Information Security Policy in the Distributed Computer Systems

Vadym MUKHIN, Artem VOLOKYTA
National Technical University of Ukraine Kiev Polytechnic Institute
Pr. Pobedy, 37, UA-03056 Kiev
mukhin@comsys.ntu-kpi.kiev.ua

Abstract — **In the paper are presented the general principles of the information security policy in the computer systems. The main components of the security policy, implemented in accordance with the requirements of the modern standards, are described in detail.**

The model of the security policy for the distributed computer systems is suggested. The potential threats to the safety of the computer systems and the main rules of the security policy for administrating in the distributed computer systems are formulated and substantiated, using the suggested model.

The suggested model for the access control of the subjects to objects in the distributed computer systems allows formalize an important component of the information security system.

Index Terms — **distributed computer systems, information security, model, security policy**

I. INTRODUCTION

The development and implementation of the information security policy is an important element of security system in the distributed computing systems (DCS).

The security policy is a set of rules and regulations on the implementation of administrative and hardware/ software mechanisms for information security in the DCS. In general, the security policy is an active component of security system, which includes a preliminary analysis of possible security threats, the rules for legal (registered) subject actions in DCS and the principles of choice of the mechanisms to prevent the unauthorized access of the violators.

The implementation of the security policy requires solving the following tasks: to define the main principles of security policy, to develop the supporting mechanisms, to analyze and to control the security policy, to formalize the security policy rules, in particular, the rules for subject's access control in the DCS.

II. THE GENERAL PRINCIPLES OF SECURITY POLICY DEVELOPMENT IN THE DISTRIBUTED COMPUTER SYSTEMS

The main goal of the development of the security policy for the distributed computer systems is to define rules for the DCS resources protection.

In general, the security policy should [1] - [3]:

1) be based on a concept, that includes the goals, guidelines and principles of information security tools implementation;
2) be based on the legitimate and regulatory requirements and on the requirements of DCS owners to the information safety assurance;
3) be consistent with the strategy of the security risks management in the DCS for which policy is developed and implemented;
4) establish the criteria for the security risks assessments;
5) be approved by the security administrator and the management of the company, which is the owner of DCS.

Initially, the security policy developer analyses the security risks, existing in the DCS. Next, he defines a strategy for security design and generates the rules for the security system configuring, for the security administrator and users actions in case of the normal and the contingency events, such as attacks of intruders [4].

Thus, security policy realizes two main functions: defines the rights of the legal subjects in the DCS; defines the rules for the DCS resources protection.

The security policy is fixed in a set of documents, describing all the basic requirements for information protection in DCS [1]. Also, the security policy defines the method of the security systems implementation, and the rules for the DCS parameters adjustment. Also, the security policy identifies the necessary mechanisms for information protection in the DCS, the reaction in case of contingency events. In the event of incidents, involving the security violation or failure in the system security, the security policy defines the actions order for the reaction on these incidents.

Thus, the information security policy in DCS is based on the generalized and strictly formalized rules, procedures and requirements, such as: to use the certified hardware and software, to define the procedures for the subject access to DCS resources, to establish the rules for DCS resources protection.

An important function of security policy is a strict distinction of the subject rights for the access to the DCS objects: all the legal subjects must know and observe their rights for access to objects and the rights of others DCS subjects to the objects owned by them.

In general, the security policy defines the actions of DCS administrators and legal subjects on the installation and using of information security tools, as well as on the processing and transmitting information in the DCS.

There are 3 main segments of security policy [2]:

- *Goal.* The security policy has a clearly defined goal, which asserts the need to implement the developed policy and the benefits from it.

- *Area.* Security policy contains a section describing the specifics of its application, for example, whether it applies to the all computer systems and networks, or only to the certain segments of the DCS.
- *Responsibility.* This section identifies the actions of the security administrator, who must follow all the requirements of security policy in a certain DCS.

