального призначення. Особливості АСУ, що розглядаються, враховуються у розроблених моделях за допомогою введеної функції корисності. При моделюванні процесів, що відбуваються у відповідних інформаційних підсистемах, використовується багаторівнева система обробки та зберігання даних. Для цього при проектуванні системи або її модернізації створюється модель ієрархічного виділення інформаційного ресурсу, що може розглядатися досить автономно та незалежно від взаємодії із зовнішніми абонентами. Кожний наступний рівень моделі ієрархічного виділення інформаційного ресурсу характеризується збільшенням часу доступу до інформації та зниженням вартості зберігання одиниці даних.

Ключові слова: інформаційний ресурс, математична модель, інформаційно-телекомунікаційна мережа, автоматизована система управління, розподілені дані.

Особливості планування розподілу інформаційного ресурсу. Система планування розміщення інформаційного ресурсу у розподіленому середовищі інформаційно-телекомунікаційної мережі (ІТМ) АСУ спеціального призначення (СП) повинна забезпечувати оптимальне значення обраної цільової функції шляхом складання плану розподілу ресурсів