CRYPTOGRAPHICALLY SECURE MULTIPLE CRITERIA OPTIMAL DECISION-MAKING SYSTEM

Bogdan Księżopolski[1], Zbigniew Kotulski[2]
[1]Institute of Physics, M. Curie-Skłodowska University,
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
e-mail:bogdan@kft.umcs.lublin.pl
[2]Institute of Telecommunications of WUT
ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
and Institute of Fundamental Technological Research of PAS
ul. Świętokrzyska 21, 00-049 Warsaw, Poland
e-mail:zkotulsk@ippt.gov.pl

ABSTRACT

In this work we present the multiple criteria optimal decision-making system (protocol) that guarantees the cryptographic safety of the whole process, and, in particular, the confidentiality and foreseeable realization.

With solving multiple criteria questions, it is worth to pay attention on determination of several key parameters. First of them is function of the criterion, which defines criteria space. In described case such a function is generated dynamically, and in dependence on earlier determined admissible solutions and from received preliminary solutions. The essential element of the system is qualification of report of dominance, which lets to describe criteria space. The relations of dominance are set partly in a moment of formulating the problem and in the moment of finding a part of its solutions.

In the described case we used cryptographic modules, thanks to which confidentiality, integrity as well as non-repudiation of the transmitted information are kept. The mentioned level of protection of information is obtained, mainly, by using the digital signature, hybrid cryptographic systems, and secure threshold schemes of secret sharing. Thanks to use cryptographic methods, the system can function as an element of larger architecture, with simultaneous keeping the safety requirements.

1. INTRODUCTION

In data communications technologies used in different fields of life, the information is the main resource of whole process. (We can say that it is a critical resource.) The amount of the transmitted information is so large, that one should classify it, in order to separate the most important from that of lower importance. Taking care about suitable management of the information processes, one should pay attention to those components of the process that are the most important for a given operation. To essential elements of all data communications processes are, for example: exchange of information, optimizations of the process and information security. Among services where the mentioned key elements are especially important, it is worthy to show new information services called "e-everything”, that is: e-government, e-commerce, e-banking, e-democracy.

It this paper we present the proposition of the secure decision support system, which pays special attention on protection of information exchanged in the process. Cryptographic modules, as well as different mechanisms of safety were used to guarantee the security of the system. Moreover, the information used within the system to make a decision is automatically optimized according to dynamically changing multiple criteria rules.

2. MODEL OF DECISION-MAKING PROCESS

Processes exchanging information by electronic way are based on communication models (protocols), which guarantee the correctness of the whole process. The choice of the protocol depends on a kind of the process. For example, they will be differences in a case of realization of "e-voting” [1] and "e-auction” [2]. The described model of decision support system can be used in a large class of protocols as a sub-protocol being some integral part of it.

The general sub-protocol of exchange of information consists of three steps (Figure 1). First of them is responsible for delivering input data (I_n) to the system of the decision support. These data should possess suitable, earlier definite format, consistent with the process using the data. The format of the data is also dependent on telecommunication standards that are defined by international organizations: IEEE, ETSI.

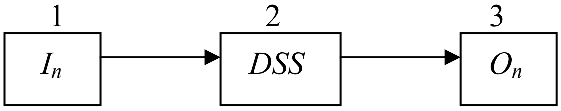

Figure 1. Model of exchange of information

In second step information is passed to the decision support system (*DSS*), which additionally should fulfill features of third trustworthy person (*TTP*). In data communications systems the existence of third trustworthy party who is not interested in the result of the process can widely extend possibilities of the system and strongly improve its security by adding new services, e.g. non-repudiation with the arbiter.

The data being transformed in the system are processed and optimized according to well-defined rules constrained by some immediate parameters delivered earlier to the system.

In the last step, the optimized and processed data are passed to the output system (O_n). During this operation one should also pay attention to the used practical data communications standards.

3. PROTECTION OF INFORMATION

The information being transmitted can be the object of different abuses and network attacks. Their degree as well as intensity is strongly correlated with the kind of information used in the information process. Another factor taking effect on the character of possible attacks is the availability of a certain service in the network. The easier attempt to the service, the greater risk of an attack. Nowadays the Internet is widespread in the world so it can be assumed that this way large amount the information will be exchanged. Thus, the fundamental assumption of our model of secure decision support system is that the system can undergo all possible attacks observed in the open network.

