Cryptographic Information Protection Algorithm Selection Optimization for Electronic Governance IT Project Management by the Analytic Hierarchy Process Based on Nonlinear Conclusion Criteria

Liliya Chyrun[1][0000-0003-4040-7588], Petro Kravets[2][0000-0001-8569-423X],

Oleg Garasym[3][0000-0001-6787-6937]3, Aleksandr Gozhyj[0000-0002-3517-580X]4,

Irina Kalinina[0000-0001-8359-2045]5

[1-2]Lviv Polytechnic National University, Lviv, Ukraine
[3]Volvo IT, Wrocław, Poland
[4-5]Petro Mohyla Black Sea National University, Nikolaev, Ukraine

lchirun21@gmail.com[1], petro.o.kravets@lpnu.ua[2],garasym-oleg@rambler.ru[3], alex.gozhyj@gmail.com[4], irina.kalinina1612@gmail.com[5]

Abstract. The problem of optimizing the choice of cryptographic information security algorithm for e-government IT project management in Ukraine by using nonlinear convolution of criteria based on the method of hierarchies taking into account requirements: security, speed, characteristics of the algorithm is solved in the paper. As a result, the optimal cryptographic algorithm is determined, which ensures the integrity and availability of information during the IT project management of e-government, authentication of users and the inability to deny the fact of sending / receiving information.

Keywords - threat, network, risk, consolidation, e-governance, crypto algorithm, choice optimization

1 Introduction

Electronic Governance means a way of organizing state power through systems of local information networks and segments of the global information network, which ensures the functioning of the authorities in real time and makes daily communication with citizens, legal entities as simple and accessible as possible, non-governmental organizations. In practice, this means the organization of government management and interaction with individuals, legal entities and public organizations through the maximum use of modern information technologies in public administration bodies. That is, e-government provides the following: any person through information and

2020 ITPM Workshop.

communication [1-2] means can apply to state authorities, local self-government bodies for the necessary information, and most importantly - to obtain administrative services. Information security experts point out that the realities of cyber crime are unknown to anyone and that losses are measured in millions of US dollars and continue to increase every year. According to official statistics [2], only 5% of "computer" crimes are known to law enforcement agencies, and about 20% of them are prosecuted. Recently, there has also been a rapid increase in crimes related to the interference with automated systems in Ukraine. As a rule, the intervention is carried out for the purpose of committing other, more serious crimes: theft of property, its extortion under the threat of destruction or distortion of information processed or stored in automated systems, acquaintance with such information, its theft, destruction and more. This, in turn, requires enhancing the security of e-government infrastructure, which can usually be achieved through the use of cryptographic information security techniques. The state policy of Ukraine in the field of information protection [3-5], which is determined by the priority of national interests, is aimed at preventing the realization of threats to information and is carried out by implementing the provisions specified in the legislation and the provisions of the concept of technical protection of information, as well as programs for the development of information security. and individual projects [3-4]. The relevance of the topic is due to the rapid development of e-government in Ukraine and the need for adequate protection of the information that functions in it [6-9]. To date, many cryptographic information security algorithms are known, but the task is to optimize their selection with a view to minimizing the cost of deployment, operation, and maximizing productivity, speed, and resistance to attack [10-17]. The paper deals with the optimization of the choice of cryptographic information security algorithm for e-governance by means of nonlinear convolution of criteria based on the method of hierarchy analysis with requirements: security, speed, algorithm characterization. The algorithm should ensure the integrity and accessibility of information during the functioning of e-government, authentication of users and the inability to deny the fact of sending / receiving information. To achieve this goal, the following tasks were set:

- Define requirements for cryptographic information security algorithms for e-governance;
- Find out the capabilities of crypto algorithms;
- Analyze the suitability of the capabilities to the requirements of e-government;
- Determine the method of the process of optimizing the process of choosing a crypto algorithm and its advantages / disadvantages;
- Justify the choice of method of decision support;
- Set benchmarks;
- Optimize the choice of cryptographic information security algorithm for e-governance.

2 Cryptographic Methods of Information Security

One of the areas of protection in information systems is cryptographic protection of information, which involves the use of mathematical methods of information transformation by means of encryption, imitation insertion or digital signature, etc. Cryptographic protection can be provided during the transmission of information through communication channels and when processed on workstations and servers [18-20].

When transmitting information through communication channels, the following requirements are imposed:

- Ensuring confidentiality of information;
- Ensuring the integrity of information;
- The authenticity of the parties to the information exchange.

Information confidentiality is ensured by symmetric (GOST 28147-89, DES, 3DES, AES, IDEA) and asymmetric (RSA, El Gamal) encryption. The integrity of the information and the authenticity of the parties is achieved through the use of hash functions and digital signature technologies. The set of technologies that ensure the confidentiality and integrity of information when it is transmitted through unsecured communication channels has been called Virtual Private Network (VPN). In the process of network interaction, information security is in particular ensured through SSL, SSH, S-HTTP, IPSec, and the like. The authenticity of the information sharing parties is achieved through the use of X.509, RADIUS, TACACS + and others. These technologies can be implemented by software and hardware. Information protection on workstations and servers can be implemented through file system-level encryption, cryptographic authentication methods (digital certificates, one-time passwords, etc.), cryptographic integrity checks (checksums).

