ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

# Model for Increasing the Security of Information and Communication Systems

**Saparova Gaukhar**

Assistant, Department of Information Security, Tashkent University of Information Technologies of Nukus branch named after Muhammad al-Khwarizmi, Karakalpakstan, Uzbekistan

**ABSTRACT:** This article proposes a model for increasing the security of information and communication systems that satisfies a given security requirement and differs from those known for using network-invariant structural units of the network - security domains.

**KEY WORDS**: Protective procedures, protective procedures, superposition operator, subgraphs, application software.

## I.INTRODUCTION

The rapid development of computer technology has opened up unprecedented opportunities for humanity to automate mental work and led to the creation of a large number of various kinds of automated information and control systems, to the emergence of fundamentally new, so-called, information technologies.
Unlawful distortion or falsification, destruction or disclosure of a certain part of information, as well as the disorganization of the processes of its processing and transmission in information-managing systems cause serious material and moral damage to many entities involved in the processes of automated information interaction.

## II. PROTECTIVE PROCEDURES FOR SECURITY EQUIPMENT

Ensuring and maintaining the integrity or normal functioning of communication security equipment with the formation of protective procedures for security equipment (PPSE). For software located in the ROM and the operating system there is no possibility of unauthorized access (UA), i.e. protective procedures performed.
Let the user work with security tools, for example, software, in which the presence of any hidden capabilities is also excluded (performed by the PPSE). In this case, malicious actions may be as follows:

– security features for which protective procedures were performed will be used on another computer in some conditions;

– software for which the protective procedures (PP) was executed will be used in a similar, non-completed PP operating environment, i.e. incorrect conditions;

– security tools are used by an unfinished PP and operating environment, and by not running an PP program that potentially carries the possibility of unauthorized access.

To exclude the above events, the following conditions must be met:

$V_1$ -on an operating environment with a completed PP installed on a computer with completed PPSE;

$V_2$ - ensured the unchanged composition of security tools and the operating environment for this session;

$V_3$ - in this executed PP system, other programs that have not completed the PP will not be launched; those. Before starting, it is necessary to monitor the implementation of the PP;

$V_4$ - excludes the launch of programs, procedural PP in any other situation, i.e. unfulfilled PP environment;

$V_5$ - the conditions are met at any time for all users who have completed the PP.

This is a complete implementation of the above conditions, the software environment is the PP.
Ensuring the completed PP significantly weakens the requirements for the basic software, since the activation of processes through the OS is controlled, the SP of the executable modules is sanitized before they are launched, and process simulation is allowed only if the conditions $V_1 - V_4$ are met simultaneously. In this case, the basic software requires only:

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

- the impossibility of launching software and software modules in addition to the completed PP;
- lack of basic software capabilities to influence the functioning environment of already running programs.

All other actions that are a violation of the conditions $V_1 - V_3$ in the remaining part will be detected and blocked. Consequently, the implementation of the PP significantly reduces the requirements for the basic software regarding the availability of hidden features.

The security of a computer system-hardware, OS, application software (AS) and data is a necessary and minimum condition for the security of electronic information exchange. Subject to the implementation of the PP security means and the established security of the computer system, we can talk about a security computer environment (SCE).

The initial stage of the sequential control algorithm for creating SCE should be based on the application of a strict order, which acts as the starting point of support for the next stages. Not all controllers are able to provide protective functions: a sufficient resource of constancy of the controller itself is necessary to perform a consistent control algorithm to create SCE. Preferred hardware implementation of algorithmic procedures.

In practice, a computer system can be considered as some many typical operations, by which, depending on the particular, you can understand individual operations, algorithms, processes, procedures, protocols, etc. The technology of information exchange can be interpreted as some sample with a return from a typical set of operations. The choice with return means that a number of typical operations can be repeatedly used as part of this technology. A program manager or technology algorithm can also be considered as a typical operation.

For the security of a computer system, it is necessary and sufficient that any technology formed on a basic set of standard operations is protected. The security of only typical operations is necessary, but not sufficient: incorrect technology can be formed on the basis of simple and several operations. In other words, the establishment of security is the correctness of any logically consistent sequence of typical operations.