The presented system, since we apply specific cryptographic modules, can assure any level of protection of information. We can take care on *data integrity* (the information will be exchanged without any errors or changes). We can guarantee *confidentiality of data* (the information can be transmitted in a secret way; the possibility of reading the information is restricted only to authorized persons) and also *anonymity of sender and recipient* (the information can be sent in a way which will not discover sender's or recipient's identity). Finally, the transmitted information can be made *undeniable* (the sender and the recipient will not have a possibility to negate the fact that they sent or received the information, or made some operation on the data in frames of the protocol) as well as *authorized* (only the authorized parties can send and receive messages and they can sign data and verify signatures to confirm and check their rights in the process). In high security protocols one can introduce the *notarization* service to have confirmation of operations and processes by some trustworthy third party. Cryptographic protocols that guarantee the above services of protection of information apply the usual cryptographic functions and algorithms, e.g.: the digital signature, the symmetric and asymmetric encryption and decryption, the secure secret share schemes, cryptographic hash functions and generators of random numbers used as randomizers.

In the analyzed model it is assumed that the security of the input information of the decision support system is critical and it should fulfill the top-level criteria of safety. Thus, the information has to be transmitted in integral, secret, anonymous, and undeniable way. Additionally, we assume the correct authorization of the parties of the protocol. For the sake of clarity we assume that the anonymity and reauthorization of the information leaving the protocol is not required.

It is worthy to mention that, in general case, the problem of safety is very complicated. The high-level protection of information depends not only on the safe exchange of information but also on the safety of the whole data communications infrastructure.

Now we present in details the steps of the protocol of Secure Decision Support System.

3.1. Step 1

In Step 1 suitably formatted information is delivered to the decision support system. The system we analyze is the sub-protocol that is a part of some main cryptographic protocol. This fact is essential because one should accept certain assumptions that are necessary to have mechanisms of information protection. Thus, we do not describe details of cryptographic operations used to deliver keys for asymmetric algorithms, share and reconstruct secrets, etc. We assume these operations are realized by the main protocol.

We assume that each person taking part in the main protocol possesses a valid pair of keys: the private key (*SK*) and the public key (*PK*) for asymmetric cryptosystem (used for digital signing documents). Figure 2 shows the diagram of information sent to the third trustworthy party. All information is encrypted by the public key of trustworthy third party PK_{DSS},. Thanks to that we get the *confidentiality* of the transmitted information.

$$\boldsymbol{I_n} \xrightarrow{\{\, m_{np}\ \{m_{ns},\{F_{m_n}\}_{SK_n}\}_{PK_O}\}_{PK_{DSS}}} \boldsymbol{DSS}$$

Figure 2. Transport of the input data.

The input data are m_{np}, m_{ns}, where n is the number of the information sent, p is the public part, s is the secret part. The function F_{m_n} is the secure cryptographic hash function of the input individual data m_n (where $m_n = m_{np} \,||\, m_{ns}$) thanks to it, it is possible to check *integrity* of the information sent. The result of the hash function is signed digitally by the secret key SK_n of the sender of the protocol input data m_n. Thus, due to the digital signature we obtain the non-repudiation of the data. The signed input data are encrypted digitally with the public key of concrete operation[1] PK_O. Such an encrypted message can be decrypted by the private key of the concrete operation SK_O. This secret key can be shown (presented to the parties interested in the content of the message) at any time, in dependence on concrete realized service. The confidentiality of the secret key of the operation can be realized by means of any secure secret sharing scheme, preferably automatic one [3]. Due to encryption with the public key of the given operation PK_O we get the *secrecy (confidentiality)* of the data. The authorization of the parties taking part in the process can be executed in the initial phase of the main protocol. Its correctness is confirmed on the ground of the possession of suitably, valid pair of public and private (secret) keys (*PK*, *SK*, respectively, with the certificates, if required).

Remark 1.

Decryption of the secret massage is possible only if the sufficient number of parts of the shared secret key is collected at a recombining place. If the shares are distributed over parties interested in the result of the protocol, the recombination is possible only if the parties cooperate to finalize the protocol.

Remark 2.

The structure of the transmitted data can be richer than that presented at Figure 2. The secret part can contain several independently encrypted pieces of information. If the decision-making process has several steps, every piece of information can be decrypted at different step of the process, with cooperation of different group of parties of the protocol. This way, it is possible to make the system can satisfy certain legal requirements, e.g., publication of the results in e-voting in presence of all participants of the election or concurrent opening of all offers in e-auction.

