STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

Joint ECE/Eurostat Work Session on Statistical Data Confidentiality
(Skopje, The former Yugoslav Republic of Macedonia, 14-16 March 2001)

Working Paper No. 34
English and Russian

Topic IV: Progress in the implementation of SDC methods and techniques in central and eastern Europe

PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS

Contributed paper

Submitted by the State Statistical Committee of Azerbaijan[1]

1. A large amount of statistical information describing almost all spheres of activities of the country is available in the State Statistical Committee of Azerbaijan Republic. All information, which is confidential and should be closed to free access is addressed to the bodies of the state statistics, on a compulsory basis, by respondents carrying out any kind of activity within the territory of the Republic. Any respondent, in accordance with the legislation, has a right to secrecy of information of a state, commercial and private character. In the Law on Statistics adopted in 1994 there is an article 11 "Statistical secrecy" specially stipulated for this aim which says: "Primary statistical (individual) data of legal and natural persons are confidential and compose a statistical secrecy. Any intentional or imprudent transfer of information by the state bodies of statistics about legal and natural persons without their consent to state bodies, enterprises, organization or citizens, who does not have a legal access to this information, or their publication in mass media is a divulgence of information which compose a statistical secrecy". As a consequence, any information disclosure can cause a moral damage to the Statestatcom itself by respondents, expressed in distrust by respondents and the public. This also can significantly influence the reliability and completeness of collected information etc. In order to avoid consequences of the divulgence of statistical data, necessary steps are taken in state statistical agencies for the protection of information from unauthorized access. So, in accordance with the "Code of administrative offences" confirmed by the National Assembly on July 2000, the following penalties are incurred to those who are guilty of divulgence of statistical secrecy: natural persons are fined for the sum of 15-25 minimum wages, sum of fines for officials makes 35-50 minimum wages, simultaneously with divulgence of statistical information its publication in mass media by natural persons the sum of fine is 30-40 minimum wages, by officials 70-90.

2. The problems of information protection from unauthorized access are especially relevant in modern computing circles, which are complex corporate network Wide Area Network. Statistical organizations of most countries have a territorially distributed infrastructure and therefore use WAN technologies to collect, process and disseminate the statistical information. Intranet-Internet technologies are widely used, to transfer and disseminate information, access technologies to databases on-line, technologies of network information processing. As a rule, these networks have a developed means of local and remote access of a large number of subscribers to resources of the network, and in particular, to databases. Naturally, safety and confidentiality of information in such systems is one of the initial tasks. Information protection means are installed from the very beginning of the functioning of the network and are developed in parallel with its development.

3. At present in the system of Goskomstat Azerbaijan there is installed a corporate network which is developing with an accelerated rate. During 2001 this network should cover all the system of Goskomstat, including all its territorially removed subdivisions, located in administrative regions of the country. It has

[1] Prepared by A.M. Veliev and V.A. Allakhverdiev.

been planned to provide access to the resources of this network on-line of about eighty territorially removed subdivisions of Goskomstat. Additionally, access services to information will be rendered also to interested outside organizations. Tasks of the development of information technologies of statistical data processing, that are planned to be solved with WAN are the following:

- automatization of primary statistical data collection using technologies and e-mail;
- automatization of information transfer between removed and local clients inside the Goskomstat system;
- application of Network technologies of statistical information processing by means of industrial distributed databases;
- realization of modern technologies of information dissemination with the help of WEB service technologies.

4. These technologies provide an access of a wide circle of clients to programme and information resources of the network, and consequently, require the application of reliable methods of information protection from unauthorized access.

5. Measures on information protection are always connected with expenditures, which are sometimes significant. It is possible to increase protection endlessly, while spending new means each time. It is necessary to indicate with the principle of sufficiency and with those real financial possibilities, which are available. Moreover, as all countries with transition economies, we work with an acute shortage of funds.

