Threat modelling for creating technical information protection system at automated machine building plants

N Y Saigushev\textsuperscript{1}, O A Vedeneeva\textsuperscript{1}, Yu B Melekhova\textsuperscript{1}, L S Ryazanova\textsuperscript{1}, M V Konovalov\textsuperscript{1}

\textsuperscript{1} Nosov Magnitogorsk State Technical University, 38 Lenina Ave., Magnitogorsk, 455000, Russia

e-mail: nikolay74rus@mail.ru

Abstract. The article addresses the issue of threat and adversary modelling for creating a technical information protection system. Due to the very fast development of information technologies now, the information security must also be taken into consideration. Information leakages can occur via different channels such as acoustic and vibro-acoustic channels, electromagnetic interferences and so on. Protection must be secured against all that. Protection is particularly required when quite important documents or methods that can constitute state secrecy are concerned.

1. Introduction
When possessing confidential information or information that contains state secrets, reliable protection of automated machine building plants against unauthorized access (UA) with regard to information security (IS) must be ensured.

Information security represents the basis of the entire complex of automated system (AS) security. It is the information security that ensures information confidentiality, integrity and availability \cite{1, 2}. IS features the lack of unacceptable risk associated with information leakage resulting from UA. Information leakages can occur via different channels such as acoustic and vibro-acoustic channels, electromagnetic interferences and so on. Protection must be secured against all that. Protection is particularly required when quite important documents or methods that can constitute state secrecy are concerned.

Therefore, apart from arranging information protection of computing tools against UA in general, it is necessary to, at least, arrange measures for reliable and safe startup of their individual components.

The following are just some of the benefits offered with the application of computing tools in organizational activities:

- possible in-process monitoring of information reliability;
- less number of potential errors when generating secondary data;
- possible immediate access to any data;
- possible fast report generation;
- saving labor and time needed for data processing.

At this moment, all the above benefits have been recognized by many organizations and, for this reason, there is a fast development process observed with specialized information systems and, therefore, AS protection is becoming more and more relevant \cite{1, 3}.
This study addresses the development of the hardware-and-software protection complex applied to the automated system of automated machine building plants, which is the duty of the information security department.

2. Non-disclosure requirements

The following conditions provided in clauses 10-13 of the Federal law of the RF must be fulfilled at automated machine building plants to ensure non-disclosure:

1. Measures related to non-disclosure of information taken by the person in possession of such information must include the following:
   - defining the list of information constituting trade secrets;
   - restricting the access to information constituting trade secrets by establishing the procedure for handling such information and monitoring the compliance with this procedure;
   - keeping records of people who have accessed information constituting trade secrets and (or) people to whom such information has been provided or communicated;
   - regulating the relations concerning the use of information constituting trade secrets by employees and counterparts pursuant to labor and civil contracts, respectively;
   - marking tangible media (documents) that contain information constituting trade secrets with the “Trade secret” crypto, specifying the person in possession of such information (full name and registered office for legal entities and full name and residential address of the person representing the individual entrepreneur for individual entrepreneurs).

2. Non-disclosure is deemed to be established once the possessor of information constituting trade secrets takes the measures specified in part 1 of this clause.

3. Individual entrepreneurs who possess information constituting trade secrets and have no employees with whom they have entered into labor agreements must take measures related to information confidentiality protection, except for items 1 and 2.

4. In addition to the measures specified in item 1, the person who is in possession of information constituting trade secrets has the right, when required, to use other tools and methods of technical protection applied to non-disclosure of such information as well as other measures, which do not conflict with the law of the Russian Federation.

5. Measures related to information confidentiality protection are recognized as reasonably sufficient given:
   - no access to information constituting trade secrets is permitted without the consent of its possessor;
   - the use of the information constituting trade secrets by employees and its communication to counterparts without any trade secret disclosure.

Developing the design of the subsystem for information protection against UA

Non-disclosure cannot be used for any purposes that conflict with requirements for protecting constitutional order foundations and other people’s morals, health, rights and legal interests as well as national defense and state security.

The design of the system for information protection against UA must be developed for the plant AS, which is created in the form of the local area network, the components of which are located within the controlled area.

All media have the same level of confidentiality. The advantages of the access to the system resources are arranged by using software means of protection against unauthorized access.
The following information services are implemented in:

- access to AS;
- access to DB;
- electronic mail;
- document printout;
- electronic document flow;
- file exchange;
- access to the Internet.

