NISSC '97 SUBMISSION

COVER PAGE

Type: PAPER

Title: "THE USE OF INFORMATION TECHNOLOGY SECURITY ASSESSMENT CRITERIA TO PROTECT SPECIALIZED COMPUTER SYSTEMS"

Abstract:

The purpose of this paper is to present a relative comparison of the information security assessment criteria used in Russia and the United States and to describe the application of the Russian criteria to a specific problem. The computer system security assessment criteria utilized by the State Technical Commission of Russia and similar criteria utilized by the U. S. Department of Defense (TCSEC) are intended for the development and implementation of proven methods for achieving a required level of information security. These criteria are utilized, first and foremost, when conducting certification assessments of general purpose systems. The Russian Federation is creating specialized systems for nuclear material control and accountancy (MC&A) within the framework of the international laboratory-to-laboratory collaboration. Depending on the conditions in which the MC&A system is intended to operate, some of the criteria and the attendant certification requirements may exceed those established or may overlap the requirements established for attestation of such systems. In this regard it is possible to modify the certification and attestation requirements depending on the conditions in which a system will operate in order to achieve the ultimate goal -- implementation of the systems in the industry.

Authors: V. A. Lykov, A. V. Shein, Russia, 127434, Moscow, PO Box 971, Atominform

A. S. Piskarev, Russia, 101000, Moscow, B. Ordynk Ulitsa 24/26, Iskra 38343, Atomzashchitinform

David M. Devaney, Ronald B. Melton, Pacific Northwest National Laboratory (PNNL), PO Box 999, Richland, WA 99352, USA

William J. Hunteman, Joan M. Prommel, Los Alamos National Laboratory (LANL), PO Box 1663, Warehouse SM3, Bikini Road, Los Alamos, NM 87545, USA

James S. Rothfuss, Lawrence Livermore National Laboratory (LLNL), PO Box 808, 7000 East Ave., Livermore, CA 94551, USA

Point of Contact: Ronald B. Melton, PNNL

tel: 509 375 2932

FAX: 509 372 4316

e-mail: ron.melton@pnl.gov

THE USE OF INFORMATION TECHNOLOGY SECURITY ASSESSMENT CRITERIA TO PROTECT SPECIALIZED COMPUTER SYSTEMS

V. A. Lykov and A. V. Shein, Russia, 127434, Moscow, PO Box 971, Atominform

A. S. Piskarev, Russia, 101000, Moscow, B. Ordynk Ulitsa 24/26, Iskra 38343, Atomzashchitinform

David M. Devaney and Ronald B. Melton, Pacific Northwest National Laboratory (PNNL), PO Box 999, Richland, WA 99352, USA

William J. Hunteman, Joan M. Prommel, Los Alamos National Laboratory (LANL), PO Box 1663, Warehouse SM3, Bikini Road, Los Alamos, NM 87545, USA

James S. Rothfuss, Lawrence Livermore National Laboratory (LLNL), PO Box 808, 7000 East Ave., Livermore, CA 94551, USA

Abstract

The purpose of this paper is to present a relative comparison of the information security assessment criteria used in Russia and the United States and to describe the application of the Russian criteria to a specific problem. The computer system security assessment criteria utilized by the State Technical Commission of Russia and similar criteria utilized by the U. S. Department of Defense (TCSEC) are intended for the development and implementation of proven methods for achieving a required level of information security. These criteria are utilized, first and foremost, when conducting certification[1] assessments of general purpose systems. The Russian Federation is creating specialized systems for nuclear material control and accountancy (MC&A) within the framework of the international laboratory-to-laboratory collaboration. Depending on the conditions in which the MC&A system is intended to operate, some of the criteria and the attendant certification requirements may exceed those established or may overlap the requirements established for attestation of such systems. In this regard it is possible to modify the certification and attestation requirements depending on the conditions in which a system will operate in order to achieve the ultimate goal -- implementation of the systems in the industry.