[1] The encryption by asymmetric algorithm, in the practical case of large data set denotes in fact the hybrid method of encryption, where the complete data set is encrypted by some symmetric algorithm, but the secret key of the symmetric cipher is encrypted by the asymmetric one with the pair of keys PK_O, SK_O.

Remark 3.

In the considered example the input data consists of two parts, secret and public. Thanks to that, it is possible to obtain the anonymity of part of the data. The described possibility is important when the part of input data should be used in some pre-calculations. That operation makes that we lose confidentiality of part of data but we obtain anonymity of the parties sides participating in the protocol. Such a protocol can be used, for example, in e-auction, where the preliminary conditions of e-auction can be modified (optimized) without reveal the identity of e-auction participants, what is indispensable from the legal reasons.

3.2. Step 2

The second step is responsible for optimizations as well as suitable processing the information. At this step we do not care about external threats because the information is being processed inside some secure system (TTP). Now, the essential element of the security of the decision support system is the security of TTP being the critical element of the whole data communications infrastructure [9]. In spite of the fact that this problem is very complicated, the appropriate level of security can be obtained by application of norms proposed by international organizations [4, 5] and by the specific structure of the data delivered to the system (see Remark 2).

3.3. Step 3

For the third step, the foundation of safety consists in the integrality and non-repudiation of decision support system output information. On Figure 3 we present the model of the output data sent to the final recipient.

$$\boldsymbol{DSS} \xrightarrow{\{\{m_{x(out)}, F_{m_{x(out)}}\}_{SK_{DSS}}\}_{PK_X}} \boldsymbol{O_n}$$

Figure 3. Transport of the output data

The output information $m_{x(out)}$ can be sent to different parties of the protocol, in dependence on a concrete service. In the presented diagram the recipient will be x. The data $m_{x(out)}$ along with their calculated value of the secure cryptographic hash function $Fm_{x_{(out)}}$ (integrity) are signed digitally by the third trustworthy party (SK_{DSS}) to confirm authenticity of the information and make it undeniable. The whole information is encrypted by the public key (PK_X) of the final recipient to have confidentiality of the transmission of the result of the process[2].

4. DECISION-MAKING SYSTEMS

For the model presented, it is possible to apply different systems of decision support [10]. In this paper we concentrate on multiple criteria optimization problems where the solutions depend on several factors. The methods of finding optimal solution in such problems can be classified according to mathematical approaches applied both in formulating the problem and solving it (see, e.g., [8,11]). Now we mention the most popular approaches.

The first one is based on creating one overall quality measure for the solution (taking into account all the criteria) and then solving the problem according to such an universal indicator of quality [12].

Another concept is based on formulating special set of admissible solutions with some hierarchic structure according to each criterion [13].

The next approach bases its mechanism on creating so called relation of dominance in the set of vector-valued functions of criteria from which the best solutions are chosen (Pareto optimality) [14].

The most suitable (for our purposes) technique of the analysis of multiple criteria decision problems seems to be the Goal Programming [6], based in fact on the concepts mentioned in the above. Now we present the outline of the decision-support system based on the Goal Programming with some additional options.

The initial step in system of decision support based on the Goal Programming is determination of the admissible solutions x in whole space of solutions Q. The next step is creation of the objective function f_i, which valuates individual admissible solutions. In the Goal Programming the basic controlling

[2] As usually, for long data set we use hybrid encryption system.

factors are the reference (aspiration) levels a_i. On the basis of the deviations the values of the admissible solutions are estimated.

In presented approach the objective functions are divided into two subgroups, each in one of two possible preferences: the maximizing group f_{max} and the minimizing group f_{min}. The composition of both subgroups gives the whole main group F_i of criteria, where i is the index of the main group and n is the number of main groups.

$$F_i = f_{\max} + f_{\min}, \quad i \in (1, n)$$
$$for\ i \in Z \quad and\ n < \infty$$

The full (global) objective function is the sum of the main groups

$$F = \sum_{i=1}^{n} L_i F_i \ .$$

The parameter L_i is the coefficient assigned to every individual main group F_i, i=1,2,…,n, which defines its contribution to the global objective function.