The security policy development involves a number of preliminary stages:

- to identify the threats to the DCS resources;
- to analyze the potentially vulnerable DCS resources;
- to assess the security risks for the certain DCS.

The full life cycle of the security policy includes the following stages:

1) the preliminary analysis of the information security in DCS;
2) the security policy development;
3) the implementation of the developed security policy;
4) the analysis of the implemented security policies and the perform of the actions for its further improvement.

In the practical applications there are 3 main levels of specifications for the security policy: high, medium and low [5].

Thus, the security policy for the all levels should be based on the following basic rules:

– the security policy at the low level must fully comply with the relevant policies of the higher levels, and also comply the current legislation and requirements in the field of information security;

–the security policy should be clearly and unambiguously formulated;

– the security policy should be clear for the staff to whom it is addressed.

The *high level* of security policy includes the decisions and the main terms for the information security strategy implementation. Also, on this level are determined: the principles for the control and coordination of the security mechanisms; the staff, responsible for the system security; the principles of the collaboration with other companies, which provide or supervise the security tools implementation.

On the high level of the information security policy are defined:

– the goals in the field of information security, and the common trends in the achievement of these goals;

–the basis for the individual security policies development (at lower levels), the rules and regulations for certain issues;

– the tools for the staff informing about the main tasks and priorities in the field of information security;

– the administrative decisions on the security issues for the whole company.

The *medium level* of the security policy determines the certain aspects of the company activities on the computer systems usage:

– the requirements (more detailed in comparison with the high level) of the company to the information flows processing in the safe way;

– the requirements to the specific information and network tools, methods and approaches to the information processing in system;

– the requirements to the staff who are the participants of the information processing, and who are responsible for the security of the information resources;

– the main methods and mechanisms for the impact on the staff in order to support the information security.

On the *low level* of the security policy are described the certain elements of computer systems and are determines the specific procedures and documents, related to the information security. This level includes the instructions for the direct actions in the usual activities of the company and these documents are related to certain services, procedures and systems. The main goal of these documentations is to ensure as much as possible detailed and formalized description of the all procedures and requirements relating to the security of the certain elements of computer system, of the information flow and data files. In particular, in order to ensure the completeness of security policy, the company must generate the full set of these documents, including:

– the forms of applications for the individual staff members, who will get the access to certain information resources;

– the rules for the access to the certain information and networks systems, software and databases;

– the duties of certain categories of the staff, related to the information security, and the requirements for the staff.

The documents with the rules on the access to the computer systems and/or modules of computer systems (databases, modules of the corporate accounting system, electronic document management system, etc.) include all the basic requirements, rules and restrictions, for example, the ban to use the external devices (such as flash-memory) for the information copying and transferring, the restrictions on the remote access to some information services, etc. The requirements and rules related to information security may be included in the general instructions or regulations on the computer systems using or presented as the dedicated instructions and reminders.

III. THE MAIN COMPONENTS OF THE SECURITY POLICY

According to the requirements of modern standards [2], [6], the security policy should include the following components:

- the setting of the access level of the subjects to the DCS resources;
- the control of the subjects access to the DCS objects;
- the support of the safe usage of the DCS objects.

Let us consider the specifics of each of these components in more details.

The setting of the access level of the subjects to the DCS resources

The subjects are assigned with the security labels in order to set up them the access level to the DCS resources. The subject's label defines the level of his rights for the access to the objects, the object's label defines the level of required security for the information contained therein. Security labels are consist from 2 parts - the level of secrecy and the list of categories. The levels of secrecy, form an ordered set, which, for example, may be as follows:

- top secret;
- secret;

- confidentiality;
- public information.

The categories form an unordered set. The categories mechanism allows to divide the information on the segments and to increase the objects security. Thus, the subject can not get access to segments of the "other" category, even in case if his access level is "top secret".

The control of the subject access to the DCS objects

The access control of subjects to the DCS objects in terms of security policy is divided into a mandatory and labeled control.