From the theory of combined it is logically known that the number of different $n$ - samples with return from $m$ different elements $m^n$ is equal. At any large and absolute $m$ and $n$ establishment of system security is impossible, since testing will require a lot of time. Although logically feasible is only a very nice part of the possible sample operations, but it's still obvious that any solution to the problem of establishing absolute security of a computer network has no prospect. Therefore, to reduce the dimension, a transition to larger scale units is necessary, which leads to a reduction as $m$ and $n$. Then, instead of some typical operations, structured objects are considered: processes as an organized set of operations, orders - a determinate sequence of processes, protocols, etc.

In this case, a serious difficulty arises - access to individual standard operations is lost, and the security of each of them has to be judged by the cumulative result. It is not possible to directly verify the fulfillment of even the necessary security condition of a computer system, the security of each operation. This is a typical case, almost always establishing the security of an individual operation is physically feasible, only if a painfully organized software product is included with pain. The problem arises of controlling the security of the process components on the radiation of the process as a whole.

The most common architectures for organizing computational procedures are linear and tree-like. Further, the properties of such architectures are specially analyzed.

## III. SECURING TECHNOLOGY WITH LINEAR ARCHITECTURE

Consider the inclusion of additional security features to ensure the security of simple CS - systems.

As it was excellent above, the sad part plays the main role - from turning on the system to activating support mechanisms for SCE. Due to the multiplicative nature of the protective properties, it is impossible to leave this stage without protection, and simply declaring its properties in practice is not enough. Although the SCE model is the development of (TCE) - a model of a trusted computing environment, therefore the introduction of a number of new provisions with specific implementations of an additional security tool (AST) that implements the functions of protecting the security of the environment.

A small CS can be displayed as a sequence of elements $a_i$ ( $A = \{a_i, i = \overline{1, N}\}$ (CS of interconnected elements $a_i$) starting with an c element $a_i$ and ending with an element $a_N$.

*Definitions 1.* A simple (Uncomplicated) system is integral if the integrity of each of its elements is established $a_i \in A, i = \overline{1, N}$.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

*Definitions 2.* The relationship between any pair of elements $(a_i, a_{i+1})$ when checking the integrity of a simple system is $(n_i + 1)$ described by the function of checking the integrity of the system: $B_i = B_i(a_i) = B_i(a_i, c_{i1}, c_{i2}, ..., c_{ini}) = a_{i+1}, i = \overline{1, N-1}$, where are $c_{i1}, c_{i2}, ..., c_{in}$ the parameters of the element $a_{i+1}$. Function, $c_i, i = \overline{1, N-1}$, sets the integrity of the element, $a_{i+1}$, if the integrity of the element is fixed. Moreover, the function $B_i(a_i) = a_{i+1}, i = \overline{1, N-1}$, is the following functions according to.

Now, it turns to the consideration of establishing the integrity of a simple system.

*Statements 1.* The integrity of a simple system is established if and only if the integrity of the element is established $a_N$.

*Evidence 1.* Let the system be protected, then by definition 1 the security of all elements of the system $a_i \in A, i = \overline{1, N}$. is established. Therefore, the security of the element is established $a_N$.

Suppose that the element $a_N$ is protected and the value of the integrity check function is known $B_{N-1} = B_{N-1}(a_{N-1}, c_{N-1,1}, c_{N-1,2}, ..., c_{N-1,n_{N-1}}) = a_N$.

A function $B_{N-1}$ is defined only when the integrity of the element is set $a_{N-1}$.

Arguing by induction, we conclude that from the integrity of the element $a_2$ it follows that the integrity is fixed. Consequently, the integrity of all elements of the system $a_i \in A, i = \overline{1, N}$ is fixed, and by definition 1, the system is integral.

The task of establishing the integrity of a simple system is equivalent to the task of establishing the integrity of an element $a_N$.

Let a subset $D \subset A$ be the set of system elements whose integrity is established.

*Definition 3.* A set is decidable if there exists an algorithm $O_D$ that gives an answer for any element $a_i$ whether it $a_i$ belongs to $D$ the set or does not belong.

