Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032

Algorithm of Combined Method for Symbol Encoding In Virtual Private Networks (VPN)

Otar Shonia*
Tinatin Kaishauri*
Ioseb Kartvelishvili*
Luka Shonia*
Zebur Beridze**
Ibraim Didmanidze**

Abstract

The work represents algorithm of combined method for symbol encoding in virtual private networks, which is given in the separate algorithm blocks. Each of these blocks is provided for the accomplishment of certain automatized safety function and is characterized with its functional significance.

Keywords: Virtual private networks; encoding; safety function; identification.

Introduction

Information technologies play decisive role in efficient operation and management of any company. When information – technological, HR, marketing or financial – is readily available, current situation can be properly assessed and timely decision can be made. Besides, information shall be available only for those for whom it is intended and inaccessible for other people. After various companies and organizations started active use of computers in different spheres of their activities, the demand of connecting these computers to one common network emerged for the purpose of fast data transfer and efficient interaction. Besides, this connection had to be reliable and secured. For efficient fight against network attacks and ensuring of opportunity of active and safe application in business or banking sphere, the concept of construction of VPN (Virtual Private Networks) was created in the beginning of 1990, which actively develops.

The word „virtual" is included in the term „VPN" in order to stress the circumstance that the connection between two stations shall be considered as temporary connection, as it is not a permanent (steady) connection and exists only in the case of transfer of information currents in open network.

Technical realization of virtual private tunnels and networks historically proceeded in two directions:

- through application of built-in mechanisms in organization of virtual channels, by construction of integration of connection between the two points of common infrastructure of the network (frame relay), which is isolated from other users;

- through application of tunnel creation technology by construction of virtual IP tunnel between the two points of common infrastructure of the network, where each IP-package is deciphered and moved to the data field of new package of special type.

The first modern network technology for creation of virtual private network was frame relay service. The mentioned network simplifies creation of connections, as only connection of the station with provider is required for working. And the routers direct the data to the required address by themselves, besides its application is much cheaper. But frame relay network did not meet the requirements of mobile users and organizations had to use modem connection, which does not allow increasing of demands of mobile connections. Consequently, it was necessary to make common decision, which would ensure not only security of corporate traffic but flexibility of connection and disconnection.

After appearance of network services active use of Virtual Private (protected) Networks (VPN) has become possible; it's based on the Internet. Such solution proved to be much cheaper as compared with previous solutions. It is then possible to actively enjoy one of the basic merits of the Internet – easy access. So each person could establish a contact with bank or various companies through the Internet connection from anywhere in the world. Although, following the openness of Internet data, the data transferred through the Internet are accessible for everybody for the

* *Faculty of Informatics and Control Systems Georgian Technical University Tbilisi, Georgia, E-mail: o.shonia@gtu.ge*
** *Faculty of Computer Technologies Batumi Shota Rustaveli State University Batumi, Georgia*

Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032

purpose of reading and modification. So, Internet-based VPN networks have the means for protection of information transferred between VPN-points. For this very reason the given networks, usually, are referred to as Virtual Private (protected) Networks – VPN, i.e. in this contest "Private" shall be understood as "private" as well as "protected".

Internet-based VPN is based on two main technologies. Primarily, this is tunneling, which allows creation of virtual tunnels; secondly, this is different methods of ensuring of confidentiality and integrity of transferred information as well as authentication and authorization of the user. Authentication is the proof of authenticity, procedure of verification of the subject and its conformity by means of unique information, in the simplest case – by means of the user name and password. Authorization is the process of verification of the required parameters, as well as the result of the process and granting of certain authorities to the person or group of persons (right of access) for performance of some actions in various systems of limited accessibility. Soon VPN technology got closely involved in cryptographic methods of protection of information and the direction of creation of Virtually Protected Networks – VPN became one of the basic priorities.

Cryptography – is a scientific-technical sphere, ensuring scrambling (securing) of information. Its main task is to solve 4 basic problems: ciphering- deciphering of information (ciphering – transformation of data (information), basically through mathematical device, into unreadable form by means of ciphering-deciphering key), i.e. security- confidentiality, authentication, integrity and control of relations of the participants (users). Cryptography is the part of mathematical technique, related to storage of information data, protected from assailants. E.g. cryptographic mechanisms were elaborated for maintenance of data confidentiality. Cryptographic mechanisms were developed the way that the information, transferred through the ether (e.g. through wireless system) is ciphered and the assailants cannot interpret it, although they can obtain ciphered data with the purpose of obtaining of the transferred data. Cryptography can be also used for making sure that the data was created by the subject who has made a statement on its creation. This parameter is also referred to as data authentication.

