UDC 004.056.55

METHODS AND RESULTS OF ELECTRONIC SIGNATURES WITH APPENDIX AND MESSAGE RECOVERY COMPARATIVE ANALYSIS

I. Gorbenko, M. Yesina, N. Kovaleva

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, rinayes20@gmail.com, natalikovalevaa@gmail.com

Reviewer: Irina Lisitska, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine;
lisitska@karazin.ua

Received on August 2016

Abstract. *The paper deals with the comparative analysis methods of electronic signature mechanisms properties. The existing methods of comparative analysis of electronic signatures based on expert estimations methods – analytic hierarchy process and variations of weight indices methods are investigated and analyzed. Some criteria and indicators, that can be used in the comparative analysis of electronic signature mechanisms properties are presented. The comparative analysis of the existing perspective electronic signatures mechanisms according to the standards DSTU ISO/IEC 14888-3:2014 and DSTU ISO/IEC 9796-3 is carried out. The results of the conducted electronic signature mechanisms evaluation are shown. Conclusions and recommendations on the use of defined electronic signature algorithms evaluation methods are made and provided.*

Keywords*: electronic signature mechanisms analysis, weight indices, electronic signature, electronic signature estimation criterion, electronic signature comparison analysis methods, electronic signature realization and application.*

1 Introduction

The significant number of standardized electronic signatures (ES) mechanisms [1-3,7] are applied in order to provide in different information technology electronic trust services at the international, regional and national levels. In the European Union (EU) it is made a number of normalization projects relatively ES [6,14]. And it would seem, that they solve problems at least to 2030 year. However, according to the recent researches, in terms of requirements and development of post quantum ES standards, appeared new, both theoretical and practical, problems of substantiation construction methods, analysis and comparative analysis of ES. Thus developers and users of electronic trust services applications have the ability to select ES from the significant number of existing international and national standards, primarily DSTU ISO/IEC 14888-1,2,3 [1,2], DSTU ISO/IEC 9796-3 [3], DSTU 4145-2002 [7] and others. Providers and users have the ability to select ES for application in the indicated conditions, moreover depending on the requirements and adopted models of threats and violator [6]. Therefore, in our opinion, now so important and, that require the solving, are theoretical and practical issues of methods substantiation and choice, and creation on their base the analysis techniques and comparative analysis of existing and perspective ES.

The special importance of solve the above mentioned problems is connected with the deployment of the development and implementation ES works, and other cryptographic primitives, that meet the post quantum period requirements [6]. This is stems from the fact, that to the post quantum cryptographic primitives demands are made not only relatively cryptographic stability, but also it is a significant number of feasibility and technical-operational requirements.

First time, according to our analysis, such analysis techniques and comparative analysis ES were proposed in [4,8,15-17] and detailed in [6]. The essence of the suggestions reduced to separation ES evaluating criteria on unconditional and conditional and then their use to calculate the values of integral conditional and unconditional ES evaluating criteria. In this case offered unconditional criteria and integral unconditional criterion on their base are effective and allow to estimate or compare ES. However, methods of calculating integral conditional criterion values based on pairwise comparisons and hierarchies methods, proposed in [4,6,8,15-17], to a large extent depend on the

experts competence and objectivity in their assessments. At the same time, there are other methods, including deserves attention method of weighting coefficients [9,11-13,18-20,22-24] and practical guidelines, that support it.

The objective of this article is the methods theoretical substantiation and practical implementation and development on their base ES evaluation technique and comparative analysis on conditional and unconditional criteria, their practical use to compare existing ES [1-3,6,7], and also the guidelines development for assessment and comparative analysis post quantum period ES.

2 Problem formulation

Analysis of a number of sources [4,6,8,15-17] showed, that an important stage of selection perspective cryptographic primitive is the decision on determine the most perspective ES method or methods, and also other cryptographic primitives, and the final stage is their comparative analysis according to determined partial and integral conditioned and unconditioned criteria. In fact, this problem practically not solved relatively cryptographic primitives, the evidence of this is carrying international projects AES, Neisse and SHA-3 [6]. In our opinion, at acceptance decision regarding recommendation of certain cryptographic primitives as standard, mainly taken into consideration their assessments and special services opinions, and experts subjective assessments. Although experts opinions and influence, in our opinion, were not significant. Therefore the important theoretical and practical problem is the substantiation and choice, according to the requirements, the sets of indicators and assessment criteria, substantiation and choice estimate method or methods and properties comparative analysis, and also the development and practical application of scientifically grounded assessment techniques and comparative analysis cryptographic primitives of certain class. In our case concentrate on existing and perspective standardized ES mechanisms, that are improved or will be developed for use in post quantum period.

The specified problem will consider mainly on algorithms, whose stability is based on complexity of discrete logarithm at finite field and the group of points of elliptic curves (EC): DSTU ISO/IEC 14888-3:2014 [1,2] and DSTU ISO/IEC 9796-3 [3]. In DSTU ISO/IEC 14888-3 is recommended to use 12 different ES mechanism, based on the use mathematical apparatus of finite fields, elliptic curves and EC points pairing.

Thus, the objective of research, which is the subject of the article is review, analysis and comparative analysis of ES with appendix according to DSTU ISO/IEC 14888-3: 2014 and DSTU ISO/IEC 9796-3 on the totality unconditional and conditional criteria [6], and also separately analysis and development of recommendations on the use methods and this type technique for ES analysis and comparison, using as example DSTU ISO/IEC 14888-3: 2014 [1,2] and DSTU ISO/IEC 9796-3 [3] algorithms, as well as possible for ES assessment, that will be developed for use in post quantum period.

3 The achievements state of the methods and assessment techniques and ES comparative analysis development and application

From described above follows the necessity and actuality of solving the problem, a great extent, automation and significantly reduce decision-making subjectivity relatively the benefits of the cryptographic primitives certain set, such as ES. The solution of tasks certain components of this problem is contained in [4,6]. Thus in [6] for ES evaluation and comparative analysis are proposed pairwise comparison methods and hierarchy method [4-6,8,10,15-17,21].

Later in the criterion will understand the sign on which basis is carried out the assessment, anything determination or classification [6], that is, in fact, will understand the measure of evaluation. Previous researches and [6] allow to substantiate the conclusion, that the evaluation and standardized ES algorithms comparison should implement using two sets of criteria: unconditional and conditional [6]. Given the [6], ES type cryptographic transformations evaluating can be carried out in 2 stages.

In the first stage it is checked the conformity standardized algorithms to requirements of unconditional criteria – partial and integral, and in the second, using conditional criteria – partial conditional criteria and integral conditional criterion. Just by using partial conditional criteria and integral conditional criterion, and it is possible to compare different ES type cryptographic transformation.

3.1 Expert assessment methods

In expert estimates understand search method and the result of applying the method, obtained based on the use personal expert opinion or collective opinion of the expert group [12,13,22-24], and also a set of logical and mathematical procedures, aimed at obtaining information from experts, its analysis and generalization for the preparation and making rational decisions [12,13,22].

Expert assessments methods – methods of organization work with specialists-experts and processing of experts opinions [12,13,22-24]. Essence of the method expert assessments – in basis of the making decision, forecast, conclusion is laid the specialist or team of specialists opinion, based on their knowledge and practical professional experience.

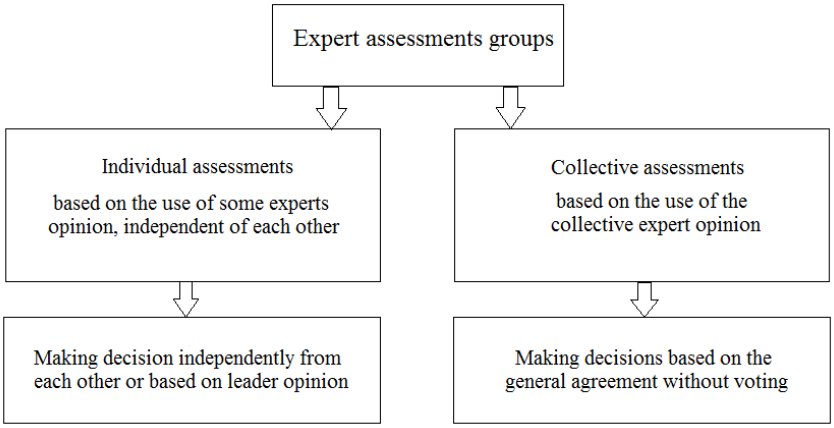

Fig. 1 – Scheme of expert assessments groups

Expert assessment stages [12,13,22-24]:

1. Research objective statement
2. The choice of research form, determining the project budget
3. Preparation of information materials, questionnaire blanks, procedure moderator
4. Selection of experts
5. Expert examination
6. Analysis of results (expert assessments processing)
7. Prepare a report with the results of expert assessment

There are known the following expert assessments methods (ways to develop both collective and individual expert assessments) [12,13,22-24]: associations method; pair (binary) comparison method; vectors advantages method; focal objects method; individual expert survey; midpoint method; simple ranking method; setting weight coefficients method; successive comparisons method; attribution points method. Methods for receiving individual opinion [12,13,22-24]: method "Delphi", interview method, report method.