Introduction

This paper is an outgrowth of the activities of a joint US-Russian working group on information security certification for MC&A. Our experience has been that while we have some differences in approach that we mostly have differences in terminology. This paper shows the common understanding that we have developed. This is done first through a comparative discussion of information security assessment criteria in the two countries. The information security assessment criteria utilized by the State Technical Commission of Russia, entitled "Automated Systems. Protection Against Unauthorized Access to Information. Classification of Automated Systems and Information Security Requirements" [1] and similar criteria utilized by the U. S. Department of Defense (TCSEC) [2] are intended for the development and implementation of proven methods for achieving a required level of information security. These criteria are utilized, first and foremost, when conducting certification assessments of general purpose systems. At some level the majority of these requirements address the characteristics of secure operating systems.

The second part of this paper describes a specific application of the Russian criteria to the MC&A application domain. In this example domain specific criteria were developed. In order to allow for practical, timely, and cost-effective certification the criteria were grouped into three categories. These results illustrate the positive outcomes that are derived from joint US-Russian activities.

---

[1] A terminology difference led to misunderstandings when each side used or heard the wor
situation plagued our early cooperative work. The Russian term translated as “certifica
US term “validation”, while the Russian term translated as “attestation” best correspon
“certification”. In this document, we consistently use the Russian terminology. The

Background - Review of Security Criteria

Unlike the U. S. standard, the State Technical Commission of Russia guidance document cited above is directly focused on the operating conditions of automated systems, the most important of which are the confidentiality level of the information being processed (its level of secrecy) and the type of user need-to-know. In addition to certification requirements, this guidance document also contains requirements established for attestation of such automated systems. Attestation is the final approval to operate the system (in the U.S. it is called accreditation). This comprehensive approach makes it possible to accelerate the process of designing and implementing secure automated systems. With regard to its functional requirements, this guidance document is fairly close to the U. S. standard.

Thus, the access control subsystem in the guidance document includes requirement subsets for the conduct of a consistent security policy with regard to limiting access and managing information flows (using labels) as well as for maintaining computer system usage accounts with regard to identification and authentication of access subjects.

The information logging and accountancy subsystem in the guidance document includes requirement subsets for accounts with regard to logging and warning of (signaling) events that are important from the standpoint of information security. The information logging and accountacy subsystem also includes security policy requirement subsets to account for any created objects that require labeling (including hard copies) and erasure of freed up resources (memory and disk).

The integrity assurance subsystem in the guidance document include requirements subsets for assurance (trust requirements for generated products) with regard to ensuring the integrity, ease of administration, testing, recovery and integrability of the automated system security measures.

However, the guidance document lacks, in particular, requirements related to architecture, specifications, or design verification, and requirements related to security system documentation, as well, even though it is tacitly assumed that system documentation will be executed in compliance with the requirements of the "Unified Software Document System" and the "Unified Engineering Document System" [3, 4]. There is no clear distinction between discretionary and mandatory access control, and confidentiality label requirements have not been narrowly specified. Although not explicitly stated, the access control subsystem assumes that the normal access control will be discretionary, whereas information flow management is assumed to be mandatory access controls. Architecture and label requirements are assumed to reside in the integrity assurance subsystem.

Continuing this comparison one should also note that, unlike the guidance document, the U. S. standard completely lacks requirements with regard to encryption, which significantly enhance the security of the whole system.

Among the attestation requirements in the guidance document one should also note the requirements for information media accountancy, the use of certified security equipment, and the physical security of the computer equipment, etc.

A full listing of the requirements and comparative analysis with regard to their presence/ absence in both standards yields the information presented in Table 1.

In the column to the right of the guidance document requirement in this table, a "+" sign indicates requirements having security indexes for which there exist functionally identical or similar requirements in the U. S. standard; a "–" sign indicates guidance document requirements that are lacking in the U. S. standard. Also indicated are those protection categories correlated with the American standard and those correlated (by category groups) with the Russian Federation standard for which security system requirements have just been added for the first time.