The problem of protecting information by converting it, which precludes its being read by outsiders, only a few decades ago concerned mainly military operations or related to espionage stories but was not widely used. The cause of the rapid development of cryptography, on the one hand, is the use of computer networks, such as the Internet, which transmit large amounts of information of state, military, commercial and private content, which prevents access to it by third parties, and on the other, - the emergence of new powerful computing tools has made it possible to discredit a number of cryptographic systems. Without cryptography, there would be no cell phones, ATMs, digital TV, Internet payments, etc.

Cryptographic information security methods involve both software and hardware use. Software implementation of encryption is cheaper and more practical. At the same time, hardware implementation is more productive and easier to use. Modern cryptographic systems must meet the following common requirements:

- The source text of encrypted text can only be played with the decryption key;
- Sequentially sorting through the possible decryption keys in order to reproduce the source text requires a considerable amount of computation time or a high cost to implement these computations;

- Encryption algorithm information should not affect the encryption resistance of the encryption system;
- Slight modification of the encryption key should result in significant changes to the ciphertext of the same text.

1. Encryption with key. The key encryption algorithm is divided into two large groups - symmetric encryption algorithms and asymmetric encryption algorithms.

Symmetric encryption / decryption methods are a method in which the encryption and decryption keys are either identical or easily computed with each other, thus providing a shared key that is secret.

Asymmetric Encryption / Decryption Methods - a set of cryptographic encryption / decryption methods that use two keys - secret (private) and public; none of the keys can be calculated from another within a specified time. Such encryption / decryption is also called public key encryption / decryption.

Until the 1970s, only cryptography with symmetric crypto algorithms was used. Cryptography with asymmetric crypto algorithms is much younger.

Symmetric and asymmetric crypto algorithms have their advantages and disadvantages. Symmetric crypto algorithms have higher speed and shorter key length than asymmetric ones. Asymmetric encryption is used in such an organization of cryptosystems when the use of symmetric algorithms is impossible. And in general, to compare the characteristics of these crypto algorithms would be incorrect: they are designed to solve different encryption tasks.

2. Symmetric encryption method. Symmetric encryption is also called encryption with a secret key, that is, a key that both parties to the exchange of information (secretly from other users) use to encrypt and decrypt messages. In Fig. 1 is a block diagram of a secret key encryption. The main purpose of symmetric crypto algorithms is to encrypt large data sets at high speed. However, due to the need for a secure secret key transmission channel, these crypto algorithms show very low flexibility when creating modern cryptosystems. There are two major groups of symmetric encryption algorithms: streaming encryption and block encryption.

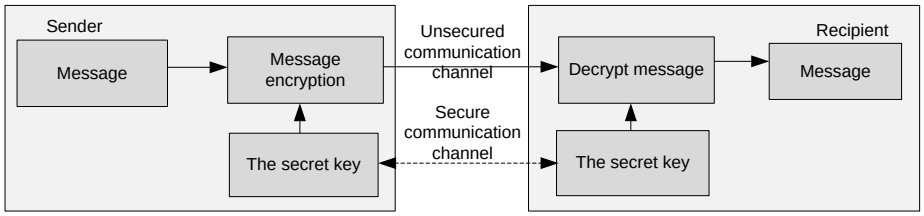

Fig. 1. Structural scheme of encryption with a secret key

3. Asymmetric encryption method. The problem of increasing the amount of encrypted information in cryptography is solved by increasing the speed of traditional secret key encryption methods. However, the application of these methods in the context of a constant increase in the number of participants in a joint work (decentralized management structure) and complications in the organization of interaction between them,

in particular pairwise exchange of information, is ineffective. This is due to the fact that as the number of participants in the exchange of information increases, the number of secret keys increases. We can show that for *N* the number of secret keys in such a system reaches *N*(*N*-1)/2. In addition, symmetric secret-key cryptography techniques have difficulty in trusting the secret key. In order to reduce these shortcomings, public key asymmetric encryption methods have been developed. Public key encryption is a relatively new field of cryptography. Asymmetric crypto algorithms use different keys for encryption and decryption: for encryption - open, for decryption - secret. Asymmetric cryptography is based on the ideas of W. Diffie and M. Hellman about two-key encryption, which became known in 1976. But the first algorithm of asymmetric encryption, which became practical, was the algorithm proposed by R. Rivest, A. Shamir, and L. Adleman in 1978. It was called the RSA algorithm. In Fig. 2 a block diagram of a public key encryption is shown.