Mandatory access control

Mandatory access control is a method on the basis of personality and specifics of the subject or group of subjects. The feature of the mandatory access control is the next: some person (security administrator or owner of the object) gives other subjects the access rights (mandate) to access the object. The current parameters of the access rights in the mandatory control are described by access matrix. The left column of this matrix describes the subjects, and the upper row describes the objects of DCS. In positions located at the intersection of rows and columns, there are determined the access rights of subject *i* to object *j*, for example: *R*-Reading, *W*-write, *E*-execute, *T*-authorize to transfer the rights to the others subjects, etc. However, due to the fact that the access matrix contains the large volume of stored data and is sparsed, i.e. most of the positions in it are set in 0, in the practice is used the more compact representation of the access matrix, which is based on the structuring of subjects rights (owner/group/other), or on the mechanism of access control lists, i.e. on the decomposition of the matrix by columns, where for each object are listed the subjects and their access rights.

The mandatory access control is realized in the most DCS. Its principal advantage is the adaptability, the main shortcoming is the control decentralization due to the complexity of centralized control, and also the separation of mandates from the data, that may lead to copy of the sensitive information into the public files [4].

Labeled access control

Labeled access control is based on a comparison of the subjects and objects security labels. The security labels of subjects and objects fix the corresponded access rights of the subjects to the objects.

The effective implementation of labeled access control mechanism requires the labels integrity. First, all (with no exception) subjects and objects should be with labels, otherwise there will appear the "holes", which are easy to use for intrusions realization. Secondly, all operations with these labels should be correct, in particular, such as the data export and import. For example, the file transfer via network must be accompanied with the label, associated with it, and in such way that the remote system could identify the label, despite of possible differences in the secrecy levels and in the categories set.

The one of the approaches to ensure the security label integrity is the division of DCS resources on single- and multi-level. The multi-level resource may store the information with different secrecy levels, the single-level resources are a special case of multi-level, when the secrecy is ranged in the one level. The analysis of the resource level allows make the decision on record and store on this resource the information with a certain label. For example, it is prohibited to print the top secret information on the network printer with the access level "confidential".

The subject security labels are more dynamic than the objects labels. The subject may change his label in the session, remaining within the predefined access rights. In particular, he may deliberately reduce his access level to reduce the probability of unintentional errors.

The subject can get access to the object in case only if the subject secrecy level is not lower than the object secrecy level, and all of the categories in the object's security label are exist in the subject's label, i.e. the subject label is "dominant" over the object label.

The subject may write information to the object in case only if the object security label is "dominant" over the subject label. In particular, the subject with the access level "confidential" may write in "secret" files, but may not write in the "open" files, i.e. the information secrecy level should not be lowered.

Labeled access control is implemented efficiently in the DCS with a high security level. Regardless of the practical usage, the labeled access control is the effective methodological basis for the initial classification of the information and for setting the access rights. In the practice, mandatory and labeled access control may be combined, and the advantages of both approaches will be strengthen.

Safety of Objects

The objects safety is considered as additional mechanisms for the access control, which allow prevent the accidental or intentional access to the secret (secured) information. The safety must be guaranteed for the RAM (in particular, for the screen images buffers, which are currently decrypted with the passwords, etc.), to the HDD blocks, and for the other data storages in the DCS.

The information about the subjects is also an object, so it is necessary to ensure the security of these data. In case, when the subject loses access rights to the DCS resources, the control mechanisms should not only deny for him the possibility to get access to the system, but also it should forbid him access to the all objects, otherwise the new registered user will be able to get identifier, which was used previously, and the all access rights of the subject-predecessor [7].

Control

The control mechanism is additional tool to the subject access control. The goal of this mechanism is to monitor the subjects actions during they are logged in the DCS.

The control tools are divided into three categories:

- the identification and authentication;
- the secured communication channel;
- the analysis of subjects actions.