Methods of expert group teamwork [12,13,22-24]: brainstorming (brainstorm), method "635", business game, commission assessment (method of "meeting", "round table"), method of "court".

3.2 ES mechanisms evaluation by unconditional criteria

To unconditional criteria will refer the criteria, which implementation for the ES type cryptographic transformations is mandatory, that is unconditional.

Analysis of the application state, development and assessment experience of the ES type cryptographic transformations properties, primarily in a group of EC points, the achieved results in the

practical solution of cryptanalysis tasks and various attacks implementing, allow as basic to choose the following unconditional evaluation criteria [6]:

$W_{\delta 1}$ – mathematical base reliability, which used in the cryptographic transformations for ES;

$W_{\delta 2}$ – ES type cryptographic transformations against known attacks practical protection;

$W_{\delta 3}$ – ES real protection against all known and the potential cryptanalytic attacks;

$W_{\delta 4}$ – ES type cryptographic transformation statistical safety;

$W_{\delta 5}$ – ES type cryptographic transformation in a group of EC points theoretical protection;

$W_{\delta 6}$ – the absence of ES type cryptographic transformation weak private key;

$W_{\delta 7}$ – the complexity of the direct I_{np} and reverse $I_{зв}$ cryptographic transformations regarding ES is not higher than polynomial character.

Since the presented partial criteria are unconditional, then the selection criterion is a logical variable yes/no (1/0), so unconditional criterion can be written as [6]:

$$\left(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}\right) \in (1,0). \quad (1)$$

Given the described above partial unconditional criteria $W_{\delta 1}$–$W_{\delta 7}$ and condition (1) cryptographic transformation accordance function can be presented as:

$$f_{фв}(\ ) = \mathrm{W}_{\delta 1} \wedge \mathrm{W}_{\delta 2} \wedge \mathrm{W}_{\delta 3} \wedge \mathrm{W}_{\delta 4} \wedge \mathrm{W}_{\delta 5} \wedge \mathrm{W}_{\delta 6} \wedge \mathrm{W}_{\delta 7}. \quad (2)$$

Hence, the quality of ES cryptographic transformation can be estimated using unconditional integral criterion – ES cryptographic transformation accordance function to requirements $f_{фв}(\ ) \in (0;1)$ and on $f_{фв}(\ ) = 1$ ES cryptographic transformation, that estimated, complies with the requirements.

Introduced thereby integral criterion allows to establish, whether the considered ES type cryptographic transformation complies considered discussed requirements. If the ES complies with the requirements, it can be reasonably recommended for use.

Provided a positive assessment of ES by integral unconditional criterion, further comparison and evaluation can be made based on the conditional criteria and integral conditional criterion [6].

3.3 ES mechanisms evaluation by conditional criteria

Research has shown that qualitative and quantitative comparison of ES type cryptographic transformations can be carried out using generalized conditional preference criterion [6] or integral conditional criterion.

As the main partial conditional criteria can (proposed) use the following:

W_{y1} – the possibility and conditions of free distribution and use of international or national ES cryptographic transformations standard in Ukraine taking into account Ukraine normative acts to export, import and restrictions on its use, including the provision of electronic trust services;

W_{y2} – the level of trust in international and national cryptographic transformation in a group of EC points standard, that defined by the results of researches and the degree of application extension and recognition in different countries, and internationally recognized systems, including for the provision of electronic trust services;

W_{y3} – the perspective of international or national standard application in Ukraine taking into account recognition and application perspective information and telecommunication systems, cloud computing and other information technology etc.;

W_{y4} – timing and spatial complexity of hardware, software, and hardware and software implementations ES means, and management and key certification, including for the provision of electronic trust services etc.;

W_{y5} – the possibility and conditions for the use of standards with different values of general system settings and keys, methods of making and maintenance public key certificates, including for the providing electronic trust services, etc.;

W_{y6} – ES flexibility degree from the standpoint of use in various applications, by different requirements and restrictions, in different conditions, the unification and standardization degree, including for the providing electronic trust services, etc.;

W_{y7} – the level of protection in the implementation of different types of threats, in different conditions of cryptanalytic attacks and rejection common parameters properties from the defined etc.;

W_{y8} – the possibility and conditions of use in the construction of anonymous signatures for national and international use, and the level of ensuring the anonymity.

Table 1 – Relations scale (degree of actions importance)

The importance degree	Definition	Explanation
1	**Equal importance**	Two actions do the same contribution to achieve the objective
3	Some advantage of one action importance over another (weak importance)	There are understandings in favor of advantage of one of the actions, but these understandings not enough convincing
5	**Substantial or strong importance**	There are reliable data or logical statements in order to show the advantage of one of the actions
7	**Obvious or very strong importance**	Convincing evidence in favor of one activity to another
9	**Absolute importance**	Evidence in favor of the advantage of one action to another supremely persuasive
2, 4, 6, 8	Intermediate values between two adjacent statements	The situation when it is necessary to compromise decision
Inverse values given above non-zero values	If to the actions i at comparison with the action j is ascribed one of the above mentioned non-zero integers, then to actions j at comparison with the action i is ascribed the reverse value	If coherence was postulated in obtaining N numerical values to form the matrix

If their application it is important to choose the method of clotting the partial conditional criteria to integral conditional criterion. The conducted analysis and practical researches have shown [4-6, 8-11, 15-21] that as a method of clotting the partial conditional criteria can choose the analytic hierarchy process based on pairwise comparisons and the weight indices determining method.

When using the analytic hierarchy process based on pairwise comparisons, obtained statements expressed in integers taking into account nine-point scale (table. 1) [4,6].

3.4 The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 by unconditional criteria evaluation

Table 2 shows the results of comparative analysis regarding unconditional criteria for ES mechanisms according to DSTU ISO/IEC 14888-3:2014. Further comparison and evaluation based on conditional criteria and integral conditional criterion will be carried out for all standard ES mechanisms, other than ES mechanisms DSA, KCDSA, Pointcheval/Vaudenay and SDSA, that mechanisms, based on the finite fields mathematical apparatus.

Table 2 – Results of comparative analysis regarding unconditional criteria

ES criterion / ES algorithm	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
DSA	0	1	0	1	0	1	1	0
KCDSA	0	1	0	1	0	1	1	0
Pointcheval/Vaudenay	0	1	0	1	0	1	1	0
SDSA	0	1	0	1	0	1	1	0
EC-DSA	1	1	1	1	1	1	1	1
EC-KCDSA	1	1	1	1	1	1	1	1
EC-GDSA	1	1	1	1	1	1	1	1
EC-RDSA	1	1	1	1	1	1	1	1
EC-SDSA	1	1	1	1	1	1	1	1
EC-FSDSA	1	1	1	1	1	1	1	1
IBS-1	1	1	1	1	1	1	1	1
IBS-2	1	1	1	1	1	1	1	1

3.5 The ES mechanisms according to DSTU ISO/IEC 9796-3:2014 by unconditional criteria evaluation

Table 3 shows the results of comparative analysis regarding unconditional criteria for ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 3 – Results of comparative analysis regarding unconditional criteria

ES criterion / ES algorithm	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
NR	1	1	1	1	1	1	1	1
ECNR	1	1	1	1	1	1	1	1
ECMR	1	1	1	1	1	1	1	1
ECAO	1	1	1	1	1	1	1	1
ECPV	1	1	1	1	1	1	1	1
ECKNR	1	1	1	1	1	1	1	1

Further comparison and evaluation based on conditional criteria and integral conditional criterion will be carried out for all standard ES mechanisms.

4 The analytic hierarchy process based on pairwise comparisons and features of its use for the ES algorithms evaluation

For use the analytic hierarchy process must choose a conditional criteria system. With such set of indicators, using the conditional criteria can calculate the integral conditional criteria value, and, consequently, make the comparison by integral conditional criterion.

The elements pairwise comparison method [4,6] can be described as follows. The set of paired comparisons matrices is constructed. Paired comparisons are carried out in terms of the dominance of one element over another. Obtained statements are expressed in integers, considering the nine scale in table 1 [4,6].

4.1 The analytic hierarchy process application analysis and conditions in cryptography

Analytic hierarchy process (AHP) – the systematic approach to the complex problems of making decision mathematical tool. AHP does not prescribe to the decision making person (DMP) any "right" decision, and allows him to interactively find this option (alternative), which the best agrees with its understanding of the problem essence and requirements to its solution [5,10,15,21].