One should also note the lexicographic order for identifying categories in the Russian Federation and American standards. In the American standard, categories increase in significance in the following order: D, C1, C2, B1, B2, B3, A1; whereas in the Russian Federation standard, the order is 3B, 3A, 2B, 2A, 1E, 1D, 1C, 1B, 1A.

Table 1

Subsystems and Requirements		RF Guidance Document	U. S. Standard
1.	Access control subsystem		
1.1	Identification, authenticity verification, and control of subject access:		
	Into the system	+3B, 2B, 1E	C1
	To terminals, computers, computer network nodes, communication links, computer peripherals	+2A, 1D	B2
	To software	+2A, 1D	C1
	To volumes, catalogs, files, records, record fields	+2A, 1D	C1
1.2	Information flow management	+2A, 1C	B1
2.	Information Logging and Accounting Subsystem		
2.1	Logging and Accounting of:		
	Entry/exit of access subjects into/out of the system (network node)	+3B, 2B, 1E	C2
	Issuing printed (graphic) output documents	+3A, 2A, 1D	B1
	Bootup/completion of programs and processes (tasks, problems)	+2A, 1D	C2
	Access subject software access to secure files, including their creation, deletion, and transmission over communication lines and links	+2A, 1D	C2
	Access subject software access to terminals, computers, computer network nodes, communications links, computer peripherals, software, volumes, catalogues, files, records, record fields	+2A, 1D	B2
	Changes in access subject authorization	+1C	B1
	Secure access objects that have been created	+2A, 1C	C2
2.2	Information media accounting	+3B, 2B, 1E	B1
2.3	Erasing (zeroing, eradicating) freed up RAM sectors in the computers and external memory devices	+3A, 2A, 1D	C2
2.4	Signaling attempts to violate security	+1C	B3
3.	Encryption subsystem		
3.1	Encoding confidential information	-2A, 1B	-
3.2	Encoding information belonging to various access subject (groups of subjects) in various keys	-1A	
3.3	Use of attested (certified) encryption equipment	-2A, 1B	-

Table 1 (cont)

Subsystems and Requirements		RF Guidance Document	U. S. Standard
4.	Integrity assurance subsystem		
4.1	Integrity assurance for software tools and information being processed	+3B, 2B, 1E	C1
4.2	Physical protection for computer equipment and information media	+3B, 2B, 1E	A1
4.3	Existence of an information security administrator (group) for the automated system	+2A, 1C	B3
4.4	Periodic testing of the system to protect information from unauthorized access	+3B, 2B, 1E	C1
4.5	Existence of means to recover the system to protect information from unauthorized access	+3B, 2B, 1E	B3
4.6	Use of certified security equipment	-3A, 2A, 1C	-

On the other hand, a similar comparison, this time taking into account the functional composition of the U. S. standard, is presented in Table 2.

In the column to the right of the index name in this table, a "+" sign indicates requirements having security indexes for which there exist functionally identical or similar requirements in the U. S. standard and the [Russian Federation] guidance document. Also indicated are those protection category indexes correlated with the American standard and those correlated (by category groups) with the Russian Federation standard for which security system requirements have just been added for the first time.

Based on these data one can conclude that although in most instances the guidance document security categories have functional requirements similar to those in the U. S. standard, the makeup of the categories differs significantly. One can state with reasonable approximation that security ratings C1-C2 in the U. S. standard essentially correspond to the third group of security categories in the guidance document; similarly, security ratings C2-B1 correspond to the second group of categories; and ratings B1-B3 correspond to the first group.