Information resources that need protection must be identified and the importance of protected information must be evaluated before implementing the AS data protection plan.

To identify information subject to protection at the plant, the following regulatory documents must be referred to:

- Federal Law on information, information technologies and information protection No. 149 d/d 27.07.2006;
- Federal Law on trade secrets No. 98 d/d 29.07.2004;
- Federal Law on personal data No. 152 d/d 27.07.2006;
- Decree of the President of the Russian Federation on approving the list of confidential information No. 188 d/d 06 March 1997

The above regulatory documents identify the following kinds of enterprise information subject to protection:

- public information – publicly available information on the staff structure and regulatory documents (charter, various provisions, etc.);
- personal data – information on managers and employees of the organization;
- professional secrets;
- trade secrets.

Complex protection of all information systems and communication channels between them must be provided. Software and hardware implementation of all servers, workstations and communication channels of the information system and other communication systems that are particularly related with information system elements must be developed to identify the required security arrangements:

- Human resources manager’s WKS
- Printer
- Human resources department’s WKS
- Switch
- Cashier’s WKS
- Security officer’s WKS
- Movie technician’s WKS
- Accountant’s WKS
- Chief accountant’s WKS
- Administrator’s WKS
- Economic security department’s WKS
- Chief superintendent’s WKS
- IT administrator’s WKS
- Security administrator’s WKS
• Duty programmer’s WKS
• PA-engineer’s WKS
• Router
• Multilayer switch
• Domain LBS-server
• Mail server
• DB-server.

Personal data represent the most critical data from the perspective of information protection. The critical level of such information is determined by the fact that its disclosure can result in significant adverse consequences for personal data subjects and implies imposition of heavy fines as well as administrative and criminal control methods on the organization [4,5,6].

Complex protection of all information systems and communication channels between them must be provided. Software and hardware implementation of all servers and communication channels of the Information system and other communication systems must be developed to identify the required security arrangements.

Automated system classification and information protection requirements are determined based on the following:

• list of protected AS resources and their confidentiality levels;
• list of people who have access to inbuilt AS tools, specifying their privilege level;
• access to subject privilege matrices in relation to protected information AS resources;
• AS data processing modes.

Based on the above documents, all users have the same levels of access (privileges) to any AS data processed and (or) stored on media of the same confidentiality level but marked with just one crypto-secret, 1B class assigned to the AS.

AS protection class definition generates a set of security requirements imposed on this system class. These requirements are described in the “Computer aids. Protection against UA. Criteria of protection against unauthorized access to information” regulatory document issued by the State committee for technical and export control. In addition, computer aids (CA) which must have the respective CA protection class are selected based on the protected AS class. The CA protection class for 1B class and maximum “confidential” level of confidentiality are not lower than the 4-th level of protection.

3. Conclusion
Based on the above listed, we determine that the 3-rd level of protection must and is sufficient to be provided at the plant for the information system, which includes the following:

• arranging for security procedures at the premises where the information system is located, which prevent the possibility of unsupervised penetration or presence of excludable people in such premises;
• ensuring the security of personal data storage media;
• certifying the document with the list of people whose access to personal data handled in the information system is required for performing their official duties (work commitments);
• using information security tools that have undergone the procedure of verifying the compliance with legal requirements applicable in the Russian Federation with regard to information security;
• appointing officials who are responsible for personal data security in the information system.
References
[1] Mikhailova U V, Saigushev N Ya, Vedeneeva O A, Tsaran A A 2018 Journal of Physics: Conference Series 1015(3) 042054
[2] Mikhailova U V, Barankova I I, Lu'y'anov G I 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) Proceedings.
[3] Ardashkin I, Martyushev N, Bezborodov V 2015 Procedia - Social and Behavioral Sciences 166 227-231
[4] Kameneva G A, Bondarenko T A 2018 Novosibirsk State Pedagogical University Bulletin 4 172-186
[5] Saigushev N Y, Vedeneeva O A, Melekhova Y B 2018 Journal of Physics: Conference Series 1015(3) 032119
[6] Savva L.I. 2015. Professional and personal formation of a university students (Ufa: Aeterna)
[7] Markelov K S, Neiman A B 2012 Wireless Security Young scientist 4 63-66
[8] Tanenbaum A 2014 Computer networks (St Petersburg: Peter)