This method belongs to the criteria class and is widely utilized at present, including in evaluative activity. Method is based on alternatives evaluating hierarchical procedure. It is represented as follows [5,21]:

Level 0: objective – to estimate the weight of approach to the evaluation.

Level 1: criteria – the reliability of the results; the conformity to the evaluation objectives.

Level 2: criteria – the reliability, due to the authenticity of the information; the reliability, due to the latitude of the information.

The analytic hierarchy process contains the priorities synthesis procedure, that are calculated on the basis of objective experts' statements.

The analytic hierarchy process application [5,21]:

1. The construction of the hierarchy quality problem model, includes objective, alternative options of the objective achieve and criteria for alternatives quality evaluation.
2. Setting all hierarchy elements priorities using the pair comparisons method.
3. The synthesis of global alternatives priorities by elements on hierarchy priorities linear convolution.
4. Check the statements on consistency.
5. Decision making based on the results.

If using AHP using so-called objectives tree (fig. 2).

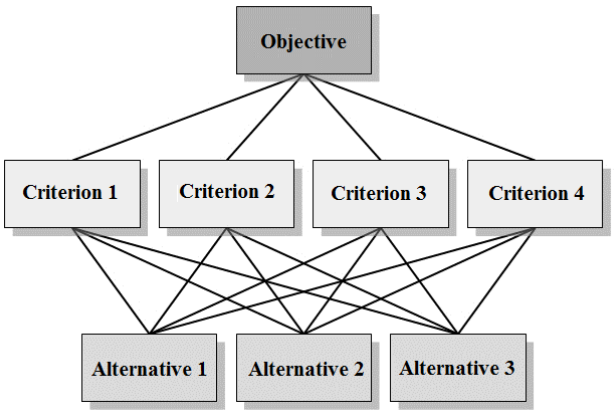

Figure 2 – Simple AHP hierarchy *(Objectives tree)*

4.2 The pairwise comparison method application analysis and conditions in cryptography

In pairwise comparison the expert compares investigated objects of their importance pairwise, establishing the most important object in each pair. All possible pairs of objects expert represents in a record of each combination (object 1 – object 2, object 2 – object 3, etc.) or in the matrix form [4,6].

The paired comparisons method is very simple and it allows to explore a large number of objects (compared, for example, by a rank method) and with greater accuracy [4].

Let $E_1,E_2,...,E_n$ – the plenty of n elements (alternatives) and $v_1,v_2,...,v_n$ – respectively their weight or intensity. Let compare pairwise the weight or intensity of each element with weight or intensity of any other element of the set relative to common to them property or objective (relative to father"–element). In this case, the pairwise comparisons matrix [E] is as follows:

The pairwise comparisons matrix has a reverse symmetry property, that is, $a_{ij}=1/a_{ji}$, where $a_{ij}=v_i/v_j$. In conducting pairwise comparisons should answer the following questions: which of the two compared elements is more important or has greater impact, which is more probable and which has a greater advantage.

When comparing the criteria, usually ask, which criterion is more important; when comparing alternatives in relation to the criterion – which of the alternatives has more advantages or more probable [4,6].

$[E] =$

	E_1	E_2	…	E_n
E_1	v_1/v_2	v_1/v_2	…	v_1/v_n
E_2	v_2/v_1	v_2/v_2	…	v_2/v_n
…	…	…	…	…
E_n	v_n/v_1	v_n/v_2	…	v_n/v_n

When constructing a pairwise comparisons matrix for all criteria, it is necessary to determine the consistency ratio [4,6] for each of criterion as follows. The assessment of eigenvector component is calculated by the formula (3):

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (3)$$

The normalized assessment of priority vector is calculated by the formula (4):

$$r_i = q_i \div z, \quad (4)$$

where z – consistency matrix ratio, which is calculated using the formula (5):

$$z = \sum_{i=1}^{n} q_i. \quad (5)$$

The consistency matrix ratio value is in the range $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ – the maximum possible eigenvector component evaluation value for the selected case.

4.3 The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 comparative analysis

Let us consider the practical application of the analytic hierarchy process based on pairwise comparisons on the example of ES mechanisms according to standard DSTU ISO/IEC 14888-3:2014. Comparing the ES algorithms relatively conditional criteria, construct for this objectives tree (fig. 3).

Now do the evaluation of each criterion. For this construct the pairwise comparisons matrix rela-

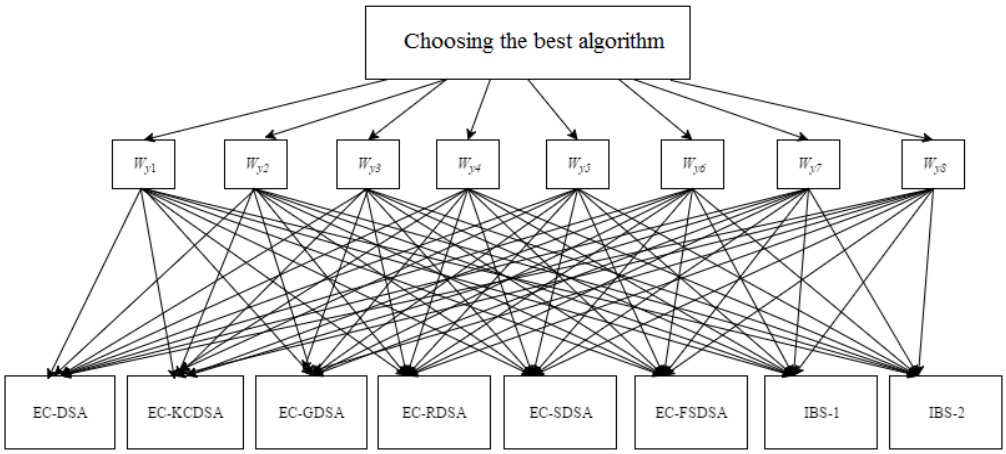

Figure 3 – Objectives tree (for DSTU ISO/IEC 14888-3:2014)

tive to the compared ES algorithms for each criterion (tabl. 4). As an example, we present a pairwise comparisons matrix relative to the compared ES algorithms for criterion W_{y1}. For this we construct table 5, using the formulas (3) – (5).

Table 4 – The criteria contribution to achieve a common objective, pairwise comparisons matrix

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	W_{y7}	W_{y8}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	1/7	3	0,575	0,048
W_{y2}	6	1	4	5	4	3	1/7	5	2,38	0,198
W_{y3}	1/4	1/4	1	3	2	1/2	1/7	1	0,636	0,053
W_{y4}	4	1/5	1/3	1	1/4	1/4	1/7	1/6	0,376	0,031
W_{y5}	2	1/4	1/2	4	1	1/3	1/7	1/4	0,575	0,048
W_{y6}	3	1/3	2	4	3	1	1/7	1	1,167	0,097
W_{y7}	7	7	7	7	7	7	1	7	5,489	0,456
W_{y8}	1/3	1/5	1	6	4	1	1/7	1	0,832	0,069

Other pairwise comparisons matrices are constructed similarly [4,6]. To calculate the resulting priorities vector multiply the level 1 priority vector and the level 1 acquired values matrix (fig. 4).

$$v := \begin{pmatrix} 0.048 \\ 0.198 \\ 0.053 \\ 0.031 \\ 0.048 \\ 0.097 \\ 0.456 \\ 0.069 \end{pmatrix} \qquad M := \begin{pmatrix} 0.201 & 0.087 & 0.082 & 0.076 & 0.166 & 0.21 & 0.051 & 0.205 \\ 0.201 & 0.169 & 0.165 & 0.061 & 0.166 & 0.229 & 0.102 & 0.19 \\ 0.201 & 0.124 & 0.165 & 0.103 & 0.166 & 0.192 & 0.086 & 0.19 \\ 0.029 & 0.025 & 0.021 & 0.05 & 0.049 & 0.027 & 0.02 & 0.028 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.334 & 0.147 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.344 & 0.147 \end{pmatrix}$$

$$V2 := M \cdot v \qquad V2^T = (0.099 \;\; 0.144 \;\; 0.125 \;\; 0.025 \;\; 0.048 \;\; 0.048 \;\; 0.256 \;\; 0.256)$$

Figure 4 – The resulting priorities vector calculation

The consistency ratio is 12,03. The consistency ratio of the pairwise comparisons matrix by criterion W_{y1} is 9,54.