Let us consider these categories in more details.

Identification and Authentication

Each user (subject) before he will get the access to the DCS must identify itself, i.e. enter the name (login) at the logon stage. In turn, the system must authenticate him, i.e. to check his authenticity and to confirm that he is really the legal subject. The simplest way of authentication based on a password, but there also can be used the more complex mechanisms, such as: personal cards, biometric devices, etc.

Identification and authentication are the first stage and very important part of the information security system, since the system can not to log subjects actions without their identification [8].

The secured communication channel

The secured channel connects the subjects directly to the DCS resources, without any mediatory components, which can be potentially dangerous to the system. The goal of the secured communication channel is to confirm for the subject the authenticity of DCS, with which he is interacting [9].

There is quite easy to implement the secured communication channel if the non-intellectual terminals are in use. In this case it is sufficient to implement a special interacting protocol for the secured channel between the terminals and the system. If the subject works with an intelligent terminal, personal computer or workstation, the task of implementation and ensuring of the secured communication channel is much more complicated [10], [11].

The Analysis of subject actions

This analysis involves the subjects actions (events), relating to the DCS safety. These events are: login; logout; the file operations (open, close, rename, delete); the access to the remote DCS resources; the change of the security attributes (the access rights, the subject access level and so on).

Full list of the events in the DCS, that should be registered and analyzed, is depending on the current security policy and on the specifics of DCS [12].

If the all events related to the DCS safety are fixing, then the volume of registration information will be increased rapidly and the effective analysis of these data will be impossible. So, the selective monitoring mechanism is used often for the subjects actions analysis (for example, only the suspicious subjects are under monitoring), and for the security events analysis as well.

The monitoring tool allow to monitor the subjects actions and to reconstruct past events, and also this tool is effective as preventing measure, because the subjects may refrain from security violations, if they know that all their actions are recorded. The events reconstruction allows analyze the security incidents, and to find out why they were become possible, to assess the damage and to take the steps to prevent such violations in the future.

The monitoring process requiring record the following events:

- date and time of the event;
- the identifier of the subject, who is initiator of the action;
- type of event;
- result of the subject actions;
- the identifiers of the used objects (e.g., open or delete files);
- security labels of the subjects and objects, which are the participants of the event;
- changes to security records (e.g. the new security label of the object).

It is very important not only to collect the security records, but also to analyze them regularly and purposefully.

Warranty

Warranty is the degree of confidence as confirmation, that the security policy, which is implemented in DCS is based on the correctly selected set of tools, and that each of these tools are functioning in a proper way.

There are two types of warranty: the operational and technological [13]. Operational warranty is referred to the security of the structural and implementing aspects of the system, and technological is referred to the methods of the system design and support.

Operational warranty

Operational warranty is based on the test of the following elements: the system structure, the system integrity, the security of network channels, the effectiveness of the security administration, the reliability of system recovery in case of failures.

Operational warranty allows to confirm that the structure of DCS and its implementation is corresponded to the current security policy. The DCS structure should support the possibility to implement the security mechanisms.

The examples of such approaches for DCS structure design are the instructions division by the priority levels, the protection of the various system processes from the mutual influence by allocating them in the separate virtual spaces, the protection for the operating system kernel.

Technological warranty

The technological warranty covers the full life cycle of the DCS, i.e. design, implementation, testing and maintenance. All these stages must be performed in accordance to the requirements to protect the DCS resources from the unauthorized access and illegal "tabs" in the software and hardware.

An important aspect of the technological warranty is the testing. The security mechanisms and user interface should be tested. The tests must confirm that security mechanisms are implemented in accordance with the description and that there is no any available way to circumvent or destroy the security tools. Also tests should to prove the effectiveness of the access control, the security of logging and authenticating information.

IV. THE MODEL OF THE INFORMATION SECURITY POLICY IN THE DISTRIBUTED COMPUTER SYSTEMS

Let us consider and formalize the aspect of the security policy: the access control of the subjects to objects. In fact, we suggest the formalization of the security policy for DCS administration.