This situation may be explained by the fact that the guidance document takes into direct account the conditions in which an automated system will operate (the confidentiality level of the information being processed and the type of user need-to-know), whereas these are not taken into account in the U. S. standard. Rather, they are considered only in the operating manuals "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" [5], and "Trusted Network Interpretation Environments Guideline. Guidance for Applying the Trusted Network Interpretation" [6], which use the concept "risk index", a concept that includes the confidentiality level of the information being processed and the functional environment of a computer system (burst mode, multilevel security, etc).

It should be noted that, the initial U. S. standards notwithstanding, these manuals now consider the possibility of employing encryption systems.

Table 2

Index	U. S. Standard	RF Guidance Document
Security Policy Implementation Requirements		
discretionary access control	+C1	+2A, 1D
repeat use of object	+C2	+3A, 2A, 1D
labels	+B1	+2A, 1C
marker integrity	-B1	-
marker information exporting	-B1	-
multilevel exporting	-B1	-
one level exporting	-B1	-
operator perceived read out	+B1	+2A, 1E
mandatory access control	+B1	+2A, 1C
subject critical markers	-B2	-
device markers	+B2	+2A, 1E
Requirements for maintaining system usage accounts		
identification and authentication	+C1	+3B, 2B, 1E
monitoring and recording (audit)	+C2	+3B, 2B, 1E
reliable route	-B2	-
Product reliability requirements		
system architecture	-C1	-
system integrity	+C1	+3B, 2B, 1E
security testing	+B2	+3B, 2B, 1E
design specification and verification	-B1	-
transparent link analysis	-B2	-
configuration management	-B2	-
configuration management	+B3	+3B, 2B, 1E
reliable delivery	-A1	-
Product documentation requirements		
user security guideline	-C1	-
reliable equipment guideline	-C1	-
testing documentation	-C1	-
design documentation	-C1	-

Characteristics of Computerized MC&A Systems

As stated in "Conceptual Design of a National Nuclear Material Control and Accountancy System" [7] the need for an MC&A system is occasioned by the presence of both civilian and military nuclear installations and storage facilities for nuclear materials at Russian Federation nuclear enterprises, as well as the potential radiation and nuclear hazards they pose. Automated MC&A systems are being developed in order to implement requirements for material protection, control, and accountancy within a national material control and accountancy system at the federal, agency, and nuclear facility levels. It has been proposed to use commercial products, the Windows NT 4.0 operating system and the SQL Server 6.5 DBMS (Microsoft Corp., USA) with Oracle 7.0 (Oracle Corp., USA) as the primary operating medium. The choice of these products for MC&A systems, both in the U. S. and in Russia, is occasioned by the fact that they most fully meet the requirements of modern information technologies.

Since the information that will be processed in the MC&A system contains sensitive information, including those that constitute government secrets, Russian Federation law requires certification of the general system software that will be used (the OS and DBMS) and any secure MC&A software media created using them. In addition, the complete automated material control and accountancy system must be attested to comply with information security requirements under realistic functionality conditions. In some instances the OS and DBMS must be certified at a higher security category than that attained by the off-the-shelf versions, which leads to the necessity of modifying and improving them.

Previously it had been true that commercially available software products did not meet minimal security requirements, but today modern OS and DBMS are being developed and certified as meeting information security requirements; they are successfully being utilized in information technologies that are critical for information security.

The MC&A systems under development differ from general purpose systems in the following ways:

First, MC&A computer equipment is being installed in secure, protected areas--as a rule, in nuclear material storage facilities. A protected area is a zone equipped with physical security equipment that eliminates the possibility of unmonitored access by outsiders without permanent or one-time passes. Therefore, with regard to physically isolated systems, the threat of unauthorized access to computer equipment or hookup to network communication lines for eavesdropping on traffic can be ignored under these conditions.

Second, MC&A personnel can be given access to all processed information and can have equal access rights. Under these conditions, the mandatory use of access limiting software (the discretionary principle) is not significant; and, if all the information in the MC&A system has the same degree of confidentiality (secrecy), the need for utilizing the mandatory principle of access control may be eliminated.