Table 5 – The pairwise comparisons matrix by criterion W_{y1}

	EC-DSA	EC-KCDSA	EC-GDSA	EC-RDSA	EC-SDSA	EC-FSDSA	IBS-1	IBS-2	q_j	r_j
EC-DSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-KCDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-GDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-RDSA	1/5	1/5	1/5	1	1/3	1/3	1/5	1/5	0,278	0,029
EC-SDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
EC-FSDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
IBS-1	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118
IBS-2	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118

Let us consider the obtained numerical results. The investigated ES algorithms based on the transformation of group of EC points and pairing EC points can arrange the places, that they occupied on the results of comparison (1 – the best, 8 – the worst):

1. IBS-1 – 0,256;
2. IBS-2 – 0,256;
3. EC-KCDSA – 0,144;
4. EC-GDSA – 0,125;
5. EC-DSA – 0,099;
6. EC-SDSA – 0,048;
7. EC-FSDSA – 0,048;
8. EC-RDSA – 0,025.

Thus ES IBS-1,2 have the greatest advantages by an integral indicator. The ES algorithm EC-RDSA has the worst result, that is substantiated by the attacks implementation on the algorithm and the inability to use nationally. It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

4.4 The ES mechanisms according to DSTU ISO/IEC 9796-3:2014 comparative analysis

Let us consider the practical application of the analytic hierarchy process based on pairwise comparisons on the example of ES mechanisms according to standard DSTU ISO/IEC 9796-3:2014. Comparing the ES algorithms relatively conditional criteria, construct for this objectives tree (fig. 5).

Now do the evaluation of each criterion. For this construct the pairwise comparisons matrix relative to the compared ES algorithms for each criterion (table. 6).

The consistency ratio is 7,7037.

As an example, we present a pairwise comparisons matrix relative to the compared ES algorithms for criterion W_{y1}. For this we construct table 7, using the formulas (3) – (5). Other pairwise comparisons matrices are constructed similarly [4,6].

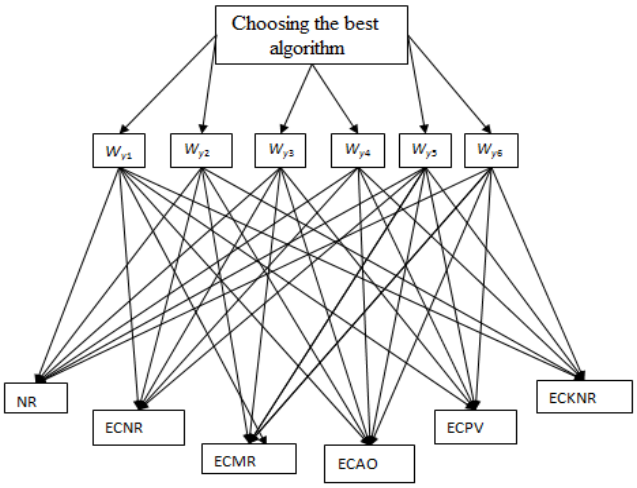

Figure 5 – Objectives tree

(for DSTU ISO/IEC 9796-3:2014)

Table 6 – The criteria contribution to achieve a common objective, pairwise comparisons matrix

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	0,5503	0,0714
W_{y2}	6	1	4	5	4	3	3,3604	0,4362
W_{y3}	1/4	1/4	1	3	2	1/2	0,7565	0,0982
W_{y4}	4	1/5	1/3	1	1/4	1/4	0,5054	0,0656
W_{y5}	2	1/4	1/2	4	1	1/3	0,8327	0,1081
W_{y6}	3	1/3	2	4	3	1	1,6984	0,2205

To calculate the resulting priorities vector multiply the level 1 priority vector and the level 1 acquired values matrix (fig. 6).

Let us consider the obtained numerical results. The investigated ES algorithms can arrange the places, that they occupied on the results of comparison (1 – the best, 6 – the worst):

1. ECPV – 0,252;
2. ECNR – 0,165;
3. ECAO – 0,155;
4. ECKNR– 0,139;
5. ECMR – 0,133;
6. NR – 0,108.

Table 7 – The pairwise comparisons matrix by criterion W_{y1}

	NR	ECNR	ECMR	ECAO	ECPV	ECKNR	q_j	r_j
NR	1	1/5	2	1/2	1/5	1/3	0,487	0,072
ECNR	5	1	1/4	3	2	3	1,680	0,25
ECMR	1/2	4	1	1/2	1/4	1/2	0,707	0,105
ECAO	2	1/3	2	1	1/4	1/3	0,693	0,103
ECPV	5	1/2	4	4	1	1/2	1,647	0,245
ECKNR	3	1/3	2	3	2	1	1,513	0,225

The consistency ratio is 6,72.

$$B1 := \begin{pmatrix} 0.071 \\ 0.436 \\ 0.098 \\ 0.065 \\ 0.108 \\ 0.220 \end{pmatrix} \qquad B2 := \begin{pmatrix} 0.072 & 0.05 & 0.105 & 0.103 & 0.245 & 0.025 \\ 0.101 & 0.16 & 0.080 & 0.140 & 0.334 & 0.127 \\ 0.042 & 0.27 & 0.08 & 0.161 & 0.373 & 0.146 \\ 0.046 & 0.104 & 0.343 & 0.157 & 0.068 & 0.280 \\ 0.167 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.152 & 0.183 & 0.193 & 0.192 & 0.136 & 0.142 \end{pmatrix}$$

$$B := B1^{T} \cdot B2 = (0.108 \quad 0.165 \quad 0.133 \quad 0.155 \quad 0.252 \quad 0.139)$$

Figure 6 – The resulting priorities vector calculation

The most perspective in DSTU ISO/IEC 9796-3:2014 are ES mechanisms ECPV (*elliptic curve Pintsov-Vanstone message recovery signature*) and ECNR (*elliptic curve Nyberg-Rueppel message recovery signature*). ECPV uses symmetric encryption (to include information in the signature) and does not provide limits on the amount of renewable information. NR algorithm has the worst result by an integral indicator, that is substantiated by mathematical apparatus, that is used in this algorithm.

5 Method and procedure of evaluation and comparative analysis ES algorithms based on weight indices

In the case, when get information about parameters comparable systems importance using informal methods is not possible, necessary to use formalized methods. Among them are methods based on determining the weight indices. There are several such methods [9,11,18-20], some of them are considered detail below.

Let us consider the general problem formulation for ES evaluation technique based on the determining the weight indices method.

Let there are [9,11,18-20]:

1) *k* systems (ES mechanisms), which is necessary to evaluate;

2) *m* indicators, according to which systems are evaluated;

3) n experts, that carry out the evaluation.

We define some partial indicators, at which can be evaluated ES mechanisms:

x_1 – the possibility of free distribution and use of international or national ES cryptographic transformations standard in Ukraine;

x_2 – the level of trust in international and national cryptographic transformation in a group of EC points and based on mathematical apparatus of pairing EC points;

x_3 – the perspective of international or national standard application in Ukraine;

x_4 – the timing and spatial complexity of hardware, software, and hardware and software implementations ES means;

x_5 – the possibility of the standards use with different values of general system settings and keys;

x_6 – the ES algorithm flexibility degree from the standpoint of use in various applications, by different requirements and restrictions;

x_7 – the level of protection against the different types of threats in different conditions of cryptanalytic attacks;

x_8 – the possibility of use ES algorithm in the construction of anonymous signatures for national and international use, and the level of ensuring the anonymity.

Now determine the weight indices values of indicators themselves. We carry out the expert evaluation of the above partial indicators for this purpose. We'll use the following methods for the weight indices determining [9,11,18-20,22] for evaluation: 1 - using the Fishburn scale; 2 - based on the ranking method; 3 - based on the points attribution method; 4 - based on the numerical method.

After the weight indices values of indicators themselves determining, it is necessary to make the system expert evaluation by the chosen determining weight indices methods.

For this, for each system it is need to perform the indicators ranking in connection with that, which indicator is the most determined in chosen system, better than other describes it. That is, arrange the indicators in relation to the chosen system, from more significant to least significant.

5.1 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 using the Fishburn scale

Let as input is selected the following:

n – the number of experts, $n=5$

m – the number of indicators, $m=8$

We construct the table of the Fishburn scale method indicators value for ES algorithms of standard DSTU ISO/IEC 14888-3:2014 (EC-DSA, EC-GDSA, EC-KCDSA, EC-RDSA, EC-SDSA, EC-FSDSA, IBS-1 and IBS-2), accordance with the rules of the evaluation according to the specified method. The results are shown in table 8.