The concept of construction of Virtual Private Networks (VPN) is based on quite simple idea: if there are two stations in global network, which want to exchange information, construction of virtually protected tunnel is necessary between these two stations for the purpose of ensuring of confidentiality and integrity of the transferred information. Accessibility to this network shall be complicated for all possible active and passive outside observers. VPN network allows connection of central office, branch offices, offices of business partners, remote users through VPN tunnels and safe exchange of information through the Internet. VPN tunnel represents connection, established in open network, through which cryptographically secured information packages of notifications of virtual network are transferred.

Presently the technologies of construction of Virtual Private Networks (VPN) attract more attention from the side of large companies (banks, departments, large governmental structures, etc.). The mentioned interest is caused by the circumstance that VPN technologies really allow such companies not only to significantly cut the expenses allocated for communication with remote sub-divisions (branch- offices) but to raise confidentiality of information exchange. VPN technologies allow organizing of secured tunnels between the offices of the company as well as between individual work stations and servers. Besides, is doesn't matter which Internet provider connects to the secured resources to specific workstation. Everything which an outside observer will see is usual flow of IP-packages with unrecognizable content. Traditional method of connection of Internet users through modems or dedicated lines is being replaced by Virtual Private Networks – VPN, which allow users to contact each other freely through the Internet.

As we have already mentioned above, the technology of construction of Virtual Private Networks – VPN for creation of secured connection channel between two remote computers using global network – Internet infrastructure, is one of the most optimal variant by present. This task is very important, however reliable connection, through which confidential information can be transferred, is simply necessary in many spheres of human activities, e.g. banking, electronic commerce, etc. Consequently, Virtual Private Networks are very convenient for solving of the mentioned task and majority of people consider VPN technology one of the most powerful and convenient way of establishing connection in global network. But the matter is not as simple. Virtual Private Networks have their drawbacks and weaknesses. Technology of Virtual Private Networks is based on the use of cryptographic methods. In particular, all information, flowing in secured connection channel, is in enciphered state. So, cryptography is the basis of VPN and some additional mechanisms like user authentication, control of data integrity, etc. also act in its area. Nevertheless, cryptographic methods have weaknesses. Reliability of use of any cryptographic method is based on the algorithm of enciphering used in it; and of course, weak enciphering of data will enable deliberate criminals to easily obtain access to the desired information. Cryptographic key is used for enciphering of information and the mechanism of enciphering, the length of key are very important, because, the more complicated the enciphering mechanism is, and the longer the key is, the more difficult it will be for criminal to identify it.

Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032

All cryptographic technologies, used so far, are based on the use of matrix methods. Of course, the more complicated the mechanism of enciphering of data is, the more difficult it will be for a criminal to decipher it. But new problem also appears – the speed of data transfer. Complication of enciphering mechanism involves reduction of data transfer, the more so when the user has to work with distributed database management system. Consequently, enciphering mechanism, which will be easy to use, not related to long computation processes and, certainly, the probability of identification of which by unauthorized persons will be very low, shall be developed. The existing enciphering methods have one more problem. Mostly, enciphering key is not changeable, and if it is - rarely, which helps deliberate criminals to decipher it during certain time. So it is desirable to introduce additional parameters (coefficients) in the system, which will make the key changeable. In particular, en ciphering and deciphering key will be unique (i.e. it will never repeat) for each authorization of the user in the system and it will become impossible to break it.

Following the above-mentioned problems, combined method of enciphering of symbols is developed. Enciphering of symbols and its identification, following its properties, involves special problems, solution of which is the requirement of construction of automated system of security. Combined method of enciphering of symbols involves the following stages:

1. Disintegration of the password, entered by the user, into symbols;
2. Transformation of each symbol in ASCII (decimal) encoding and determination of their codes;
3. Determination of additional symbols by means of the obtained codes with the help of special operation according to the parameter set in the system;
4. Unification of symbols and additional symbols and their disintegration into words (creation of groups) according to the parameter set in the system;
5. For the symbols of each group, the relevant codes will be determined in ASCII (decimal) encoding;
6. With the help of special operation, numeric value of the obtained codes will be transformed into other numeric value and new unity of codes will be obtained;
7. Groups, consisting of special symbols will be received from the obtained unity of codes;
8. Enciphered information, consisting of the unity of special symbols will be obtained by unification of the received groups.