*Definition 3*.* A set is decidable if it has a computable everywhere defined function such that

$$X_D(a_i) = \begin{cases} 1, если a_i \in D \\ 0, если a_i \notin D \end{cases} (1)$$

*Definition 4.* A set is called $D$ enumerable if it is a domain of values of some general recursive function, i.e. there is a general recursive function $\psi_D(x)$ such $a_i \in D$, that if and only if for some $x \in N$ $a_i = \psi_D(x)$. A function $\psi_D(x)$ is called an enumerator for a set $D$.

Then the following statement about the use of protective procedures PP can be formulated.

*Statements*2. The task of monitoring the security of the system is solvable only in the presence of PP.

*Evidence2*. It shows that without an additional RP, building a system with establishing security is impossible.

It constructs an enumeration function for the set $D$. It should be general recursive, i.e. everywhere defined on a partially recursive function.

Now we define

$\psi_D = a_i$ (1)

Function $\psi_D(x)$ as follows.

Then it can be represented through the functions of checking the integrity of objects $B_i$. To do this, we define a family of superposition.

$\{P^{n_i+1}_{n_{i+1}+1}\}$.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

$P_{n_{i+1}+1}^{n_i+1}(B_{i+1},B_i)=B_{i+1}(a_i,B_i(a_i))(2)$ (2)

In this case, the enumerating function will take the form:

$\psi_D(i)=P_{n_{i+1}+1}^{n_i+1}(B_{i+1},B_i)$

Moreover, it is $\psi_D(i)$ a partially- recursive function, since it is built from functions that are elementary as a sequence function $B_i$, by successively applying superposition operators to them $\{P_{n_{i+1}+1}^{n_i+1}\}$.

However, $\psi_D(i)$ it is not everywhere defined, because the value of the function $B_1$ at the point $a_i$ is not defined. This is due to the fact that it is not defined (according to Definition 2) the connection $B_0$ that would establish the security of the object $a_1$.

Therefore, it is impossible to construct an enumerating function of a $D$ set is not enumerable.

According to the decidability theorem, the set is $D$ not decidable and, by definition 2[1], the system is not secure.

It shows that with the use of PP, the construction of a protected CS is possible.

Add to the system an element whose security is reliably determined. Consider a system with many objects $A^0=A\cup\{a_0\}$.

Define $B_0$, the connection that establishes the security of the object: $a_1$ : $B_0(a_0)=B_0(a_0,c_{1i},...,c_{1ni})=a_1$..

Then the enumerating function of the set will be defined according to (1) as follows:

$$\begin{cases}\psi_D(0)=B_0(a_0)=a_1\\ \psi_D(i)=P_{n_{i+1}+1}^{n_i+1}(B_{i+1},B_i)=a_{i+1}\end{cases}$$

Define $\overline{D}=A^0\setminus D=\{a_0\}$. An enumeration function $\psi_D$ for a set can be $\overline{D}$ defined as an authentication function for an object $a_0$.

$\psi_{\overline{D}}(0)=a_0$, т.е. $a_0\in\overline{D}$,

$\psi_{\overline{D}}(i)=a_i$, $\{a_i\}_{i=1}^N=A$, т.е. $a_i\notin\overline{D}$ (3)

In this case, it is everywhere defined, computable, i.e. a general recursive function, therefore, the set is enumerated.

Then, by the decidability theorem, there is a decidable set; therefore, by virtue ofDefinition 1, the security of the system can be established.

From the proven statement about the use of PP follows:

*Corollary 1:* Establishment of the security of the CS is possible only with the expansion of the CS the presence of PP.

*Corollary 2:* Establishing the security of the CS is impossible only at the expense of software without the use of PP.

Let us now consider the issue of establishing protective procedures with a system described at this stage by a simple structure.

It assumes that the PP is implemented in the system as an object $a_0$.

*Statement 3*. (on the establishment of the PP in a simple system): PPs can be installed in the system with a simple structure in an arbitrary way, provided that an object is present in the system $a_0$.

*Evidence 3*. Consider the issue of establishing the security of a system object $a_k, k\le N$.