Table 8 – Weight indices values

Experts	**Indicators**							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	0,194	0,167	0,111	0,139	0,056	0,028	0,222	0,083
2	0,194	0,167	0,111	0,083	0,028	0,056	0,222	0,139
3	0,222	0,139	0,111	0,056	0,028	0,083	0,194	0,167
4	0,222	0,111	0,139	0,028	0,083	0,056	0,194	0,167
5	0,167	0,139	0,028	0,056	0,111	0,083	0,222	0,194
w_i	0,200	0,144	0,100	0,072	0,061	0,061	0,211	0,150

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014. After the evaluation, we obtain the following results, shown in fig. 7.

$$M\_Fishbem := \begin{pmatrix} 0.211 & 0.172 & 0.128 & 0.078 & 0.044 & 0.072 & 0.161 & 0.156 \\ 0.2 & 0.189 & 0.144 & 0.05 & 0.056 & 0.094 & 0.128 & 0.139 \\ 0.194 & 0.167 & 0.139 & 0.05 & 0.05 & 0.072 & 0.161 & 0.167 \\ 0.067 & 0.061 & 0.072 & 0.2 & 0.194 & 0.189 & 0.106 & 0.111 \\ 0.061 & 0.05 & 0.056 & 0.167 & 0.172 & 0.167 & 0.167 & 0.161 \\ 0.061 & 0.05 & 0.056 & 0.161 & 0.161 & 0.183 & 0.178 & 0.15 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \end{pmatrix}$$

$V\_Fishbem := w\_pokaz1$

$V\_Fishbem = (0.2 \quad 0.144 \quad 0.1 \quad 0.072 \quad 0.061 \quad 0.061 \quad 0.211 \quad 0.15)$

$Rez\_Fishbem := M\_Fishbem \cdot V\_Fishbem^T$

$Rez\_Fishbem^T = (0.15 \quad 0.142 \quad 0.147 \quad 0.106 \quad 0.117 \quad 0.118 \quad 0.159 \quad 0.159)$

Figure 7 – The priorities resulting vector calculation

Further carry out analysis of the results according to fig. 7. For this we place *Rez_Fishbern* values as they decrease, i.e.

1. IBS-1 – 0,159;
2. IBS-2 – 0,159;
3. EC-DSA – 0,15;
4. EC-GDSA – 0,147;
5. EC-KCDSA – 0,142;
6. EC-FSDSA – 0,118;
7. EC-SDSA – 0,117;
8. EC-RDSA – 0,106.

It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

5.2 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 using the Fishburn scale

Let as input is selected the following:

n – the number of experts, $n=4$

m – the number of indicators, $m=6$

Table 9 – Ranking indicators by experts

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6
1	1	6	5	2	3	4
2	3	4	6	1	5	2
3	1	4	5	3	6	2
4	2	3	6	1	4	5

We construct the table of the Fishburn scale method indicators value for ES algorithms of standard DSTU ISO/IEC 9796-3, accordance with the rules of the evaluation according to the specified method. The results are shown in table 9–10. Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 10 – Weight indices values

Experts	Indicators					
	x_1	x_2	x_3	x_4	x_5	x_6
1	0,285	0,047	0,095	0,238	0,190	0,142
2	0,190	0,142	0,047	0,285	0,095	0,238
3	0,285	0,142	0,095	0,190	0,047	0,238
4	0,238	0,190	0,047	0,285	0,142	0,095
w_i	0,249	0,130	0,071	0,249	0,118	0,178

After the evaluation, we obtain the following results, shown in fig. 8.

Further carry out analysis of the results according to fig. 8. For this we place *Rez_1* values as they decrease, i.e.

1. ECPV – 0,245;
2. ECNR – 0,223;
3. ECAO – 0,186;
4. ECKNR – 0,179;
5. ECMR – 0,160;
6. NR – 0,144.

It should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

$$M\_1 := \begin{bmatrix} 0.142 & 0.130 & 0.273 & 0.106 & 0.249 & 0.094 \\ 0.273 & 0.130 & 0.082 & 0.190 & 0.379 & 0.226 \\ 0.094 & 0.189 & 0.166 & 0.249 & 0.237 & 0.059 \\ 0.225 & 0.190 & 0.566 & 0.106 & 0.154 & 0.118 \\ 0.118 & 0.273 & 0.237 & 0.522 & 0.142 & 0.094 \\ 0.273 & 0.094 & 0.142 & 0.202 & 0.201 & 0.08 \end{bmatrix}$$

$$V\_F := \begin{bmatrix} 0.249 & 0.130 & 0.071 & 0.249 & 0.118 & 0.178 \end{bmatrix}$$

$$Rez\_1 := M\_1 \cdot V\_F^{\mathrm{T}}$$

$$Rez\_1^{\mathrm{T}} = \begin{bmatrix} 0.144 & 0.223 & 0.16 & 0.186 & 0.245 & 0.179 \end{bmatrix}$$

Figure 8 – The priorities resulting vector calculation

5.3 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the ranking method

n – the number of experts, n=5

m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 11).

Table 11 – Weight indices values

Experts	Indicators							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	7	6	5	4	2	1	8	3
2	8	7	5	3	1	2	6	4
3	8	6	4	3	2	1	7	5
4	7	6	3	4	1	2	8	5
5	6	7	5	3	2	1	8	4
$r_j = \sum_{i=1}^{n} r_{ij}$	36	32	22	17	8	7	37	21
w_j	0,2	0,178	0,122	0,094	0,044	0,039	0,206	0,117

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014. After the evaluation, we obtain the following results, shown in fig. 9.

$$M\_Ranj := \begin{pmatrix} 0.189 & 0.183 & 0.156 & 0.1 & 0.067 & 0.061 & 0.072 & 0.172 \\ 0.189 & 0.161 & 0.122 & 0.056 & 0.072 & 0.094 & 0.15 & 0.156 \\ 0.194 & 0.15 & 0.172 & 0.05 & 0.061 & 0.106 & 0.144 & 0.122 \\ 0.05 & 0.05 & 0.067 & 0.133 & 0.194 & 0.2 & 0.133 & 0.172 \\ 0.05 & 0.061 & 0.056 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.056 & 0.061 & 0.05 & 0.156 & 0.15 & 0.161 & 0.183 & 0.183 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \end{pmatrix}$$

$$V\_Ranj := w\_pokaz2$$

$$V\_Ranj = (0.2 \quad 0.178 \quad 0.122 \quad 0.094 \quad 0.044 \quad 0.039 \quad 0.206 \quad 0.117)$$

$$Rez\_Ranj := M\_Ranj \cdot V\_Ranj^{T}$$

$$Rez\_Ranj^{T} = (0.139 \quad 0.143 \quad 0.142 \quad 0.103 \quad 0.111 \quad 0.115 \quad 0.147 \quad 0.147)$$

Figure 9 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 9. For this we place *Rez_Ranj* values as they decrease, i.e.

1. IBS-1 – 0,147;
2. IBS-2 – 0,147;
3. EC-KCDSA – 0,143;
4. EC-GDSA – 0,142;
5. EC-DSA – 0,139;
6. EC-FSDSA – 0,115;
7. EC-SDSA – 0,111;
8. EC-RDSA – 0,103.

Thus ES IBS-1 and IBS-2 have the greatest advantages by the integral indicator. ES algorithm EC-RDSA (*as in the case of the analytic hierarchy process and method based on the Fishburn scale comparison*) has the worst result, that is substantiated by attack implementation on this algorithm and its inability to use nationally.

5.4 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the ranking method

n – the number of experts, n=4

m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 12). Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 12 – Weight indices values

Experts	**Indicators**					
	x_1	x_2	x_3	x_4	x_5	x_6
1	5	1	4	6	3	2
2	4	2	6	5	3	1
3	5	3	6	4	2	1
4	5	2	4	6	1	3
$r_j = \sum_{i=1}^{n} r_{ij}$	19	8	20	21	9	7
w_j	0,226	0,095	0,238	0,250	0,226	0,083

After the evaluation, we obtain the following results, shown in fig. 10. Further we carry out analysis of the results according to fig. 10. For this we place *Rez_2* values as they decrease, i.e.

1. ECNR – 0,209;
2. ECPV – 0,207;
3. ECKNR – 0,200;
4. ECAO – 0,179;
5. ECMR – 0,168;
6. NR – 0,157.

Thus ES ECNR has the greatest advantages by the integral indicator. ES algorithm NR (*as in the case of the analytic hierarchy process and method based on the Fishburn scale comparison*) has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

$$M\_2 := \begin{bmatrix} 0.130 & 0.270 & 0.178 & 0.059 & 0.107 & 0.250 \\ 0.107 & 0.059 & 0.238 & 0.202 & 0.273 & 0.119 \\ 0.071 & 0.190 & 0.071 & 0.166 & 0.238 & 0.261 \\ 0.154 & 0.261 & 0.059 & 0.261 & 0.130 & 0.130 \\ 0.250 & 0.130 & 0.095 & 0.238 & 0.226 & 0.059 \\ 0.107 & 0.059 & 0.154 & 0.238 & 0.261 & 0.178 \end{bmatrix}$$

$$V\_2 := [0.226 \quad 0.095 \quad 0.238 \quad 0.250 \quad 0.226 \quad 0.083]$$

$$Rez\_2 := M\_2 \cdot V\_2^{\mathrm{T}}$$

$$Rez\_2^{\mathrm{T}} = [0.157 \quad 0.209 \quad 0.168 \quad 0.179 \quad 0.207 \quad 0.2]$$

Figure 10 – The priorities resulting vector calculation

5.5 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the points attribution method

n – the number of experts, n=5

m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 13). Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014.