Let us introduce the following notations:

$ND = \{nd_i\}$ - the set of DCS nodes, which includes the servers and workstations, $SR = \{sr_i\}$ - the subset of servers (routers) of DCS domains, $WS = \{ws_i\}$ - the subset of the workstations, and: $SR \cup WS = ND$, $SR \cap WS = \varnothing$.

$U = \{u_i\}$ - the set of DCS subjects;

$A\ (u,ws)$ - the function that determines for the subjects $\{u_i\}$ the set of workstations $\{ws_i\}$, to which they have access locally or via network;

$M\ (u,ws)$ - the function that determines for the subjects $\{u_i\}$ the set of workstations $\{ws_i\}$, where they can store and modify their own resources: files, data or processes;

$R\ (u,ws)$ - the function that determines the set of the access rights of subjects $\{u_i\}$ to workstations $\{ws_i\}$;

R_{wsj} - the set of the access rights of subjects U to the workstation ws_j, such as: read, modify information, run processes, to administrate the operating system, etc.

The security system has the following features:

1) the sets ND, SR, WS and $R\ (u, ws)$ are constant in time. The subject registration, the setting up their access rights to the system, as well as the parameters of the servers and workstations in the DCS are defined by the system administrator before the subject will get access to the DCS

2) initially, the subjects of DCS do not store any data on the workstations, i.e., for each $\{u_i\}$:

$M\ (u,ws)\ = \varnothing.$ (1)

3) legal (registered) subject $\{u_i\}$ on the workstation ws_j has rights $R(u_i,\ ws_j)$ for the access to it.

4) if subject u_i has some special access rights to a certain workstation ws_j, for example: R_1 = "Debug", R_2 = "Install Driver" etc, he may get the full access rights R_{wsj} to the resources of this workstation , i.e.:

$\{R_1,R_2,...,R_n\} \cap R\ (u_i,\ ws_j) \neq \varnothing) => R_{wsj}.$ (2)

Trusted subjects of workstation ws_j are such subjects u_i, who have the access rights $R\ (u_i,\ ws_j)$. The set of the trusted subjects of workstation ws_j denoted as U_{wsj}. The other subjects from the set $U \backslash U_{wsj}$ for this workstation are untrusted.

Further, the node nd_2 *is directly subordinated* to the node nd_1, if at least the one of the following conditions is true:

1) nd_1 is the server (router) of domain, nd_2 is the workstation of this domain;
2) nd_1 is the server of the first domain, nd_2 is the server of the second domain, which is trusted the first.

Thus, let us draw a directed graph $G\ (N,\ L)$ of the nodes subordination in the DCS. In this graph: N is the set of nodes, L is the set of edges.

All registered nodes (servers and workstations) of DCS in the graph $G\ (N,\ L)$ are shown as the circles, in which the only one edge is come and no one edge comes from to the unregistered nodes. If a node is not a member of this domain, then in the graph $G\ (N,\ L)$ this node is shown as an isolated circle. And $(nd_1,\ nd_2)\ \in L$ if and only if the node nd_2 is directly subordinated to the node nd_1, and node nd_2 is subordinated to the node nd_1 ($nd_1 \rightarrow nd_2$) if and only if in the graph $G\ (N,\ L)$ exists an oriented path from nd_1 to nd_2.

Let us consider the fragment of the graph $G\ (N,\ L)$ of the nodes subordination in the DCS (Fig. 1).