Third, as a rule the MC&A software environment consists of a fixed set of precisely installed components and processes. The list of files and programs that MC&A operators can create or launch is strictly specified. Therefore, information streams and security mechanisms can be defined statically, which in turn may eliminate the need for using the mandatory access method and allow for all access control to be conducted using the discretionary access method.

MC&A System Classification

MC&A systems are separated into categories based on the conditions in which they will function in order to have a basis for developing and implementing measures to achieve the required level of information security. Differentiating the approach to selecting methods and security equipment is necessitated by the importance of the information being processed; by differences among MC&A systems with regard to components, structure, and the methods used to process, store and transmit information; and by the characteristics and number of users and service personnel.

Security class selection criteria, which are used to group MC&A systems, include:

- Information of various classification levels present in the MC&A system;
- Authorized subject (user) access levels to secret information;
- Procedures and conditions relating to component location and functionality, as well as thephysical protection of system computer equipment.

Based on conditions under which MC&A systems will operate, three classes of system protection are established: Three (III), Two (II) and One (I).

A MC&A system designated as Class Three is characterized by:

- Presence of only one secrecy level;
- All access subjects have equal access rights (authorization) to all MC&A information;
- All MC&A computer equipment is housed in a protected area and has no exterior (extending beyond the protected area's territory) physical information links.

A MC&A system designated as Class Two is characterized by:

- Information of several secrecy levels present;
- Access subjects have different access rights to MC&A information;
- All MC&A computer equipment is housed within the confines of one or several protected areas and has no unprotected exterior physical information connections.

A MC&A system designated as Class One is characterized by:

- Information of several secrecy levels present;
- Access subjects have different access rights to MC&A information;
- MC&A computer equipment is housed in a protected area and has exterior physical information connections with computers not related to the MC&A system.

These classes are presented schematically in Fig. 1.

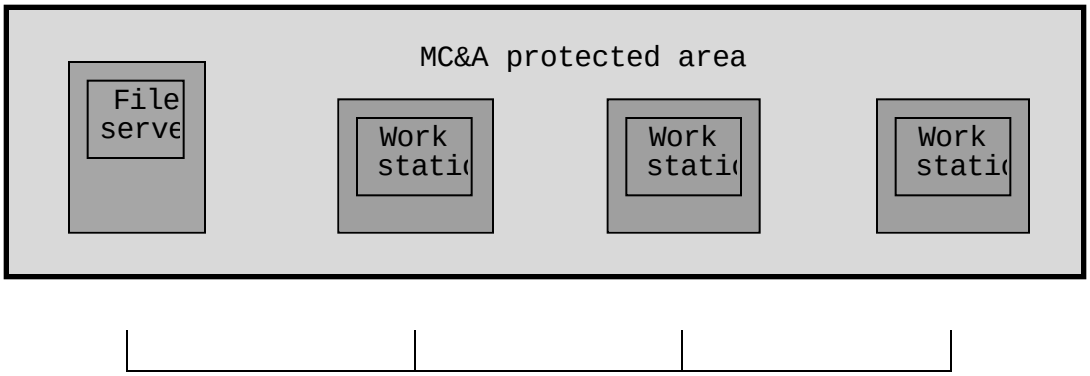
A minimum set of requirements for information security is presented for each MC&A class.

The totality of hardware, software, and organizational decisions related to the protection of information from unauthorized access are to be implemented within an overall security system to protect against unauthorized access to information consisting of the following four subsystems:

