UDC 004.896:005

K. Balushok, PhD, M. Birouk
(Motor Sich PJSC, Ukraine)

The security system of information technologies of Motor Sich chief technologist department

The security system of information technologies of Motor Sich chief technologist department is described. Existing problems and approach for system improvement task resolving are shown.

Motor Sich PJSC is an industrial enterprise which stability, profitability and competitiveness largely depends on protection of commercially valuable information.

The information security of an enterprise assumes effective information service and management of all means of complex information protection.

There are more than 370 units of computer equipment in the department of chief technologist. More than 30 of them is ones with increased requirements for information security. In the departments network segment the following kinds of information are being processed: design, technological, test, repairing, production as well as CNC programs.

As a result of analysis of the departments security system the next problems were found:

– insufficient level of protection from unauthorized access;

– possibility of operation violation as result of uncontrolled use of in/out ports of PCs;

– insufficient level of reliability of own domain of the department

– the advanced requirements of information security insurance were not determinated for specific groups of PCs

– existing level of implementation of the information security policy had to be significantly strengthened in part of users activity control

The main purpose of efforts was construction of a computer-aided security system for ensuring of confidentiality, sustainability and accessability of the information in the department's network segment.

For achieve this goal the next tasks were resolved:

1. Technical aspect:

– construction of the server system for uniform management of PCs and user accounts;

– Domain and ActiveDirectory system construction;

– Installation of DeviceLock DLP system;

– Antivirus protection;

– providing inventory of computer hardware and software.

2. Organizational aspect:

– Familiarization of users with enterprise poly for information security and rules of PC using;

– Development of documents that establish rules for computer equipment control and verification;

As a result of work carried out, a set of technical facilities was created, including:

– Servers for unified PCs and user accounts administration with use of Active Directory;

– A server that provides backup tasks for a domain controller, as well as a specialized file server for information exchange.

– Allocation of the department's network segment to a separate VLAN with subsequent configuration of controlled access to the network of the enterprise (prohibition of the SMB protocol).

– Allocation of the department's network segment to a separate VLAN with subsequent configuration of controlled access to the network of the enterprise (prohibition of the SMB protocol).

-Applying of Device Lock system for restriction using of I / O ports, logging and accounting for printing, the shadowing of information passing through I / O ports in a group with increased security requirements.

– Applying of Anti-virus protection system (Symantec, Eset software) for a PCs with enhanced security requirements, such as: access to the Internet and LAN of the enterprise, use of authorized flash-drives.

– Applying of Inventory system for computer equipment and software management (OCS + GLPI).

The organizational support of the system includes:

– Information security policy of the enterprise, rules for using the PC;

– An order "On strengthening control over the targeted use of computer equipment";

– An order "On Ensuring the Information Security Policy".

The information security system of chief technologist department is implemented in a unified information environment of the Motor Sich PJSC. Thus, it shares data transmission channels with other enterprise information systems. All PCs are located in the domain ugt.msich.com, which is the subsidiary domain of the enterprise (msich.com).

The information exchange between the department's network segment and systems running in the enterprises network is carried out in different ways:

– transfer of electronic documents with Lotus Notes EDS;

– transfer of electronic technical documents with Search PDM;

– file exchange with the controlled file server;

– the transfer with approved flash-drives.

The level of reliability of the system's hardware and software ensures the data preservation in the case of malfunctions:

– power failure;

– network failure;

– software and hardware failures.

The system runs in authomatic mode and provides:

1. Preventing the possibility of using a PC for non-business purposes:

– Restricting the use of I / O ports according to approved roles.

– Audit of information exchange through a centralized server.

– Unable to install third-party software.

– Logging and accounting of print jobs.

2. Unified management and administration of user accounts and PCs using Active Directory:

– Users and PCs grouping by roles.

– Protecting user data by backup.

3. Improving the reliability and fault tolerance of the domain controller:

– Domain controller replication.

– Using RAID arrays for the domain controller and its replica.

– Backing up controller and its replica.

4. Ensuring the integrity, confidentiality and control of information in a group with increased security requirements:

– Obligatory shadow copying of information passing through the I / O ports.

During the trial operation of the system, several attempts of sequrity violation were found.

After clarifying the system settings and explanatory work with users, the possibility of leaking confidential information and using external devices for personal purposes was blocked.

Conclusions.

The results of IT security system implementation make it possible to draw conclusions about the correctness of the efforts for confidential information protection. Prevention of the potential leakage of protected information makes it possible to recommend the use of the system in all divisions of the enterprise.