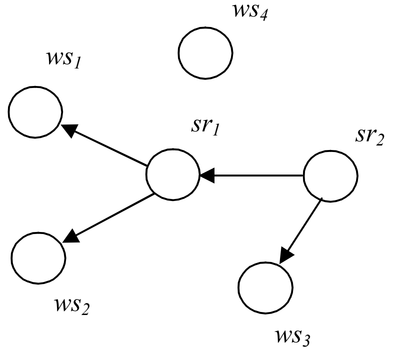

Figure 1. The graph $G\ (N,\ L)$ of the nodes subordination in the domain of DCS

In this graph: ws_1, ws_2 - workstations of the first domain; ws_3 - workstation of the second domain; ws_4 - the workstation, that is non-member of any domain; sr_1 - the server of the first domain; sr_2 - the server of the second domain, that is trusted by the first server. Then $\{(sr_1,\ ws_1),\ (sr_1,\ ws_2),\ (sr_2,ws_3),\ (sr_2,\ sr_1)\} \in\ L.$

In result, if subject u_i has the access rights to the workstation ws_i, it means that he has the relevant rights to the workstations, which are subordinated to it, i.e. for all $ws_i \rightarrow ws_j$:

$R(u_i,\ ws_i)\ => R(u_i,\ ws_j)$ (3)

Let us define the potential threats for the DCS with the parameters described above.

Threat 1. If the subject u_i has rights to store his resources on the workstation ws_j, there is a threat, that he may get the full access rights to this workstation, i.e.:

$\{M\ (u_i,ws_j),\ R\ (u_i,ws_j) \neq R_{wsj}\ \} =>\ R\ (u_i,ws_j) = R_{wsj}$ (4)

Threat 2. The access of subject u_i to resources of the workstation ws_j generates a threat of the interception of his access rights by the other subject u_{i+1}, who has rights to store his resources on this workstation, i.e.:

$\{A(u_i,ws_j):\ M\ (u_{i+1},\ ws_j),\ R(u_{i+1},ws_j) \neq R_{wsj}\} =>$
$R(u_{i+1},ws_j) = R_{wsj}$ (5)

It should be noted, that not every legal subject of the DCS is trusted for a certain workstation. Thus, there is the potentially untrusted subject of workstation, who stores his resources on it and may realize the threat 2.

Let us formulate the main principle of the security policy for DCS safe administration:

DCS meets the requirements of the secured administration if and only if the conditions 1, 2, 3 and 4 are confirmed.

Condition 1. When the subject u_i allocates his resources on the workstation ws_i, there is necessary, that he will not be able to obtain the full access rights to other workstation ws_j, i.e.:

$\{M\ (u_i,\ ws_i),\ R\ (u_i,\ ws_i) = R_{wsi}\} \neq > R\ (u_i,\ ws_j) =\ R_{wsj}$ (6)

Condition 2. When the subject u_i addresses to the workstation ws_i , the others subjects u_j must not obtain the access rights to the other workstation ws_j, including the workstation (ws_i), the access rights to which he has, i.e.:

$\{\ A\ (u_i,\ ws_i),\ R\ (u_i,\ ws_i) = R_{wsi}\ \} \neq >$
$\{\ R\ (u_j,\ ws_i) =\ R_{wsi}\ \ \&\ R\ (u_j,\ ws_j) =\ R_{wsj}\ \}$ (7)

The checking up of the conditions 1 and 2 requires the consideration of the all possible variants of the system states, that is, in general, NP-complete problem. However, in the practice, there is sufficient to monitor only those variants, which are implemented actually in the DCS.

Condition 3. The subject u_i is able to allocate his resources on the workstation ws_j in 2 cases only:

1) no one from the other workstations is subordinated to this workstation;
2) the subject is a trusted subject for the all workstations, which are subordinated to this (ws_j), i.e.:

$\{(ws_j\ \longrightarrow\ ws_k),\ M\ (u_i,\ ws_j)\} \cup \{(ws_j\ \rightarrow ws_k),$
$M\ (u_i,\ \forall\ \ ws_k)\} = > M\ (u_i,\ ws_j)$ (8)

Condition 4. The subject u_i may address the workstation ws_j only if the all workstations ws_k, for which he is a trusted subject, are subordinated to this workstation, i.e.:

$\{(ws_j\ \rightarrow\ \forall\ \ ws_k),\ A\ (u_i,\forall\ \ ws_k)\} = > A\ (u_i,\ ws_j)$ (9)

Proofs. Let us prove the need to satisfy the conditions 1, 2, 3 and 4 for the secured administration of DCS. The proof will be based on the contradiction.