For individual subgroups of objective function, the levels of deviations d_i are calculated; then they are expressed as the weighted norms. Such calculations are performed only if $a_i \neq f_i(x)$; otherwise we assume d_i=0. The expressions for the levels of deviation are:

for f_{max}:

$$d_i = \frac{a_i - f_i(x)}{a_i};$$

for f_{min}:

$$d_i = \frac{f_i(x) - a_i}{a_i}.$$

In the above calculation of the levels of deviation the most important element is determination of the minimum and maximum values of the levels. Such an operation should not give too high values of individual deviations, what could negatively effect on the final optimization.

The next step of the process is the determination of the aggregation function $g(d)$, which is the global measure of deviation. The aggregation function is defined as the sum of weighted deviations:

$$g(d) = \sum_{i=1}^{m} \omega_{ik} d_i \ ,$$
$$m < \infty,\ k \in (0{,}100)\ and\ k \in Z,$$

where:

m is the number of solutions,

k is the priority of optimization.

The weights are defined for individual objective functions. Every weight has also the priority of optimization k assigned.

Having appointed the aggregation functions for individual solutions, we optimize the reference levels. In the whole process of optimization only these solutions are important that take positive value of the global objective function F. If in the set of solutions none of them reach the positive value the global objective function, then the problem has no solution.

The important element of the primary optimization is the creation the optimum reference levels. The correction of the reference levels strongly depends on the priority of optimization k. Fixing the weights for individual objective functions, we also fix their priority. Thanks to this parameter it is possible to decide which of the objective functions we want to optimize and which of them cannot be changed. If for the primary optimization we fix the priority to be k = 100 (maximum), than all the reference coefficients with the weights smaller than this number will be optimized.

The primary optimization is performed according to the following formulae:

$$D_i = \sum_{i=1}^{n1} \sum_{a=1}^{n2} \frac{d_i^a}{a} \qquad for\ f_i = f_{\min}$$ [3]

$$D_i = \sum_{i=1}^{n1} \sum_{a=1}^{n2} - \frac{d_i^a}{a} \qquad for\ f_i = f_{\max}$$

We calculate there the coefficient of optimization, which will used for the modification of the certain reference levels.

[3] i is the optimized reference coefficient for the *i-th* objective function, with an appropriate priority;
a is the solution corresponding to some positive aggregation function;
n1 - the number of solutions which have positive aggregation of function;
n2 – the number of objective function;
D_i is the coefficient of optimization.

Last step of primary optimization is the correction of the original (initially calculated) reference levels

$$a_i^N = \sum_{i=1}^{n} \left(D_i a_i \right) + a_i$$ [4]

Now, the new reference coefficients for the concrete objective functions replace the initial values of the coefficients. The coefficients which priorities did not permit the optimization remain unchanged.

After realizing the whole procedure of modification of the reference levels, the levels of deviations of the optimized reference levels are again analyzed according to the principles described in the above. After obtaining the levels of deviations, the aggregation function is calculated for individual solutions. The last step of the described system is the final decision of finding the maximum value of the objective function.

5. EXAMPLE

In the previous section we described the decision-support system which (even in its clear version) could have wide area of applicability. To show its applicability in the secure version we start from the presentation a numerical example of optimization. In the further consideration we deal with the problem of electronic auction being a component of the electronic office. The object of the auction is the computer equipment. The conditions of auction are simplified to reduce calculations and present the idea of the problem. In order to show the obtained results, the e-auction is shown in two variants: the optimum (complete optimization) and the suboptimum (without optimization of the reference coefficients).

The total objective function consists of two main groups. The first one is responsible for the conditions of auction (F_1) and second for object of auction (F_2). Presenting the individual objective functions, one should mark whether he is interested in minimum or maximum value.

The main element for logical correctness of results is selecting suitable weight coefficients for the individual objective functions. The additional parameter L is the coefficient for the main objective functions which defines their contribution to the global objective function. In the considered case, for the main function F_1 we have $L_1 = 2$ and for F_2, $L_2 = 1$.