The efficiency of automatized system solution, which guarantees safety, depends on the algorithm. For the optimal solution of this problem, we divide the safety task into separate algorithms for each method. Every algorithm block should be provided for the accomplishment of certain automatized safety function. At the stage of algorithmization of the system, it is necessary to make the refinement of each algorithm block in such a way that the programming process should be possible and simplified. We also include the complex of those programs into the algorithm blocks, which sets the working process of the different parts of a computer and gives the consumers an opportunity to solve their tasks in the desirable way.

According to the algorithm of combined method for symbol encoding [1-3], a computer makes encoding, recognition of the denotation (password or words consisting of symbols) made by the consumer and accordingly the formation of the database. Let's consider the algorithm of combined method for symbol encoding (Fig.1.).

At the starting stage of work it is necessary to define whether the consumer's information is entered. At the first stage the password entered by the consumer is written in the special array, where the beginning and the ending of the word are defined. Also the division of the word into symbols occures and there is the index for each separate symbol.

Extra variables are taken into the system in order to define the indexes of symbols and extra symbols with their quantities. Then the devision of symbols in the word and definition of index for every symbol take place at the result of which we can get the word consisting of complex of symbols, where each symbol is defined by its index. Every symbol is considered through ASCII (decimal) encoding and the codes are defined for them. On that purpose there are arrays, where the beginning and ending of the symbols are defined. Then the process of code defining and their entering into the symbol code arrays occures, that gives the numbers consisting of complex of symbol codes, where the index code is defined for each symbol. Then comes the procedure of filling the word with the extra symbols with installation of certain parameters. At first the number of extra symbols should be defined, which is followed by an array, where the extra symbols are written and the beginning and ending of the word with extra symbols are defined. Then modified codes are defined for certain code of separate symbols that are written in special array, where the extra the beginning and ending of the code with extra symbols are defined.

The goal of the given method is the transferring of encodable symbols into special symbols. In the system of ASCII (decimal) encoding the symbol codes match from 32 to 126, and special symbol codes match from 128 to 255.

Transforming of symbol codes can be done in the following way: the first symbol code of the word is taken and the area of its location is checked over. If the code is between 32 and 50, the following action should be done:

Symbol code is added with its order, or index, then the second symbol code is added the second index and so on to the end of the word. If the code is located between

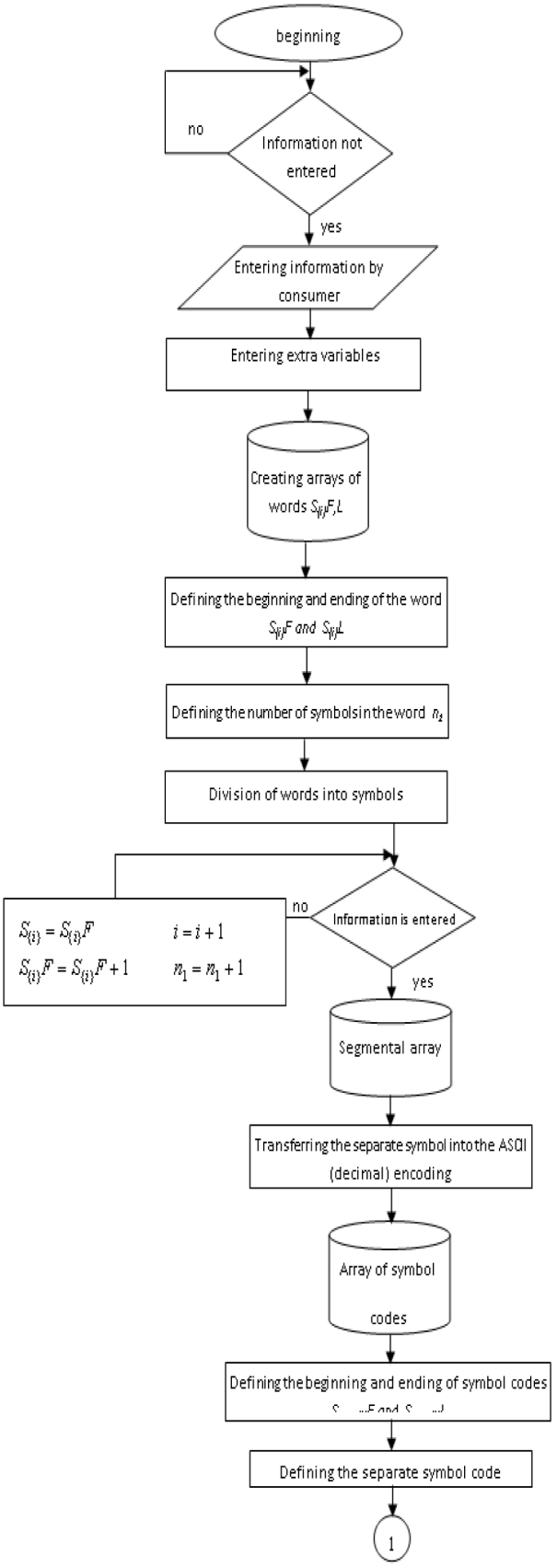
Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032