Let us prove that condition 1 is confirmed if and only if the condition 3 is satisfied. First, we prove the need to satisfy the condition 3 to confirm the condition 1.

Let there is the subject u_i with rights $M(u_i, ws_j)$, for which is not satisfied the condition 3, i.e. exists ws_k, and $ws_k \neq ws_j$, $ws_j \rightarrow ws_k$, but subject $u_i \notin U_{wsk}$, i.e. he has no rights $M(u_i, ws_k)$.

The definition of the threat 1 leads to the fact, that subject u_i may get the access rights $R(u_i, ws_j) = R_{wsj}$ to the workstation ws_j. The (3) implies, that if subject u_i has rights R_{wsj} and $ws_j \rightarrow ws_k$, then he can get rights: $R(u_i, ws_k) = R_{wsk}$. Further, if the subject u_i has the rights R_{wsk}, then, in a consequence, he also has the rights $M(u_i, ws_k)$. Thus, we receive the contradiction, which proves the need to satisfy the condition 3 for the condition 1 confirmation.

Let us prove the sufficiency to satisfy the condition 3 for the conditions 1 confirmation.

Let there are workstations ws_j, ws_k, $ws_j \neq ws_k$, and for which is not satisfied the condition 1, i.e. $\{ M (u_i, ws_j), R (u_i, ws_j) = R_{wsj}\} = > R (u_i, ws_k) = R_{wsk}$. Thus, the subject u_i can allocate his resources on the workstation ws_j, and may use this fact to obtain the full rights to the workstation ws_k. Since $ws_j \neq ws_k$, then (3) implies that this is possible in the one case only: $ws_j \rightarrow ws_k$, i.e. the all workstations ws_k are subordinated to the workstation ws_j, but this fact contradicts to the condition 3, because the subject u_i is not a trusted subject for the all workstations ws_k. Thus, the satisfying of the condition 3 is sufficient to confirm the condition 1.

Further, let us prove that condition 2 is satisfied in the case only if the condition 4 is confirmed.

First, we prove the need to satisfy the condition 4 to confirm the condition 2.

Let there is a subject u_i with the rights $A(u_{i,} ws_j)$ to the workstation ws_j, and there is not satisfied the condition 4, i.e. there is the workstation ws_k, for which subject u_i has the rights $A(u_{i,} ws_k)$, but $ws_j \longrightarrow ws_k$. Suppose, that there is a subject u_j with the rights $R(u_j, ws_k) = R_{wsk}$. Then, the conditions 1 and 2, the definitions of the threat 2 and (5) implies, that the subject u_j has the rights $M(u_{j,},ws_k)$. But if $ws_j \nrightarrow ws_k$, then subject u_j can not have rights R_{wsk}, i.e. $R(u_j, ws_k) \neq R_{wsk}$, and this fact contradicts the assumption above. Thus, the condition 2 is not satisfied, because the access of the subject u_i to the workstation ws_j can not be used by subject u_j to get him the full access rights on the workstation ws_k. So, the condition 4 should be satisfied for the condition 2 confirming.

Let us prove the sufficiency to satisfy the condition 4 for the condition 2 confirmation.