The initial parameters of the optimization problem are:

The conditions of the auction, F_1:

1. The prize,
2. The guarantee period,
3. The time of delivery.

The object of the auction, F_2:

1. The size of RAM,
2. The speed of CPU,
3. The memory of a graphic card.

The assigning the objective function with the weights, priorities as well as reference coefficients:

F_1:

The prize: $f_{1(max)}$, $\omega_{1,10} = 90\%$,
$a_1 = 5000$ PLN,
The guarantee period: $f_{2(min)}$, $\omega_{2,30} = 8\%$,
$a_2 = 24$ months,
The time of delivery: $f_{3(max)}$, $\omega_{3,50} = 2\%$,
$a_3 = 14$ days

F_2:

The size of RAM: $f_{1(min)}$, $\omega_{1,100} = 40\ \%$,
$a_1 = 256$ MB
The speed of CPU: $f_{2(min)}$, $\omega_{2,10} = 50\ \%$,
$a_2 = 2000$ MHz
The memory of a graphic card: $f_{3(min)}$,
$\omega_{1,70} = 10\%$, $a_3 = 64$MB

On the entry of the decision support system, the concrete data with a suitable formatting should be delivered. In the considered example, we assume that information has already reached the system. The immediate data is shown in the Table 1:

	1	2	3
	F_1		
f_1	4980	5200	4450
f_2	24	36	24
f_3	7	3	10
	F_2		
f_1	256	256	256
f_2	2200	2500	1800
f_3	64	64	64

Table 1. Example input data

[4] i is the index of i-th objective function;
n – the number of objective function;
N is the marker of the new reference coefficient.

5.1. Suboptimal Solution

The suboptimal solution is obtained if we choose the best offer for the fixed values of the reference coefficients of the individual objective functions. Such a solution will be realized when the priority of the optimization will be equal 0 (k=0). Below we present the numerical results for the three cases considered (Table 2):

	1	2	3
F_1:f_1:**d**[5]	0,004[6]	-0,04	0,11
F_1:f_2:**d**	0	0,5	0
F_1:f_3:**d**	0,5	0,785714	0,285714
F_2:f_1:**d**	0	0	0
F_2:f_2:**d**	0,1	0,25	-0,1
F_2:f_3:**d**	0	0	0
g(d)	**0,0772**[7]	**0,164429**	**0,159429**

Table 2. Results of the Example 1

From the Table 2 we see that second solution is the best one because its objective function takes the highest value.

5.2. Optimum solution

The optimum solution depends on the option of optimization of the reference coefficients. It is possible to control the level of optimization with the help of priority, in the analyzed case we will choose the maximum level of optimization, that is *k*= 100.

F_1		
D_1; $\mathbf{a_1}^{N}$[8]	-0,02467[9]	**4876,667**[10]
D_2; $\mathbf{a_2}^{N}$	0,166667	**28**
D_3; $\mathbf{a_3}^{N}$	-0,52381	**6,666667**
F_2		
D_1; $\mathbf{a_1}^{N}$	0	**256**
D_2; $\mathbf{a_2}^{N}$	0,083333	**2166,667**
D_3; $\mathbf{a_3}^{N}$	0	**64**

Table 3. Results of the Example 2

The next step is the execution the renewed process of evaluation of the objective function, this time together with optimized reference coefficients. Its results are shown in Table 4:

	1	2	3
F_1:f_1:**d**	-0,02119	-0,0663	0,087491
F_1:f_2:**d**	-0,14286	0,285714	-0,14286
F_1:f_3:**d**	-0,05	0,55	-0,5
F_2:f_1:**d**	0	0	0
F_2:f_2:**d**	0,015385	0,153846	-0,16923
F_2:f_3:**d**	0	0	0
g(d)	**-0,05531**	**0,025294**	**0,030012**

Table 4. The results for the optimized reference coefficients.

The results obtained in the earlier optimization of coefficients are different from those represented in the previous (suboptimal) case. The highest value of the aggregation function was reached by the third proposition and this solution is the optimum one. Analyzing the obtained results it is possible to notice, that the first solution, which have taken the positive value of the function without optimization, after optimization gave the negative value, what confirms the fact of optimizing the obtained results. The results calculated by two remaining solutions also reduced their value, what is another confirmation of their optimization.

The presented example is very simple if we consider it as an optimization problem. If we consider it as a case of electronic auction, by solving this problem one should pay attention on legal restrictions connected with the norms of state law regulations. For example, the originally assumed conditions of the auction cannot be changed after the auction is announced (opened). In our model, during optimization process the weights do not change, however reference coefficients of the individual objective functions change. Thus, also realizing the e-auction we observe that the mentioned reference coefficients cannot change. That is why in this case we consider the process of optimization as preliminary and in the moment of obtaining of optimized results we can fix the final conditions of e-auction.