51 and 126, , the index is diminished.With the codes, got through the above mentioned activities, the groups of extra sumbols are created. This process goes on until the meaning of certain parameter is defined.The new modified code are used to create the group of extra symbols, at the result a word consisting of the complex of extra symbols is got, where every symbol has its defined index.

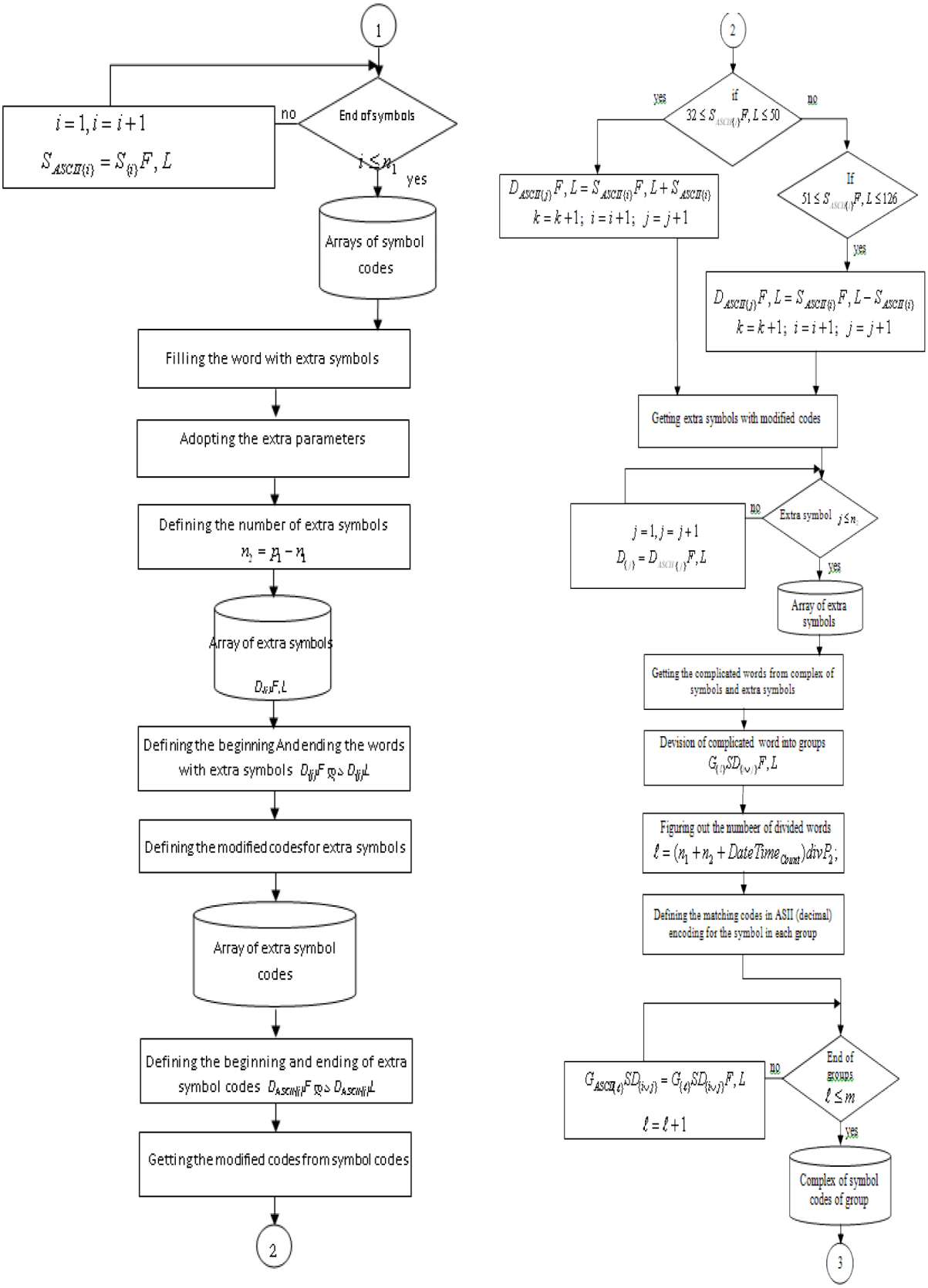
By the union of new symbols and extra symbols a „complicated“ word (password) is created, that is added with numeral meaning of current date and time.