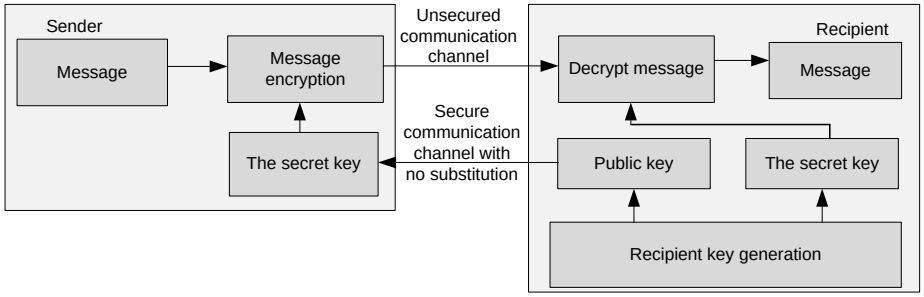

Fig. 2. Outline encryption scheme with public key

Mathematical justification for asymmetric crypto-algorithms consists of heavy-duty (one-way) functions. The theory of complexity calculates the concept that characterizes the level of complexity of calculations (number of operations), depending on the size of the input data. Common are the polynomial and exponential nature of the dependence of the complexity of the calculations on the amount of input data. In asymmetric cryptography, V. Diffie and M. Hellman encrypt the message in the presence of a secret key for the polynomial operating time of the computer system, and in the absence of it, for exponential time. Modern asymmetric cryptography is based on the algorithms of El-Gamal and Miller-Koblitz. The theoretical basis for the stability of the RSA algorithm is the problem of factorization of large integers, and the algorithms of El-Gamal and Miller-Koblitz - the problem of discrete logarithm. Numerous vulnerabilities of these algorithms are known today. Public key encryption algorithms have been replaced by more robust encryption algorithms on elliptic curves, proposed separately by V. Miller and N. Koblitz in 1986 [6].

3 The Main Problems

Asymmetric encryption algorithms, as well as symmetric encryption, are used to encrypt data arrays, but their speed is much lower. The main purpose of asymmetric algorithms is to ensure the efficient functioning of modern cryptosystems. It is these algorithms that underpin the tasks of user authentication, control of the integrity and accessibility of information, the impossibility of rejection of authorship or the fact of obtaining data, etc., in particular, in the organization of e-government. The following asymmetric encryption algorithms satisfy the most of these requirements: Mars, RC6, Rijndael, Serpent, Twofish (Table 1).

Table 1. Selected for comparing asymmetric encryption algorithms

Algorithm	Developer	Country	Speed (asm, 200 MHz)
MARS	IBM	US	8 MB/s
RC6	R.Rivest & Co	US	12 MB/s
Rijndael	V.Rijmen & J.Daemen	BE	7 MB/s
Serpent	Universities	IS, UK, NO	2 MB/s
TwoFish	B.Schneier & Co	US	11 MB/s

Asymmetric crypto algorithms have become important in the application of electronic-digital signature systems. Electron-digital signature is a digital sequence that is attached to a message to ensure the integrity of information and authentication, and is formed using asymmetric cryptosystems. The electronic-digital signature uses a secret key to form signed messages, and a public key to verify the signature. In the process of organizing e-government, there is a problem of optimal choice of the cryptographic information security algorithm. Each of a large number of cryptographic algorithms has its advantages and disadvantages. Therefore, the amount of analysis of information regarding the evaluation and selection of the cryptographic algorithm that best meets the requirements of information security in e-governance is quite large. The selection process involves quantitative and qualitative analysis in the process of comparing different alternatives. With the increasing number of comparison criteria and the number of alternatives that can significantly affect the end result, one can make a choice among such many options (Table 2 [7]). That is why there is a need to use decision support systems, which allows to optimize the choice of cryptographic information security algorithm based on expert evaluations, as well as allow not only to make qualitative, quantitative analysis, taking into account the most important requirements for algorithms, but also to scientifically substantiate the choice [8].

Table 2. Characteristics of basic asymmetric information security algorithms

Encryption algorithm	Characteristic
MARS	performs the sequence of transformations in the following order: adding modulo 2 with the key as pre-whitening, 8 rounds of direct conversion without the key, 8 rounds of direct conversion with the key, 8 rounds of reverse conversion