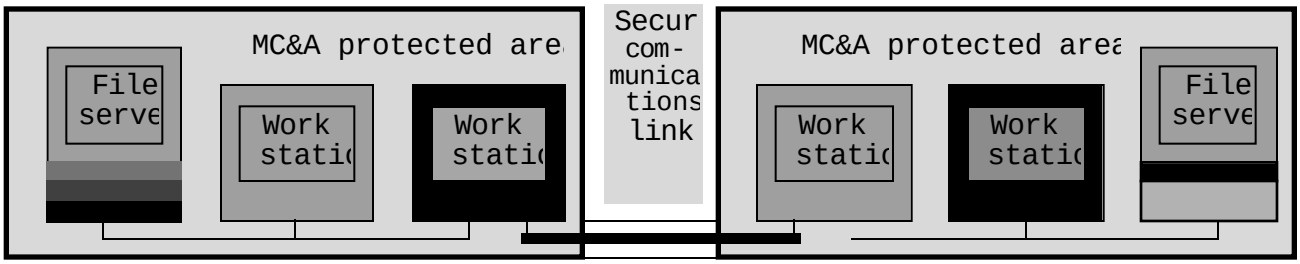
- Access control subsystem;
- Information logging and accountancy subsystem;
- Cryptographic subsystem;
- Integrity assurance subsystem.

Depending upon the MC&A system class, the requirements listed in Table 3 must be implemented for each subsystem.

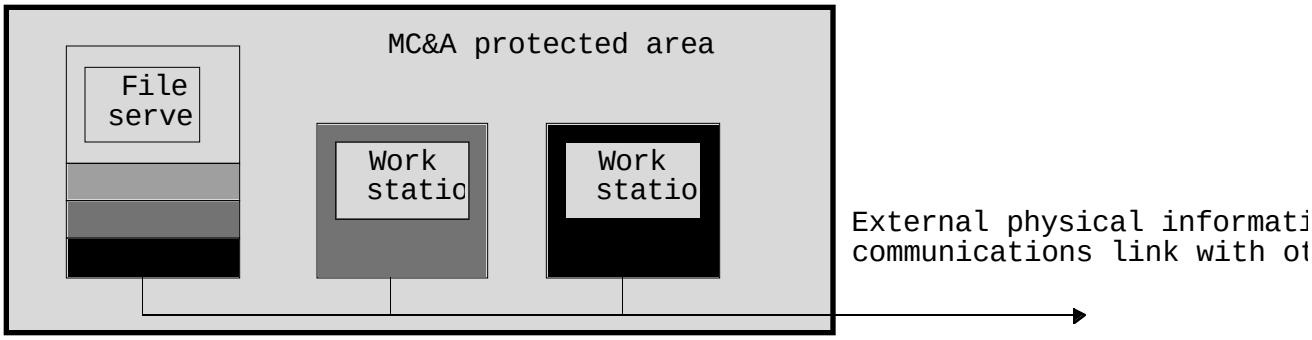
Figure 1



Class III MC&A system: various operator righ information on one secrecy level



Class II MC&A system: various operator rights; processed information



Class I MC&A system: various operator rights; processed information contains external physical information communications links

Symbols:

"-" not required of the given class;

"+" required of the given class.

Table 3

Subsystems and Requirements	MC&A Class		
	III	II	I
1. Access Control Subsystem			
1.1 Identification, Authenticity Verification and Access Subject Control:			
• Upon entry into the operating system	+	+	+
• Upon access to the DBMS	+	+	+
• Upon access to OS objects (work stations, servers, networks, domains, communication channels, ports, RAM sectors, peripherals, processes, disks, volumes, catalogs, files, etc.) and to DBMS objects (files, tables indexes, records, record fields, diagrams, procedures, etc.)	+	+	+
1.2 Data Transmission/Reception Network Control	-	+	+
1.3 Data Access Process Restrictions	-	+	+
1.4 Data Stream Management	-	+	+
2. Information Logging and Accountancy System			
2.1 Information Logging and Accountancy:			
• Entry/exit of access subjects into/out of an operating system (work station, server)	+	+	+
• Production of printed (graphic) output documents	+	+	+
• Bootup/completion of all programs (processes, tasks)	+	+	+
• Software access (processes, programs, projects, tasks) to secure files and catalogs	+	+	+
• Software (process) access to network nodes and segments (domains, servers work stations), ports (lines, communications channels), and peripherals (processes)	-	+	+
• Access to DBMS objects (files, tables, indexes, records, record fields, diagrams, procedures, etc.)	+	+	+
• Changes in access subject authorization or status of access objects	-	-	+
• Secure access objects	-	+	+
• All disruptions during a network data exchange	-	+	+
• Connections between remote processes	-	-	+
2.2 Information Media Accountancy	+	+	+
2.3 Erasure (zeroing, initializing, eradicating) of freed up RAM sectors and external memory sectors	-	+	+
2.4 Signaling of an Attempt to Bypass Security	-	-	+