Then the word, got through the mentioned operation is dismantled (groups are created) according to the established parameters in the system. Then for the symbols of each group their suitable codes are defined in the ASCII(decimal) encoding, at the result of which we can get the numbers consisted of the complex of symbol codes of the group, where index code for each symbol is defined. The numeral meaning of the gotten codes are transformed into other numeral meanings and the multitude of new codes is created. The transforming of the new symbol codes can be made in the following way: the first symbol code of the word is taken and the area of its location is checked over. If the code is between 32 and 99, the following action should be done: the symbol code is added with the meaning of the parameter, but if the code is between 100 and 126 the symbol code is added with the meaning of the parameter. The new modified codes are used to create the group of special symbols. By the union of the groups consisted of the special symbols an encoded information consisted of the complex of special symbols is got.

The encoded information is passed to the central server in the form of groups. If the identification of the first group is successfully accomplished, the server informs and orders to transfer the next group and so on until the last group. If any group does not match, the server blocks the consumer immediately. The decoding of the encoded information by the central server is done by means of the above considered backalgorithm using the same parameters.



Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032



Journal of Technical Science and Technologies, 1(2):15-20,2012 ISSN:2298-0032

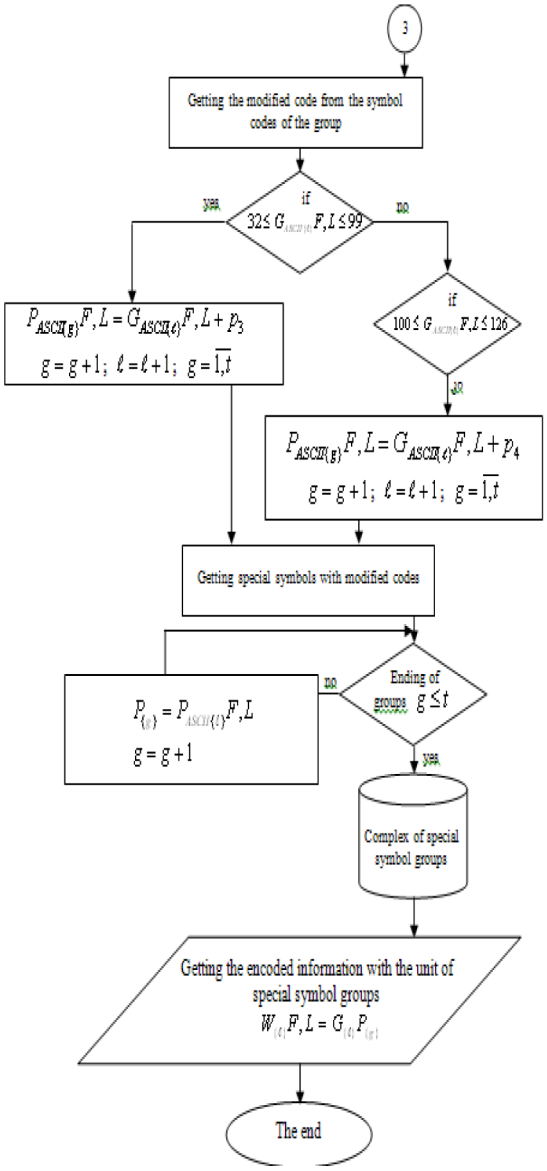


Figure1. *Algorithm of combined method for symbol encoding*

References

O. Shonia, G. Nareshelashvili, I. Kartvelishvili – „Wireless Network Safety“ Georgian Technical University, Tbilisi, 2009.

O. Shonia, I. Kartvelishvili, L. Shonia, Z. Beridze – „Combined Methods of Symbol Encoding in Virtual Private Networks (VPN) Georgian Technical University,Computer-aided systems of management 1(12), 2012.

G. Chogovadze, G. Gogichaishvili, G. Surguladze, T. Sherozia, O. Shonia – „Computer-Aided Systems of Management“ Tbilisi, 2001.