Let there are subjects u_i, u_j and the workstations ws_j, ws_k , and $ws_j \neq ws_k$, for which is not satisfied the condition 2, i.e.: there are rights $R(u_i,ws_j) = R_{wsj,}$, $R(u_j, ws_k) = R_{wsk}$. There is realized the threat 2 and the access of subject u_i to the workstation ws_j was used by subject u_j to obtain him the all access rights to the workstation ws_k. However, under the conditions 1 and 2 and the definition of threat 2: $R(u_j, ws_k) \neq R_{wsk}$ and, consequently, in view of (3) in this case: $ws_j \nrightarrow ws_k$. Thus, the full access rights $R(u_j, ws_k) = R_{wsk}$ to the workstation ws_k the subject u_j could obtain in result of the simple request on the access to the workstation ws_k or from the other untrusted subject u_{j+1}, who receives the access rights as unauthorized subject. But, in the secured DCS there are no any untrusted subjects, who have the full access rights to any nodes. Hence, in this case, the subordination $ws_j \rightarrow ws_k$ must hold, but then the condition 4, contrariwise, does not hold. This fact proves the assumption that the satisfying of the condition 4 is sufficient to confirm the condition 2.

Thus, the suggested model allows formally define the rules for the access of the subjects to the objects, to describe the security threats for DCS and to define the principles and conditions for the secured administrating of the DCS.

V. CONCLUSION

The effective security policy is a key requirement for the complex protection of the hardware/software in the distributed computer systems.

The suggested element of the security policy – the model of secured administration of the subjects to objects access in the DCS allows formalize an important part of the information security mechanism. The improvement of the developed information security policy on the suggested model is based on the realization of the following additional tools: the adjustment of the security policy strategy at the all levels, the continuous enhancement of the response to incidents system; the enhancing of the methods and mechanisms for the information security monitoring.

REFERENCES

[1] S. Barman, "Writing Information Security Policies". Boston, “New Riders”, 2002, 342 p.

[2] ISO/IEC 27001:2005. "Information Technology. Security Techniques. Information Security Management Systems. Requirements". 18 October 2005, 44 p.

[3] T.R. Peltier, "Information Security Policies. Procedures and Standards: Guideline for Effective Information Security Management". Boca Raton, “Auerbach Publication”, 2002, 176 p.

[4] C.C. Wood, "Information Security Policies Made Easy" (9th ed.). Houston, Texas, USA. Pentasafe Security Technologies Inc, 2002. – 84 p.

[5] E. Maiwald, "Fundamentals of Network Security". “McGraw-Hill. Technology Education”, New York, 2004.

[6] "National Institute of Standards and Technology: An Introduction to Computer Security", NIST Special Publication 800-12, Gaitherburg, MD 48, 2002.

[7] L. Tobarra, D. Cazorle, F. Cuartero and G. Diaz, "Application of Formal Methods to the Analysis of Web-services Security"//In Proc. 2nd International Workshop on Web Services and Formal Methods (WS-FM’05), Versailles, France, September 2005, pp. 215 – 229.

[8] M. Hentea, "Information Security Management. Encyclopedia of Multimedia Technology and Networking. IDEA Group Reference". “Hershey”, Pennsylvania, 2005, pp. 390 -395.

[9] F.Y. Wang. "Agent-based Control for Networked Traffic Manage-ment systems". // IEEE Intelligent Systems, N 5(19), 2005, pp. 92 - 96.

[10] K. Bhagavan, C. Fournet, A.D. Gordon and G. O’Shea. "An Advisor for Web Services Security Policies".// In Proc. of ACM Workshop on Secure Web Services (SWS’05), Fairfax, Virginia, USA, November 2005, pp. 197 – 206.

[11] "NCSA Security Policies and Procedures". Available: www.ncsa.uluc.edu/People/ ncsairst/Policy.html

[12] R.C. Cardoso and M.M. Friere, "Security Vulnerabilities and Exposures in Internet Systems and Services. Encyclopedia of Multimedia Technology and Networking. IDEA Group Reference", “Hershey”, Pennsylvania, 2005, pp. 910 - 916.

[13] M. Swanson and B. Guttman, "Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)", National Institute of Standards and Technology, NIST Special Publication 800-14, Gaitherburg, MD, 2002.