Encryption algorithm	Characteristic
	with the key, 8 rounds of non-key conversion and key deduction as post-whitening. 16 rounds using a key called the cryptographic core. Keyless rounds utilize two 8x16-bit S-boxes, and addition operations and XOR. In addition to these elements, key-rounds use a 32-bit key multiplication, which depends on data cyclic shifts and key addition. Both conversion rounds and kernel rounds are rounds of a modified Feishtel network in which a quarter of the data block is used to change the remaining three-fourths of the data block. MARS is offered by IBM.
RC6	is a family of parameterized encryption algorithms based on the Feishtel network; 20 rounds have been proposed for AES. The round function in RC6 triggers variable cyclic shifts that are determined by the quadratic function from the data. Each round also includes Module 32 multiplication, addition, XOR and key addition. Key assembly is also used for pre- and pos-whitening. RC6 was proposed by the RSA Laboratory.
Rijndael	is an algorithm that uses linear substitution transformations and consists of 10, 12, or 14 rounds, depending on the length of the key. The data block processed using Rijndael is divided into byte arrays, and each encryption operation is byte-oriented. The Rijndael round function consists of four layers. The first layer uses an 8x8 bit S-box for each byte. The second and third layers are linear transformations in which the rows are treated as offset arrays and the columns are mixed. In the fourth layer, XOR bytes of the subkey and each byte of the array are performed. Column mixing was omitted in the last round. Rijndael is offered by Joan Daemen (Proton World International) and Vincent Rijmen (Katholieke Universiteit Leuven).
Serpent	is an algorithm that uses linear substitution transformations and consists of 32 rounds. Serpent also identifies non-cryptographic initial and final permutations that facilitate an alternative implementation mode, the so-called bitslice. The round function consists of three layers: XOR key operation, 32 parallel applications one of eight fixed S-boxes and linear conversion. In the last round, the XOR layer with the key is replaced by a linear transformation. Serpent proposed by Ross Anderson (University of Cambridge), Eli Biham (Technion) and LarsKnudsen (University of California San Diego).
Twofish	is a Feishtel network with 16 rounds. The Feishtel network was modified using one-sided rotations. The round function affects 32-bit words using four key-dependent S-boxes, followed by fixed maximal single matrices in GF (28), pseudo-adamar transformations and key addition. Twofish was proposed by Bruce Schneier, John Kelsey and Niels Ferguson (Counterpane Internet Security, Inc.), Doug Whiting (Hi / fn, Inc.), David Wagner (University of California Berkley) and Chris Hall (Princeton University).

4 Methodology and Comparison Criteria

For e-government, the following benchmarks are crucial: reliable algorithm execution in both hardware and software; rapid generation and matching of keys, their use; minimal memory usage resistance to attacks; flexibility; high bandwidth. So let's define the main criteria for comparing cryptographic information security algorithms for e-government: security; speed; general algorithm parameters. The criterion "security" is the most important factor in evaluating and comparing such capabilities as the stabil-

ity of the algorithm to cryptanalysis, the study of its mathematical basis, the randomness of the original values of the algorithm and the relative security compared to other algorithms. The "speed" criterion is another important evaluation criterion that characterizes computational performance across platforms, memory requirements, time spent on encryption and decryption, and attack speed. The third priority in order to evaluate algorithms for e-government is the characteristic of the algorithm, which means: flexibility, hardware, software suitability and simplicity of the algorithm. Flexibility includes the ability of the algorithm to:

- Key management, minimizing size;
- Implementation of safe and efficient functioning in different types of software environment;
- Implementation of hashing algorithm, possibility of providing additional cryptographic services.

The fulfillment of these requirements is necessary in order that in electronic governance the hardware and software support the implementation of the selected crypto algorithm. Table 3 shows the comparative characteristics of the five crypto algorithms according to the identified comparison criteria [9].

Table 3. Comparative characteristics of five cryptoalgorithms

№	Category	Serpent	Twofish	MARS	RC6	Rijndael
1.	Cryptocurrency	+	+	+	+	+
2.	Cryptocurrency margin	+ +	+ +	+ +	+	+
3.	Encryption speed in software implementation	-	+ -	+ -	+	+
4.	Protection against runtime attacks and power usage	+	+ -	-	-	+
5.	Protection against attacks with the necessary power to the key expansion procedure	+ -	+ -	+ -	+ -	-
6.	Protection against attacks by using the power to be implemented in smart cards	+ -	+	-	+ -	+
7.	Possibility of parallel calculations	+ -	+ -	+ -	+ -	+
8.	Ability to extend the key “on the fly”	+	+	+ -	+ -	+ -

The cryptocurrency of the algorithms is sufficient - no real-time attacks were detected in the full version of the algorithms. In this case, cryptanalysts usually explore variants of algorithms with truncated number of rounds, or with some modifications made, minor but which weaken the characteristics of the algorithm. Cryptocurrency reserves mean the ratio of the total (provided in the specifications of the algorithms) of the number of rounds and the maximum of the variants against which any cryptanalytic attacks are affected. For example, differential linear linear cryptanalysis reveals an 11-round Serpent, while the original algorithm performs 32 rounds. The

cryptocurrency margin is slightly lower in Rijndael and RC6 than in the rest of the algorithms. The algorithms show that they all support on-the-fly key extensions (subkeys can be generated directly during the encryption process as needed), however, only Serpent and Twofish support this capability without any restrictions.

Implementation options (flexibility) imply the ability to perform any optimization algorithm operation for specific purposes in different ways. Most illustrative in this sense are the previously mentioned options for the procedure of the extension of the key of the Twofish algorithm, which allow to optimize the implementation of the algorithm depending, first of all, on the frequency of key change.

5 Analysis of Scientific Results

One approach to assigning "weights" to the final set *n* compared objects on the basis of the matrix of paired comparisons was proposed by T. Saati [10]. In the future, this approach was shaped into a whole section of decision making in the presence of one and several criteria [11] - [14] and was called the method of analysis of hierarchies. At present, the method of analyzing hierarchies has seriously entered the theory and practice of multicriteria selection. The number of articles of applied nature in which the method of analyzing hierarchies is used to solve a variety of applied multicriteria problems, has exceeded one thousand ten years ago. AII-compiled EXPERT CHOICE, MPRIORITY and IS «Vybor». In accordance with the method of analysis of hierarchies, experts form the so-called matrix of pairwise comparisons *A*, and the desired measure vector $w = (w_1, w_2, ..., w_n)^T$ is calculated as the eigenvector of this matrix corresponding to the maximum eigenvalue. This method of determining the vector of measure by virtue of the violation in practice of the compatibility properties [15-18] of the pairwise comparison matrix is not substantiated.