Table 13 – Weight indices values

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$\sum_{j=1}^{m} h_{ij}$	Indicators weights							
										r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}	r_{i7}	r_{i8}
1	7	5	2	4	6	1	10	8	43	0,163	0,116	0,046	0,093	0,139	0,023	0,232	0,186
2	6	5	3	4	9	2	8	7	44	0,136	0,114	0,068	0,091	0,204	0,045	0,182	0,159
3	8	6	1	5	4	3	9	7	43	0,186	0,140	0,023	0,116	0,093	0,070	0,209	0,163
4	7	5	3	8	4	2	9	6	44	0,159	0,114	0,068	0,182	0,091	0,045	0,204	0,136
5	9	6	2	5	4	3	10	7	45	0,196	0,130	0,043	0,109	0,087	0,065	0,217	0,152
									$\sum_{i=1}^{n} r_j$	0,84	0,614	0,248	0,591	0,614	0,248	1,044	0,796
									w_j	0,168	0,123	0,050	0,118	0,123	0,050	0,209	0,159

After the evaluation, we obtain the following results, shown in fig. 11. Further we carry out analysis of the results according to fig. 11. For this we place *Rez_Bal* values as they decrease, i.e.

1. IBS-1 – 0,137;
2. IBS-2 – 0,137;
3. EC-RDSA – 0,132;
4. EC-FSDSA – 0,128;
5. EC-DSA – 0,127;
6. EC-SDSA – 0,127;
7. EC-GDSA – 0,126;
8. EC-KCDSA – 0,124.

$$M\_2 := \begin{bmatrix} 0.130 & 0.270 & 0.178 & 0.059 & 0.107 & 0.250 \\ 0.107 & 0.059 & 0.238 & 0.202 & 0.273 & 0.119 \\ 0.071 & 0.190 & 0.071 & 0.166 & 0.238 & 0.261 \\ 0.154 & 0.261 & 0.059 & 0.261 & 0.130 & 0.130 \\ 0.250 & 0.130 & 0.095 & 0.238 & 0.226 & 0.059 \\ 0.107 & 0.059 & 0.154 & 0.238 & 0.261 & 0.178 \end{bmatrix}$$

$$V\_2 := [0.226 \quad 0.095 \quad 0.238 \quad 0.250 \quad 0.226 \quad 0.083]$$

$$Rez\_2 := M\_2 \cdot V\_2^{\mathrm{T}}$$

$$Rez\_2^{\mathrm{T}} = [0.157 \quad 0.209 \quad 0.168 \quad 0.179 \quad 0.207 \quad 0.2]$$

Figure 11 – The priorities resulting vector calculation

5.6 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the points attribution method

n – the number of experts, n=4
m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 14).

Table 14 – Weight indices values

Indicators / Experts	x_1	x_2	x_3	x_4	x_5	x_6	$\sum_{j=1}^{m} h_{ij}$	Indicators weights					
								r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}
1	8	7	10	2	5	4	36	0,222	0,194	0,277	0,055	0,138	0,111
2	7	8	9	1	4	3	32	0,218	0,250	0,281	0,031	0,125	0,093
3	9	5	7	1	3	2	27	0,333	0,185	0,259	0,037	0,111	0,074
4	8	6	10	1	4	3	32	0,250	0,187	0,312	0,031	0,125	0,093
							$\sum_{i=1}^{n} r_j$	1,023	0,816	1,129	0,154	0,499	0,371
							w_j	0,256	0,204	0,282	0,038	0,125	0,092

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

After the evaluation, we obtain the following results, shown in fig. 12.

Further we carry out analysis of the results according to fig. 12. For this we place *Rez_3* values as they decrease, i.e.

1. ECPV – 0,202;
2. ECNR – 0,170;
3. ECKNR – 0,162;
4. ECAO – 0,148;
5. ECMR – 0,138;
6. NR – 0,130.

Like in the previous method, ES NR has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

ES mechanism ECPV has the best result.

$$M\_3 := \begin{bmatrix} 0.162 & 0.037 & 0.089 & 0.290 & 0.185 & 0.233 \\ 0.108 & 0.175 & 0.245 & 0.178 & 0.120 & 0.170 \\ 0.155 & 0.065 & 0.086 & 0.229 & 0.295 & 0.164 \\ 0.061 & 0.282 & 0.115 & 0.202 & 0.123 & 0.212 \\ 0.197 & 0.248 & 0.284 & 0.107 & 0.100 & 0.049 \\ 0.226 & 0.06 & 0.179 & 0.231 & 0.167 & 0.128 \end{bmatrix}$$

$$V\_3 := [0.256 \;\; 0.204 \;\; 0.282 \;\; 0.038 \;\; 0.125 \;\; 0.092]$$

$$Rez\_3 := M\_3 \cdot V\_3^{\mathrm{T}}$$

$$Rez\_3^{\mathrm{T}} = [0.13 \;\; 0.17 \;\; 0.138 \;\; 0.148 \;\; 0.202 \;\; 0.162]$$

Figure 12 – The priorities resulting vector calculation

5.7 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 14888-3:2014 based on the numerical method

n – the number of experts, n=5
m – the number of indicators, m=8

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 15). Coefficients values are selected from the method based on the Fishburn scale.

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 14888-3:2014.

Table 15 – Weight indices values

Indicators / Evaluation	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
$x_{i\min}$	0,167	0,111	0,028	0,028	0,028	0,028	0,194	0,083
$x_{i\max}$	0,222	0,167	0,139	0,139	0,111	0,083	0,222	0,194
δ_i	0,250	0,333	0,800	0,800	0,750	0,667	0,125	0,571
w_i	0,058	0,078	0,186	0,186	0,175	0,155	0,029	0,133

After the evaluation, we obtain the following results, shown in fig. 13.

$$M\_Chisl := \begin{pmatrix} 0.065 & 0.075 & 0.131 & 0.196 & 0.131 & 0.229 & 0.075 & 0.098 \\ 0.059 & 0.059 & 0.101 & 0.156 & 0.156 & 0.205 & 0.117 & 0.147 \\ 0.09 & 0.103 & 0.15 & 0.16 & 0.16 & 0.18 & 0.069 & 0.09 \\ 0.166 & 0.147 & 0.166 & 0.055 & 0.055 & 0.055 & 0.178 & 0.178 \\ 0.15 & 0.15 & 0.15 & 0.113 & 0.113 & 0.113 & 0.113 & 0.097 \\ 0.155 & 0.155 & 0.155 & 0.117 & 0.117 & 0.117 & 0.087 & 0.1 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \end{pmatrix}$$

$V\_Chisl := w\_pokaz4$

$V\_Chisl = (0.058 \;\; 0.078 \;\; 0.186 \;\; 0.186 \;\; 0.175 \;\; 0.155 \;\; 0.029 \;\; 0.133)$

$Rez\_Chisl := M\_Chisl \cdot V\_Chisl^{T}$

$Rez\_Chisl^{T} = (0.144 \;\; 0.138 \;\; 0.141 \;\; 0.109 \;\; 0.123 \;\; 0.126 \;\; 0.15 \;\; 0.15)$

Figure 13 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 13. For this we place *Rez_Chisl* values as they decrease, i.e.

1. IBS-1 – 0,15;
2. IBS-2 – 0,15;
3. EC-DSA – 0,144;
4. EC-GDSA – 0,141;
5. EC-KCDSA – 0,138;
6. EC-FSDSA – 0,126;
7. EC-SDSA – 0,123;
8. EC-RDSA – 0,109.

Also in this case it should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

5.8 The weight indices determining method, evaluations and comparative analysis of ES mechanisms according to DSTU ISO/IEC 9796-3:2014 based on the numerical method

n – the number of experts, n=4

m – the number of indicators, m=6

We construct the table for indicators, accordance with the rules of the evaluation according to the specified method (table 16). Coefficients values are selected from the method based on the Fishburn scale.

Similarly, we construct tables for all ES mechanisms according to DSTU ISO/IEC 9796-3:2014.