[5] Fx – the main group which defines the contribution to the global objective function;
fx – the subgroup of objective function;
d – the level of deviation;
g(d) – the aggregation function.

[6] The level of deviation -(d).

[7] The aggregation function -g(d).

[8] Dx – the coefficient of optimization;
a_x^N -the new (optimal) reference of coefficient.

[9] The coefficient of optimization -(D).

[10] The new (optimal) reference of the coefficient

5.3. Data format

The input information should possess suitable structure. In the described example of electronic auction, the input data can be divided into two parts.

The first part (the message header) contains information concerning identities of the party participating in the e-auction process. These data need not be secret and anonymous because, by assumption, only authorized persons can take part in the electronic auction.

The second part of the message (the main part) contains the input data of the decision support system. These data should be formatted in a suitable way. An example of such data for the problem considered in this paper is given in Table 1. Obviously, for more complex processes the data format is much more complicated (see Remark 2).

The second part of massage should be sent in the secret way as well as anonymously. Here we can apply more security services. We can get confidentiality thanks to suitable cryptographic modules contained in an appropriate cryptographic protocol [2].

Anonymity of the second part of the information block can be achieved by application of adequate cryptographic modules, e.g., the secure secret sharing scheme [3]. The applied cryptographic methods can be supported by additional non-cryptographic methods. It is possible to get the anonymity of message using the systems based on architecture of proxy server [7]. Using the intermediary element during the transport of information it is possible to hide every information about customer before the target server.

6. APPLICATIONS

The presented system of decision support can be used to services, in which the information is transmitted electronically. Additional advantage of the system is the guarantee of the protection of information sent, suitable in a certain case. System can be used for planning of deliveries of supply, keeping simultaneously anonymity as well as confidentiality of data, which analysis can deliver classified information.

Described system, can be also used to optimal control systems, in which the sent information is gathered with many measuring points as well as their exchange has to be conducted in a safe way.

Another possibility of the use of safe model of decision support can be the analysis of effectiveness and development of organization which parameters can be gathered in safe way from many measuring places.

The discussed model can be used everywhere where the exchanged information is main supply for process and mechanisms of their protection should be used. The trump card of the system of decision support is a possibility of creation of the automatic mechanisms, which can in a simple way conduct the whole process of optimization, without interference by additional parties.

Acknowledgement

This work was partially supported by the grant from the State Committee for Scientific Research No: 2 P03D 016 25.

BIBLIOGRAPHY

[1] L. Barlow, „A Discussion of Cryptographic Protocols for Electronic Voting"; 2003.

[2] B. Księżopolski, Z. Kotulski, "Cryptographic protocol for electronic auctions with extended requirements"; Annales UMCS, Informatica; 2004.

[3] K. Kulesza, Z. Kotulski, "On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme", in: J. Sołdek, L. Drobiazgiewicz, [ed.], Artificial Intelligence and Security in Computing Systems, Kluwer 2003, pp. 281-292. ISBN: 1-4020-7396-8.

[4] ISO/IEC 17799: Information technology, Code of practice for information security management. 2000-12-01.

[5] ISO/IEC 2689: Information technology – Security techniques – Specification of TTP Services to support the Application of Digital Signatures. 200-10-18.

[6] W. Ogryczak, Linear and Discrete Multiple Criteria Optimization, Warsaw University Edition, Warsaw 1997.

[7] The Anonymizer, http://www.anonymizer.com

[8] A. Ameljańczyk, “Multiple Criteria Optimization in Control and Management Problems”, Polish Academy of Sciences Edition, Warsaw 1984.

[9] B. Księżopolski, Z. Kotulski, “Security of e-Government. Center of Certification.” In: “Actual Problems of the Real-Time Systems”, WN-T, Warsaw 2004, pp. 349-360, ISBN 83-204-3023-2.

[10] M.M. Kostreva, W. Ogryczak, A. Wierzbicki, „Equitable Aggregations and Multiple Criteria Analysis,” European Journal of Operational Research, 158 (2004), 362-377.

[11] A. Ameljańczyk, “Multiple-Criteria Optimization”, WAT, Warsaw 1986.

[12] C. Romero, „Handbook of Critical Issue In Goal Programming”, Pergamon Press, Oxford.

[13] A. Ameljańczyk, “The Game Theory”, WAT, Warsaw 1978.

[14] R. Kulikowski, „The Control in Large-Scale Systems”, Polish Scientific Edition, Warsaw 1970.