Let's make it clear. It is well known that the vector of measure *w* is a native vector of compatibility (in some sources, the name is fully compatible) of the matrix *A*, corresponding to its own maximum value *n*. Thus, in the case of a compatible matrix, the measure vector is a specified eigenvector. But when hierarchies are formed in accordance with the method of hierarchy analysis, it is not necessary to count on the compatibility of the matrix of pairwise comparisons. This is known to all who are familiar with the method of hierarchy analysis. This means that in practice, you have to deal with another situation (model) that is matched by an incompatible matrix. Nevertheless, according to the method of analysis of hierarchies, the measure vector is again proposed to be found as an eigenvector of an (incompatible) matrix of pairwise comparisons, and this eigenvector corresponds to an eigenvalue that is no longer equal (but strictly larger) *n*. In the general literature on the method of hierarchy analysis, there is (at least at the moment) no proof that the required measure vector must be an eigenvector of an incompatible matrix corresponding to its maximum eigenvalue greater than *n*. For this reason, this method can not be called justified, it is a certain heuristic approach, the logic of which is to recommend to act in such a way in situations that may be very different from those for which the validity of these actions is established. This means that the application of the hierarchy analysis method almost

always contains some "model" error of calculating the vector of measure (not taking into account errors of purely computational nature) and, if this error is large, then the application of the method of hierarchy analysis becomes simply unjustified. Therefore, a special numerical indicator of consistency index is introduced, which characterizes the degree of confidence in the hierarchy results obtained by the method of analysis. This index is interpreted as a kind of deviation of the original incompatible matrix from some compatible one. As T. Saati points out [15], with a sufficiently small value of the compatibility index, the pair of comparisons is "close" to some matrix with zero of this index (i.e. to some compatible matrix). Thus, the result of applying the method of hierarchy analysis in the form of a vector of measure is to some extent "close" to the result obtained on the basis of this compatible matrix. If the compatibility index exceeds the "threshold" value, then it is impossible to conclude that these matrices are close, so it is not recommended to use the method of hierarchy analysis in such cases. However, it should be noted that the value of the compatibility index can only indirectly judge the magnitude of the effective "model" error; it is precisely never and no one can be identified. This is the specificity of this heuristic approach. The method of analyzing hierarchies has repeatedly been criticized by various authors, mainly for failing to keep the ranking solution while removing one of the possible solutions [18]. In this case, it is suggested to review the other two important components of the method. First, the process of forming a matrix of paired comparisons is proposed to substantially simplify, requiring the expert to know not about all elements of this matrix located above (or below) the main diagonal, but only about certain "basic" elements, on the basis of which it is then easy and without of computational errors is the desired vector of measure. In this case, the choice of a specific "base" set corresponds to one or another object comparison scheme, which can be selected in order to obtain the most reliable results from an expert. In general, the proposed option is much simpler than the initial method as at the stage of matrix formation *A*, and in the process of calculating the vector of measure. In addition, it is completely free of the "model" error discussed above because it is based on a compatible matrix *A*. Secondly, according to the Edworth-Pareto principle, when solving multicriteria problems, the application of linear convolution of criteria is possible only under certain sufficiently limited assumptions. In this regard, we propose to use a convolution instead of a linear convolution as a function of the minimum contained in Yu. B. Hermeyer's theorem [19, 20], whose application is justified for the broadest class of multiobjective choice problems with a finite set of possible solutions. The result of the revision, the method of solving multicriteria problems is called the simplified version of the method of analysis of hierarchies based on nonlinear convolution of criteria. The decision-making task has two main varieties:

- Choice task (select or reject several options from the group of possible ones);
- The task of allocating resources (each of these options is taken into account according to its priority).

Let’s note that in the real decision-making process there are related problems that are successfully solved using the method of hierarchy analysis. The method of analyzing

hierarchies is a methodological basis for solving the problems of choosing alternatives by means of their multicriteria ranking. The main application of the method is to support decision making with the help of hierarchical composition of the task and the ranking of alternative solutions. Given this fact, it is necessary to recalculate the possibilities of the method.

1. The method allows to analyze the problem. The problem of decision making is presented in the form of hierarchically ordered:

- The main purpose (main criterion) of ranking possible solutions;
- Several groups (levels) of the same type of factors that affect the rating in one way or another;
- Groups of possible solutions;
- Communication systems that indicate the interplay of factors and decisions.

All of these "nodes" are assumed to indicate their mutual effects on each other (links to each other).

2. The method allows to collect data on the problem. In accordance with the results of hierarchical decomposition, the model of the decision-making situation has a cluster structure. The set of possible solutions and all the factors that influence the priorities of the solutions are broken down into relatively small groups - clusters. The hierarchy procedure of paired comparisons, developed in the method of hierarchy analysis, allows to determine the priorities of the objects belonging to each cluster. This is done using the eigenvector method. Therefore, the complex problem of data collection is broken down into a number of simpler ones, which are solved for clusters.