Table 3 (cont)

Subsystems and Requirements		MC&A Class	
	III	II	I
3. Cryptographic Subsystem			
3.1 Classified Information Encryption	-	-	+
3.2 Use of Certified Cryptographic Security Equipment	-	-	+
4. Integrity Assurance Subsystem			
4.1 Integrity of Software and Information Being Processed	+	+	+
4.2 Connectivity Integrity	-	-	+
4.3 Proof of Data Transmission and Reception	-	-	+
4.4 Physical Protection of Locations, Computer Devices and Information Media	+	+	+
4.5 Presence of an MC&A Information Security System Administrator (Group)	-	+	+
4.6 Periodic Testing of Security Systems against Unauthorized Access to Information	+	+	+
4.7 Presence of Capability to Restore the Security System against Unauthorized Access to Information	+	+	+
4.8 Use of Secure Communication Lines	-	+	+
4.9 Use of Certified Internetwork Filters	-	-	+
4.10 Use of Certified Security Equipment	+	+	+

When information that does not constitute a government secret, but nonetheless requires protection from unauthorized access, is used under the realistic conditions of an MC&A system, the set of requirements the MC&A system must meet may comprise a subset of the requirements outlined below (sic).

Based on a preliminary analysis of the commercially available Windows NT 4.0 operating system and the SQL Server 6.5 DBMS, which are being proposed as the primary system software tools for the creation of the MC&A system, one can draw the following conclusions that take into account the certification requirements that have been specified.

The standard components information protection tools contained in the Windows NT 4.0 OS and the SQL Server 6.5 DBMS come closest to satisfying the requirements proposed for Class III MC&A systems.

For example, these products have the capability of indentifying and authenticating users upon entry into the system (the maximum length of passwords in the Windows NT 4.0 OS is 14 characters, and in the SQL Server 6.5 DBMS -- 30 symbols).

All access objects in the operating system (domains, servers, work stations, peripherals, network devices, ports, RAM sectors, processes, catalogs, files, etc.) are uniquely identified in the system by name and special system token.

DBMS access objects (tables, procedures, indexes, circuits, records --in the form of lines and column tables, etc.) are also uniquely identified in the system by name.

The operating system can create detailed logs of the following events: system bootup and shutdown; user entry into and exit from the system; access to objects; bootup and completion of processes; changes in subject privileges; etc. The logging tools are accessible only to the

administrator and include for his use the capability to review and analyze with respect to the indicated parameters all events that have occurred (Event Viewer), as well as archiving capabilities. Operating system resources are isolated using an Object Manager, which, together with a Security Refernce Monitor, employ the discretionary principle to control access to objects. A Registry and the presence of the appropriate modules are used to verify system integrity at startup.

The integrity of the DBMS protection tools is ensured by isolating them from the users using the security mechanisms in the operating system and the DBMS, as well as by the capability of the DBMS to recover data bases in a timely manner.

One must also take into account the fact that Class III MC&A systems must satisfy a number of attestation requirements that modify the security mechanisms in the OS and DBMS and limit the conditions under which they may be used.