Table 16 – Weight indices values

Indicators / Evaluation	x_1	x_2	x_3	x_4	x_5	x_6
$x_{i\min}$	0,190	0,047	0,047	0,190	0,047	0,095
$x_{i\max}$	0,285	0,190	0,095	0,285	0,190	0,238
δ_i	0,333	0,752	0,505	0,333	0,752	0,600
w_i	0,101	0,229	0,154	0,101	0,229	0,183

After the evaluation, we obtain the following results, shown in fig. 14.

$$M\_4 := \begin{bmatrix} 0.246 & 0.053 & 0.109 & 0.262 & 0.108 & 0.219 \\ 0.054 & 0.108 & 0.224 & 0.180 & 0.216 & 0.216 \\ 0.250 & 0.166 & 0.054 & 0.250 & 0.054 & 0.222 \\ 0.073 & 0.083 & 0.357 & 0.179 & 0.223 & 0.083 \\ 0.052 & 0.240 & 0.214 & 0.213 & 0.214 & 0.064 \\ 0.227 & 0.170 & 0.204 & 0.113 & 0.113 & 0.171 \end{bmatrix}$$

$$V\_4 := [0.101 \;\; 0.229 \;\; 0.154 \;\; 0.101 \;\; 0.229 \;\; 0.183]$$

$$Rez\_4 := M\_4 \cdot V\_4^{\mathrm{T}}$$

$$Rez\_4^{\mathrm{T}} = [0.145 \;\; 0.172 \;\; 0.15 \;\; 0.166 \;\; 0.175 \;\; 0.162]$$

Figure 14 – The priorities resulting vector calculation

Further we carry out analysis of the results according to fig. 14. For this we place *Rez_4* values as they decrease, i.e.

1. ECPV – 0,175;
2. ECNR – 0,172;
3. ECAO – 0,166;
4. ECKNR – 0,162;
5. ECMR – 0,150;
6. NR – 0,145.

Also in this case it should be noted, that the results cannot be taken for use, most likely, this is the ES comparison technique. For real use you'll need to choose conditional criteria and conduct researches.

6 The analysis of ES researches results according to DSTU ISO/IEC 14888-3:2014

For chosen ES mechanisms evaluation techniques were obtained results, that are shown in previous chapters. ES mechanisms comparison was made based on expert evaluations. After that, calculations were made by aforementioned techniques.

One can assume, that the results of the evaluation ES mechanisms according to DSTU ISO/IEC 14888-3:2014, by different methods have been obtained almost identical – almost the same ES mechanisms arrangement from the best to the worst. Numeric scatter of weight indices values for one algorithm is almost negligible, only numeric values for ES mechanisms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons differ from weight indices values for these ES mechanisms according to other evaluation methods, that is substantiated by more strong influence of the subjective experts opinion.

Fig. 15 graphically shows the results of the ES mechanisms evaluation by different evaluation methods.

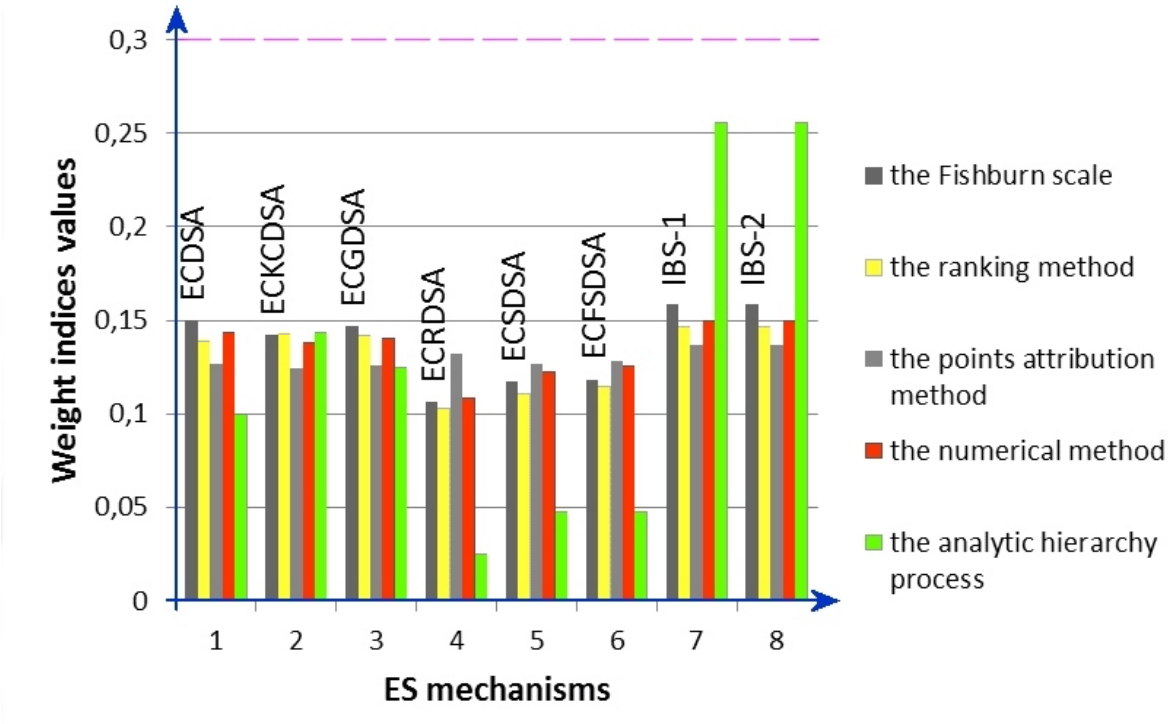

Figure 15 – Analysis of the comparisons results

7 The analysis of ES researches results according to DSTU ISO/IEC 9796-3:2014

For chosen ES mechanisms evaluation methods were obtained results, that are shown in previous chapters. ES mechanisms comparison was made based on expert evaluations. After that, calculations were made by aforementioned techniques.

ES mechanisms according to DSTU ISO/IEC 9796-3:2014 assessments have a similar ranking order by different evaluation methods – from highest to lowest.

Fig. 16 graphically shows the results of the ES mechanisms evaluation by different evaluation methods. The numbers from 1 to 6 are indicated the ES mechanisms: 1 – NR; 2 – ECNR; 3 – ECMR; 4 – ECAO; 5 – ECPV; 6 – ECKNR.

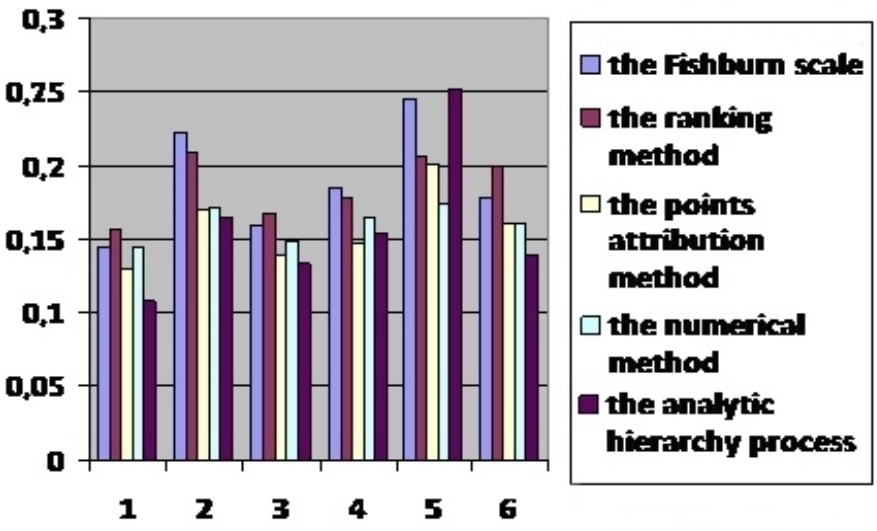

Figure 16 – The results of the ES mechanisms evaluation by different methods

8 Conclusions

1. In connection with the specific requirements for cryptographic transformations, including for ES, the main criteria should be divided into two classes: conditional and unconditional.

Unconditional criteria are those criteria, whose execution for any cryptographic transformations is mandatory, that is unconditional.

Conditional are called criteria, whose execution for any cryptographic transformations is occurred only on certain condition.

2. As a result of conducted researches, it was determined, that as the main criterion for integral evaluation can be and is recommended to use the integral unconditional criterion, that is derived by partial unconditional criteria.

If at least one partial criterion does not meet conditions, such cryptographic transformation is rejected as being, that does not meet the requirements.

3. The proposed comparative analysis technique of standardized ES based on the use of the partial unconditional and conditional criteria set, upon which calculated integral conditional and integral unconditional criteria value.

4. The research results allow to conclude, that in terms of evaluation objective the best use the weight indices determining method, because the experts subjectivity has the a significant impact to the result in the analytic hierarchy process based on pairwise comparisons.

5. The comparative analysis results of standardized ES algorithms DSTU ISO/IEC 14888-3:2014 allowed to make the following conclusions and recommendations: the maximum integral conditional criterion value for DSTU ISO/IEC 14888-3:2014 has been achieved for algorithms IBS-1 and IBS-2 by all evaluation methods.

The ES mechanisms according to DSTU ISO/IEC 14888-3:2014 evaluation results have been obtained almost identical by different methods. Numeric scatter of weight indices values for one algorithm is almost negligible, only numeric values for ES mechanisms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons differ from weight indices values for these ES mechanisms according to other evaluation methods, that is substantiated by more strong influence of the subjective experts opinion in this method.