3. The method makes it possible to evaluate and minimize data conflicts. To this end, harmonization procedures have been developed in the method of hierarchy analysis. In particular, it is possible to identify the most conflicting data, which allows to identify the least clear areas of the problem and to organize more careful selective reflection of the problem.

4. The method allows to synthesize the problem of decision making. After analyzing the problem and collecting data for all clusters, a final rating is calculated, using a special algorithm, which is a set of priorities for alternative solutions. The properties of this rating allow you to support decision making. For example, the highest priority decision is made. In addition, the method allows you to build ratings for groups of factors, which allows you to evaluate the importance of each factor.

5. The method allows to organize the discussion of the problem, promotes consensus. Thoughts that arise when discussing the problem of decision making can themselves be considered as possible solutions in this situation. Therefore, the hierarchy analysis method can be applied to determine the importance of accounting for each participant's opinion.

6. The method allows to evaluate the importance of accounting for each decision and the importance of accounting for each factor affecting the priorities of decisions. According to the formulation of the decision-making task, the priority value is directly related to the optimality of the decision. Therefore, low priority decisions are dismissed as non-influential. As noted above, the method allows to evaluate the priorities

of the factors. Therefore, if the priority of decisions is changed when a factor is excluded, such a factor can be considered non-influential for the task.

7. The method allows to evaluate the stability of the decision. A decision that can be made can be considered justified only if the inaccuracy of the data or the structure of the model of the decision-making situation does not significantly affect the ranking of alternative decisions.

If it is sufficient to use only objective data for decision making, then other methods (e.g., target criterion optimization methods) may be predominant in terms of accuracy and speed. The method may be too cumbersome to decide in simple situations, because many pairs of comparisons are needed to collect data. However, if a large-scale problem is considered and the cost of the consequence of a wrong solution is high, adequate tools are needed. The method of analysis of hierarchies allows you to break a complex problem into a series of simple, to identify contradictions. Strategic decision-making often has to rely more on the experience and intuition of professionals than on objective data. In this case, the results obtained by the method of hierarchy analysis may be more realistic than the results obtained by other methods. Ratings of possible solutions are based on "transparent" principles. Therefore, they may be more persuasive than the information to support decision-making obtained through black box models. In such models, the input of the problem will be transformed into the output of the decision-making process according to "opaque" principles and the structure of the decision-making situation is not disclosed. The method of analysis of hierarchies does not require simplification of the structure of the task, which is the a priori rejection of some features. Therefore, it is more effective than other analytical tools to take into account the influence of various factors on the choice of decision.

Composing a decision model can be a cumbersome process. However, if folded, it can then be reused. It is only necessary to correct this structure and fill it with data. In this case, the solution of typical problems can be put in the flow. Thus, the application of the method becomes more efficient. Now, let's look at a specific example of optimizing the choice of cryptographic information security algorithm for e-governance with a simplified method of hierarchy analysis based on nonlinear convolution. [14]

Software tools for the process of selecting the nomenclature of security elements. As mentioned above, we will use the software system to optimize the process of choosing the cryptographic information security algorithm for e-government IS «Vybor». The results of the calculation are presented in Fig. 3-4; Table 4.

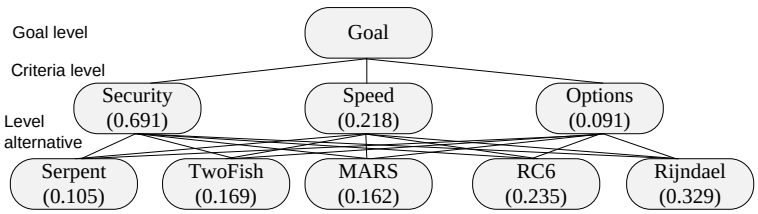

Fig. 3. Hierarchy: cryptographic information security algorithms for e-government

Table 4. Calculation results

Factors (Measure)		**Serpent (0.105)**	**TwoFish (0.169)**	**MARS (0.162)**	**RC6 (0.235)**	**Rijndael (0.329)**
Node	**General safety**					
Measure	0.691					
Matrix of pairwise comparisons	№	1	2	3	4	5
	1	1,000	0,500	0,500	0,500	0,333
	2	2,000	1,000	1,000	1,000	0,500
	3	2,000	1,000	1,000	1,000	0,500
	4	2,000	1,000	1,000	1,000	0,500
	5	3,000	2,000	2,000	2,000	1,000
Characteristic of the matrix	λ_{max} = 5.007 CI = 0.002 RC = 0.002					
Node	**Speed**					
Measure	0.218					
Matrix of pairwise comparisons	№	1	2	3	4	5
	1	1,000	0,500	0,500	0,250	0,333
	2	2,000	1,000	1,000	0,333	0,500
	3	2,000	1,000	1,000	0,333	0,500
	4	4,000	3,000	3,000	1,000	2,000
	5	3,000	2,000	2,000	0,500	1,000
Characteristic of the matrix	λ_{max} = 5.032 CI = 0.008 RC = 0.007					
Node	**General characteristics**					
Measure	0.091					
Matrix of pairwise comparisons	№	1	2	3	4	5
	1	1,000	2,000	4,000	1,000	0,500
	2	0,500	1,000	3,000	0,500	0,333
	3	0,250	0,333	1,000	0,250	0,200
	4	1,000	2,000	4,000	1,000	0,500
	5	2,000	3,000	5,000	2,000	1,000
Characteristic of the matrix	λ_{max} = 5.052 I3 = 0.013 RC = 0.012					

CI – consistency index, RC – relation of consistency; if CI and RC ≤ 0.1, then the measure of consistency is at a satisfactory level.