The standard components information protection tools contained in the Windows NT 4.0 OS and the SQL Server 6.5 DBMS are insufficient for Class II and Class I MC&A systems, because such multilevel systems require, additionally, use of the mandatory access control, zeroing freed up memory sectors on external media, monitoring of data being transmitted over the network, inter-network filters, data encryption, etc. Therefore, such systems require that appropriate modifications be made to mechanisms within the Windows NT 4.0 OS and the SQL Server 6.5 DBMS.

In order to certify the security mechanisms within the Windows NT 4.0 OS and the SQL Server 6.5 DBMS for compliance with the requirements established for all classes of MC&A systems, it is necessary to conduct research and experiments (testing) in accordance with the program and methodology established in the document "Regulations on Certification of Information Security Equipment for Compliance with Information Protection Requirements" [8], which has been adopted for use in the Russian Federation. Certification testing procedures in the U.S. and in Russia presuppose, in particular, that research will be conducted and that design documentation for the software products being certified will be analyzed, including the software source texts. Although issues regarding the conditions under which developers are to provide design documentation to testing centers have been resolved by legally and logistically on the national level, on the international level they cause great and sometimes unresolvable difficulties. In this regard, it seems reasonable to try to resolve such issues within the framework of an international agreement that would incorporate, in particular, the establishment of international certification centers.

Conclusions and Future Activities

When designing specialized computer systems such as MC&A systems, it is recommended to take into account the following typical considerations:

1. Location and the possibility of physically isolating the MC&A equipment; information processing modes and the conditions under which they will operate; principles for selecting MC&A personnel.

2. The possibility of using commercial products such as the Windows NT operating system, UNIX, VAX/VMS, the Oracle DBMS, Informix, SyBase, etc. (which have been developed to satisfy information security requirements) as the primary system software tools.

3. When designing multilevel extended systems, the security systems in off-the-shelf commercial products must be modified and improved in order to achieve a higher security category.

Moreover, it is very important, when designing the primary system software tools (OS, DBMS) for the federal computer system security evaluation criteria to be brought into line, for instance,

with the Common Criteria Program that is being developed to serve the interests of the world community.

This comparison of the information security assessment criteria used in Russia and the United States reveals both similarities and differences. The authors feel this comparison can only contribute to an improved joint understanding of information security issues. The authors hope that improved understanding will in turn lead to the development of strong international standards for information security assessment, with participation by countries outside the current North American and Western European communities. International cooperation is needed on this topic and many more to sustain and nurture the US-Russian cooperation in nuclear non-proliferation, which led to this investigation. One should also note the importance of developing an international agreement regarding the certification of software products; this agreement should incorporate, in particular, the establishment of international certification centers.

Acknowledegments

1. Part of this work was performed under the auspices of the U.S. Department of Energy by Pacific Northwest National Laboratory under contract no. DE-AC06-76RLO 1830.

2. Part of this work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract no. W-7405-Eng-48 UCRL-JC-127687.

3. Part of this work, performed by Los Alamos National Laboratory, was supported by the US Department of Energy, Office of Arms Control and Nonproliferation.

References

1. Guidance document. "Automated Systems. Protection Against Unauthorized Access to Information. Classification of Automated Systems and Information Security Requirements." State Technical Commission of Russia, 1992.
2. Department of Defense Standard. "Department of Defense Trusted Computer System Evaluation Criteria." DOD 5200.28-STD. December 1985.
3. "Unified Software Document System." Compilation of Russian Federation standards.
4. "Unified Engineering Document System." Compilation of Russian Federation standards.
5. National Computer Security Center. "Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments." CSC-STD-003-85. 25 June 1985.
6. National Computer Security Center. "Trusted Network Interpretation Environments Guideline. Guidance for Applying the Trusted Network Interpretation." NCSC-TG-011, Version-1. 1 August 1990.
7. “Conceptual Design of a National Nuclear Material Control and Accountancy System”, Russia, 1996.
8. "Regulations on Certification of Information Security Equipment for Compliance with Information Protection Requirements." State Technical Commission of Russia, 1994.