6. Below are given effective methods of information protection, which we apply in the system of Goskomstat Azerbaijan.

Choice of the network operating system

7. Any network operating system has an installed means of protection of network resources. Difference exists only in the organization of this protection and its effectiveness. In any case, when choosing a network operation system, it is necessary to check if it is certified by class of network protection of C2 level. Network operation system Novell Net Ware 5, used by us has a rich range of such means, basic of which are given below:

- access to the network only with individual password. Information on password of users is coded and completely protected from break;
- delimitation on level of access. Network resources and attachments are classified by levels and access to them depends on the level of a user;
- setting of individual restrictions of access. An administrator may put any restriction for access of any user of any attachment;
- restrictions on time of access. The user may work only during the period allowed to him;
- fixation of working stations. This user may enter the network only form one working station;
- control of repeated entrance the network. The client may enter the network repeatedly, if he/she at present is already in network;
- restriction of user access. Restricted are actions of users on a certain operation (for example on record operation);
- restriction of access to attachments. The user may use only those attachments, to which he/she has an access.

8. Information on user rights are stored in his/her record information to which an administrator has access. Actions of the administrator are not restricted, but they are registered and may be controlled by an independent audit.

Training of serving personnel

9. Protection of information depends greatly on the level of training of personnel rendering services. This comprises the ability to assess the situation and apply to a full extent all installed means of protection in operation system. This mainly refers to personnel of network administrators.

Technical methods

10. The server, active network equipment and cable system should be given maximum protection from physical entrance. All server equipment should be located in a special place, protected from unauthorized persons access. Active network equipment must be located in the special rivers. Network outlets in the work place which are not functioning should be switched off from active equipment.

Client operating system

11. Client operating system should protect information stored at this work station. As experience has shown, password protection Windows'95 can be easily removed and the computer becomes completely accessible. It is recommended to use Windows 2000 Workstation system wherever possible.

Security actions

12. All work sites of the office, where computing technology is located should be under security during the whole non-working time. It is recommended to use electronic security systems: movement detectors, video cameras and other security means.

Protection of an electronic post

13. A significant amount of information is received and transferred within the system of the State Statistical Committee by e-mail. This mainly is:

- primary statistical information addressed by reporting organizations to bodies of statistics;
- information, transferred between remote subdivisions of SSC;
- information transferred between local and remote clients;
- statistical information transferred to interested outside organizations.

14. If the electronic mail is delivered by Internet network as a used decoded letter, then it is absolutely not protected from being read by outside people. The matter is that a copy of such a letter remains on a minimum in four computers: on the sender's, on the server of the sender's provider, at the server of the receiver's provider and at the computer of the receiver. Administrators of providers all have software means of intercepting, reading and copying this mail. Reporting to the SSC organization may even not suspect that in sending their reports, it spreads that data itself. The same can be said concerning internal agency information exchange through e-mail between remote subdivisions of Goskomstat. In order to solve the problems of e-mail using Goskomstat should ensure security of this technology.

15. It is possible to solve the problem in two ways:

- applying methods of programme coding (for example by PGP – Pretty Good Privacy method);
- installing own mail service, allowing to organize corporate mail service skirting the Internet provider. In this case the client is registered in the corporate network of State Statistical Committee, receives access to it and all the mail in two directions is transferred through the mail server of SSC.

Network data processing

16. Effective processing of statistical information is connected with the application of industrial SUBD, for example ORACLE. In the environment of this SUBD, there are developed attachments for group work with databases, located in the server. Users of the network receive an access to their own information and participate in joint work with them regardless of their own location. Protection in this case is carried out by limiting access to data between attachments by the network administrator. The attachments themselves should have a means of protection, restricting access of work executors as to information, and by circle of implemented operations as well. It is necessary to have a database administrator who would carry out necessary protection measures on data leak from the base.

Information dissemination

17. Wide access to information is carried out by access to data through WWW technology. However, in this case it is possible to have an unauthorized entrance to confidential information of the database. It is possible to ensure security by two means:

- to set up a separate database open for disseminated information and to organize access only to this from the Web page. The remaining information should not be available for Internet;
- not to use the server of the provider to store Web-pages and information. It is necessary to set up own Web server, which would contain a database able to be disseminated and would not have an access to other servers of network, responsible for storage of other information.

18. Network security systems are developing in parallel with the network itself and require constant attention and planning. In general, security of the network depends on an understanding of the importance of this problem by the management of the enterprise. The management should in a timely way solve problems of funding the security measures, purchase of required equipment, programme means and personnel training. Economy may lead to numerous financial and moral losses in future.