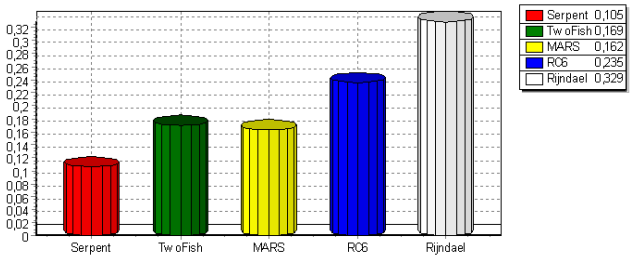

Fig. 4. Diagram of the result

IT project management is the process of planning, organizing and delineating responsibility for the completion of an organizations' specific information technology (IT) goals. One of the scientific concepts is that project management is an orderly sequence of decision making. The features of life cycle and project management technologies impose specific requirements for the application of management decision-making methods in them, which provide instrumental support for decision-making processes in projects. Some popular approaches include the Hierarchy Analysis Method or Analytic Hierarchy (AHP) method proposed by American Professor T. Satie (AHP), and its generalization to the Analytical Hierarchy Method (MAC).

The implementation of projects in specific areas, especially at the level of security organization of the functioning of information systems, requires the priority consideration of their business models for the assessment of situations and decision making. Project activity in the educational and public sphere attracts attention due to the participation of a large number of highly qualified specialists, non-standard value look at the criteria of project implementation efficiency, constant interaction with traditional processes that can resist any and all innovations. The use of decision-making methods in educational and governmental projects is additionally related to the public nature of most of them, which requires the use of clear (including for non-specialist) and constructive (regarding the processing of quality information) decision-making technology. The criteria for maintaining safety in education / government projects by the Saati method are the subject of this study. Government and educational projects have peculiarities in the structure of the phases of the life cycle, which determines the specific nature of the application of management methods in them security-enabled solutions at the IT project management. Different methods of government / educational IT project management can use different methods as an instrumental tool for managerial decision making and one of the most versatile is the Saati method. The accumulated experience of implementing IT projects in areas with high levels of intellectual saturation creates preconditions for comparing life cycles and opportunities for applying management decision-making methods. The life-cycle features of government / educational IT projects are often driven by the high level of their intellectual saturation and the complexity of evaluating intermediate stages of implementation. In this regard, a comparative study of the life-cycle phases of government / educational IT projects and software development IT projects appears promising. Such comparisons can be made in a broad context on the basis of the international standard ISO / IEC 12207: 2008 “System and software engineering. Software Lifecycle Processes” and in a narrow sense based on software development lifecycle models.

6 Conclusions

According to the criteria of evaluation of cryptographic information security algorithms for use in e-governance, it is recommended to choose the algorithm that is the most effective in the integral indicator. The “security” criterion has the highest priority and has the greatest impact on the results, and the “speed” and “algorithm” criteria are secondary to “security”. Guided by the robust security of attack algorithms,

MARS, Serpent and Twofish have a high level of security, but RC6 and Rijndael have higher and more secure protection. RC6 and Rijndael generally show higher encryption and decryption rates than average for 128 bit keys but 32 bit platforms, and RC6 has the highest speed. MARS has an average speed of doing the same. For Twofish, the time spent on encryption and decryption is different, but in both cases the level is above average. Serpent showed the lowest performance compared to other algorithms.

Rijndael requires little RAM and is therefore best handicapped. Serpent also provides the right level of encryption and decryption for low RAM. The RC6 has a small amount of RAM, which is a positive thing in the limited space, but there is a downside to the continuous ability to compute decryption subkeys, creating a high RAM requirement for other algorithms. MARS does not meet the requirements in a restricted environment and requires additional resources. Serpent and Rijndael have the best hardware performance for both feedback and feedback. Serpent has the highest performance in feedback, Rijndael offers the best performance in feedback. The RC6 and Twofish have average performance, and both algorithms can run compactly. MARS has high requirements and overall performance is below average. When performing attacks, Rijndael and Serpent's algorithms performed well, quickly detecting and preventing them. Twofish performs longer and with greater complexity, and RC6 and MARS counteract attacks with the greatest amount of time and difficulty. Twofish, MARS, and RC6 require little extra space to encrypt and decrypt. Although Rijndael is inferior in this aspect, it may share some technicalities. Twofish supports continuous calculation of subkey counts for both encryption and decryption. Serpent also supports continuous calculation of subkey counts for both encryption and decryption; however, the decryption process requires one additional calculation of the calculation. The Rijndael algorithm supports continuous computation of encryption subkeys, but requires the previous one-time execution of the full key list before decryption with a specific key earlier. MARS has special features that are similar to Rijndael, but additionally loads the resource for MARS execution. RC6 supports continuous computation of encryption-only subkeys. Each of the algorithms provides reliable security and has advantages in certain areas compared to others. The method of hierarchy analysis based on nonlinear convolution of criteria has been investigated and mathematically substantiated the choice of Rijndael algorithm as the one that best satisfies the requirements of information security in e-governance.