According to all evaluation methods in the first place are ES mechanisms IBS-1 and IBS-2, and in the last place – ES mechanisms EC-RDSA *(only for the determining the weight indices method based on the points attribution method on the last place based ES mechanism EC-KCDSA).*

6. Comparative analysis of signature mechanisms according to DSTU ISO/IEC 9796-3:2014 has shown that the most perspective mechanisms are signature mechanisms ECPV *(elliptic curve Pintsov-Vanstone message recovery signature)* and ECNR *(elliptic curve Nyberg-Rueppel message recovery signature).*

ES algorithm NR has the worst result, that is substantiated by mathematical apparatus used in this algorithm.

7. To obtain more precise evaluation results and for exact match of ES arrangement mechanisms by all evaluation methods, it is necessary to perform the evaluation procedure several times and carefully approach to the choice of experts that will conduct the evaluation.

References

[1] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2): 2014. – 130 p.

[2] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2 (2006-11-15)): 2006. – 68 p.

[3] Information technology – Security techniques – Digital signatures schemes giving message recovery. – Part 3: Discrete logarithm based mechanisms: ISO/IEC 9796-3:2014.

[4] Andreichikov A.V. Analiz, sintez, planirovanie reshenii v ekonomike / A.V. Andreichikov, O.N. Andreichikova // – M.: Finansy i statistika, 2002. – 359 s.

[5] Analiticheskaya ierarkhicheskaya protsedura Saati [E-resource]. – Access mode: http://www.gorskiy.ru/Articles/Dmss / AHP.html.

[6] Gorbenko Ju.I. Metody pobuduvannja ta analizu kryptografichnyh system. Monografija. / Ju.I. Gorbenko // Kharkiv. Fort. 2015, 959 s.

[7] Informacijni tehnologii' – Kryptografichnyj zahyst informacii' – Cyfrovyj pidpys, shho g'runtujet'sja na eliptychnyh kryvyh – Formuvannja ta perevirka: DSTU 4145-2002. – K.: Derzhstandart Ukrai'ny, 2003. – 35 s. – (Nacional'ni standarty Ukrai'ny).
[8] Korchenko A.G. Postroenie sistem zashchity informatsii na nechetkikh mnozhestvakh / A.G. Korchenko // – M.: MK-Press, 2006. – 320 s.
[9] Makarova I.L. Analiz metodov opredeleniya vesovykh koeffitsientov v integral'nom pokazatele obshchestvennogo zdorov'ya / I.L. Makarova // Mezhdunarodnyi nauchnyi zhurnal «Simvol nauki», Ufa, 2015. – № 7 – S. 87–94.
[10] Metod analiza ierarkhii [E-resource]. – Access mode: https://ru.wikipedia.org/wiki/ Metod analiza ierarkhii.
[11] Metody opredeleniya vesovykh koeffitsientov [E-resource]. – Access mode: http://8v83.tom.ru/.
[12] Metody ekspertnykh otsenok [E-resource]. – Access mode: https://habrahabr.ru/post/189626/.
[13] Metod ekspertnykh otsenok [E-resource]. – Access mode: http://center-yf.ru/data/Marketologu/Metod-ekspertnyh-ocenok.php.
[14] Novyc'kyj A. M. Elektronnyj dokumentoobig jak element zabezpechennja pravovogo reguljuvannja stanovlennja instytutiv informacijnogo suspil'stva / A.M. Novyc'kyj // Naukovyj visnyk Nacional'nogo universytetu derzhavnoi' podatkovoi' sluzhby Ukrai'ny (ekonomika, pravo). – 2013. – № 4. – S. 11–20. – Rezhym dostupu: http://nbuv.gov.ua/UJRN/Nvnudpsu_2013_4_3.
[15] Nogin V.D. Uproshchennyi variant metoda analiza ierarkhii na osnove nelineinoi svertki kriteriev / V.D. Nogin // Access mode: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf.
[16] Okunev Yu.B. Printsipy sistemnogo podkhoda k proektirovaniyu v tekhnike svyazi / Yu.B. Okunev, V.G. Plotnikov // – M.: Svyaz', 1975. – 184 s.
[17] Orlovskii S.A. Problemy prinyatiya reshenii pri nechetkoi iskhodnoi informatsii / S.A. Orlovskii // – M.: Nauka, 1981. – 208 s.
[18] Postnikov V.M Metody vybora vesovykh koeffitsientov lokal'nykh kriteriev / V.M. Postnikov, S.B. Spiridonov // NAUKA i OBRAZOVANIE – Nauchnoe izdanie MGTU im. N.E. Baumana, 2015. – № 6. Access mode: http://technomag.bmstu.ru/index.html.
[19] Potapov D.K. O metodikakh opredeleniya vesovykh koeffitsientov v zadache otsenki nadezhnosti kommercheskikh bankov / D.K. Potapov, V.V. Evstaf'eva // Access mode: http://www.ibl.ru/konf/041208/60.pdf.
[20] Romanova I.K. Ob odnom podkhode k opredeleniyu vesovykh koeffitsientov metoda prostranstva sostoyanii / I.K. Romanova // NAUKA i OBRAZOVANIE – Nauchnoe izdanie MGTU im. N.E. Baumana, 2015. – № 4. Access mode: http://technomag.bmstu.ru/doc/763768.html.
[21] Saati T. Prinyatie reshenii: metod analiza ierarkhii / T. Saati // per. s angl. – M.: Radio i svyaz', 1993.
[22] Soglasovanie rezul'tatov otsenki ob"ektov uluchshenii [E-resource]. – Access mode: http://edu.dvgups.ru/METDOC/EMEN/FK/OTS_NEDV/METOD/UP/frame/3_4.htm.
[23] Ekspertnoe otsenivanie [E-resource]. – Access mode: https://ru.wikipedia.org/wiki/Ekspertnoe otsenivanie.
[24] Ekspertnye otsenki pri razrabotke reshenii [E-resource]. – Access mode: http://books.ifmo.ru/file/pdf/817.pdf.

Рецензент: Ірина Лисицька, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.
E-mail: lisitska@karazin.ua

Надійшло: Серпень 2016.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkoi@iit.kharkov.ua
Марина Єсіна, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rinayes20@gmail.com
Наталія Ковальова, студентка (магістр), Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: natalikovalevaa@gmail.com

Методи та результати порівняльного аналізу електронних підписів з додатком та з відновленням повідомлення.

Анотація. У статті розглянуто методи порівняльного аналізу властивостей механізмів електронного підпису. Досліджено та проаналізовано існуючі методи порівняльного аналізу електронних підписів на основі методів експертних оцінок – метод аналізу ієрархій та варіації методу визначення вагових коефіцієнтів. Наведено певні критерії та показники, що можуть бути використані при порівняльному аналізі властивостей механізмів електронних підписів. Проведено порівняльний аналіз існуючих перспективних механізмів електронних підписів згідно стандартів ДСТУ ISO/IEC 14888-3:2014 та ДСТУ ISO/IEC 9796-3. Наведено результати проведеного оцінювання механізмів електронного підпису. Зроблено висновки та надано рекомендації із застосування методів оцінки визначених алгоритмів електронних підписів.

Ключові слова: аналіз механізмів ЕП, вагові коефіцієнти, електронний підпис, критерій оцінки ЕП, методи порівняльного аналізу ЕП, реалізація та застосування ЕП.

Рецензент: Ирина Лисицкая, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: lisitska@karazin.ua

Поступила: Август 2016.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Марина Есина, аспирантка, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rinayes20@gmail.com

Наталья Ковалёва, студентка (магистр), Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: natalikovalevaa@gmail.com

Методы и результаты сравнительного анализа электронных подписей с дополнением и с восстановлением сообщений.

Аннотация. В статье рассмотрены методы сравнительного анализа свойств механизмов электронной подписи. Исследованы и проанализированы существующие методы сравнительного анализа электронных подписей на основе методов экспертных оценок – метод анализа иерархий и вариации метода определения весовых коэффициентов. Приведены некоторые критерии и показатели, которые могут быть использованы при сравнительном анализе свойств механизмов электронных подписей. Проведено сравнительный анализ существующих перспективных механизмов электронных подписей согласно стандартам ДСТУ ISO/IEC 14888-3:2014 и ДСТУ ISO/IEC 9796-3. Приведено результаты проведенного оценивания механизмов электронной подписи. Сделаны выводы и предоставлены рекомендации по применению методов оценки определенных алгоритмов электронных подписей.

Ключевые слова: анализ механизмов ЭП, весовые коэффициенты, электронная подпись, критерий оценки ЭП, методы сравнительного анализа ЭП, реализация и использование ЭП.