References

1. Gozhyj, A., Kalinina, I., Vysotska, V., Gozhyj, V.: The method of web-resources management under conditions of uncertainty based on fuzzy logic, 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018 – Proceedings 1, 343-346 (2018).
2. Gozhyj, A., Vysotska, V., Yevseyeva, I., Kalinina, I., Gozhyj, V.: Web Resources Management Method Based on Intelligent Technologies, Advances in Intelligent Systems and Computing, 871, 206-221 (2019).
3. Rusyn, B., Lytvyn, V., Vysotska, V., Emmerich, M., Pohreliuk, L.: The Virtual Library System Design and Development, Advances in Intelligent Systems and Computing, 871, 328-349 (2019).

4. Lytvyn, V., Vysotska, V., Veres, O., Rishnyak, I., Rishnyak, H.: The Risk Management Modelling in Multi Project Environment.. In: Computer Science and Information Technologies, Proc. of the Int. Conf. CSIT, 32-35 (2017).
5. Kanishcheva, O., Vysotska, V., Chyrun, L., Gozhyj, A.: Method of Integration and Content Management of the Information Resources Network. In: Advances in Intelligent Systems and Computing, 689, Springer, 204-216 (2018).
6. Korobchinsky, M., Vysotska, V., Chyrun, L., Chyrun, L.: Peculiarities of Content Forming and Analysis in Internet Newspaper Covering Music News, In: Computer Science and Information Technologies, Proc. of the Int. Conf. CSIT, 52-57 (2017).
7. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C (second Edition. N.Y. : John Wiley & Sons, Inc. (1996).
8. Vysotska, V., Fernandes, V.B., Emmerich, M.: Web content support method in electronic business systems. In: CEUR Workshop Proceedings, Vol-2136, 20-41 (2018).
9. Advanced Encryption Standart (AES), http://www.intuit.ru/department/security/networksec/4/5.html. (2012)
10. Saaty, T. L.: An eingenvalue allocation model for prioritization and planning. In: Energy Management and Policy Center. University of Pennsylvania (1972).
11. Demchuk, A., Lytvyn, V., Vysotska, V., Dilai, M.: Methods and means of web content personalization for commercial information products distribution. In: Lecture Notes in Computational Intelligence and Decision Making, 1020, 332–347. (2020).
12. Lytvyn, V., Vysotska, V., Demchuk, A., Demkiv, I., Ukhanska, O., Hladun, V., Kovalchuk, R., Petruchenko, O., Dzyubyk, L., Sokulska, N.: Design of the architecture of an intelligent system for distributing commercial content in the internet space based on SEO-technologies, neural networks, and Machine Learning. In: Eastern-European Journal of Enterprise Technologies, 2(2-98), 15-34. (2019).
13. Saaty, T. L.: Multicriteria decision making. the analytic hierarchy process: Planning. Priority Setting. Resource Allocation. University of Pittsburgh, RWS Publications (1990).
14. Yu, P. L.: Multiple criteria decision making: Concepts, Techniques, and Extensions. Plenum Press, N.Y. (1985).
15. Naum, O., Chyrun, L., Kanishcheva, O., Vysotska, V.: Intellectual system design for content formation. In: Computer Science and Information Technologies. In: proc. of the Int. Conf. CSIT, 131-138 (2017).
16. Su, J., Sachenko, A., Lytvyn, V., Vysotska, V., Dosyn, D.: Model of touristic information resources integration according to user needs. In: International Scientific and Technical Conference on Computer Sciences and Information Technologies, 113-116 (2018).
17. Vysotska, V., Chyrun, L.: Analysis features of information resources processing. In: Proc. of the Int. Conf. on Computer Science and Information Technologies, 124-128 (2015).
18. Rusyn, B., Vysotska, V., Pohreliuk, L.: Model and architecture for virtual library information system. In: International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018, 1, 37-41 (2018).
19. Lytvyn, V., Peleshchak, I., Vysotska, V., Peleshchak, R.: Satellite spectral information recognition based on the synthesis of modified dynamic neural networks and holographic data processing techniques. In: International Scientific and Technical Conference on Computer Sciences and Information Technologies, 330-334 (2018).
20. Lytvyn, V., Kuchkovskiy, V., Vysotska, V., Markiv, O., Pabyrivskyy, V.: Architecture of system for content integration and formation based on cryptographic consumer needs. In: International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018, 1, 391-395 (2018).