Let be $k=1$. In this case, the establishment of security of the object $a_1$ is carried out on the basis of a priori defined security of the object $a_0$. To do this, using a computable function, a connection is determined that establishes the security of the object $a_1$ : $B(a_0)=a_1$.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

Let $2 < k < N$. Then, having an object $a_0$ in the system, it is possible to establish the security of the object $a_k$ c of interest using communication $B_i(a_i) = a_{i+1}, \overline{i = 1, k-1}$ and the recursion of a certain function.

$$\psi(0) = B_0(a_0) = a_1$$

$$\psi(i) = P_{n_{i+1}+1}^{n_i+1}(B_{i+1}, B_i) = a_{i+1}, i = \overline{1, k-1}$$

$$P_{n_{i+1}+1}^{n_i+1}(B_{i+1}, B_i) = B_{i+1}(a_i, f_i(a_i))$$

where
is the superposition operator.

Similarly, to the problem for a set of system objects on a set $A = \{a_i\}_{i=1}^N$, one can determine the relationships $B_j^1(a_j) = a_{j+1}, j = \overline{1, i-1}$ and the function

$$\begin{cases} \psi^1(0) = B_0^1(a_0) = a_1 \\ \psi^1(i) = P_{n_{i+1}+1}^{n_i+1}(B_{i+1}^1, B_i^1) = a_{i+1}, i = \overline{1, k-1} \end{cases}$$

On the set $A^{11}$, we consider the problem of establishing the security of an object $a_k$. In this case, the definition of relationships $B_j^{11}(a_j) = a_{j+1}, j = \overline{i+1, k}$ and functions $\psi^{11}(j), j = \overline{i+1, k-1}$ is not enough to establish the security of objects $a_k$. The presence of an element whose security is established reliably is necessary.

As such an element, a system object $a_i$ can be selected, due to the fact that its security is the result of solving a problem for a set $A^1$.

Theorem: Whatever the Turing program $\Pi_1$ is and $\Pi_2$, a Turing program $\Pi_3$ can be effectively constructed such that for all the words under consideration $E^1 : \Pi_3(E) = \Pi_2(\Pi_1(E))$ ..
In accordance with the theorem, a sequential composition of machines and, in particular, machines, such that $T(a_1) = T^{11}(T^1(a_0)) = a_2$.

Thus, it is possible to establish the security of an element $a_k$ while relying on the guaranteed security of the object $a_i$, if $[a_1, a_i]$ it is only possible to establish the security of the segment or, what is the same, relying on the protective procedures available to the point, it is possible to establish the security of the objects $\{a_i\}_{i=1}^i$.

Due to the arbitrariness of the choice of the object $a_i$, it can be argued that the result obtained is valid for any, $i$, $1 < i < k$.

Now it will consider the introduction of PP while securing technologies with complex architecture.
The process of computer network activation is characterized by a topology, which can be represented as an ordered root tree as in Fig.1(a), $G_i$, $i = \overline{1, m}$
where, the ordered root trees.

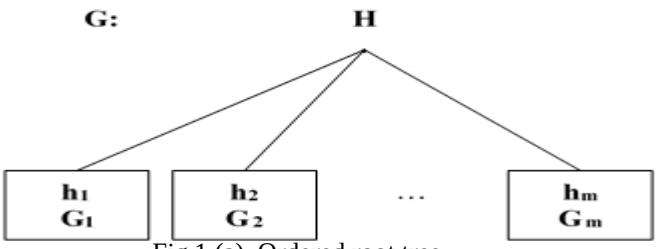

Fig.1 (a). Ordered root tree

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

The network components correspond to the top of the tree $G$. Possible connections between network components correspond to tree edges. A network component is considered activated if there are edges emanating from the corresponding tree top.
The task of establishing the security of the network in question is equivalent to the task of establishing the security of all end nodes of the tree $G$.

The process of network-consistent hierarchy of network installation is described by a directed graph $\vec{O}$, which is built from a tree $G$ by assigning to all arcs the directions from a lower vertex to a higher one (Fig.2(b)).

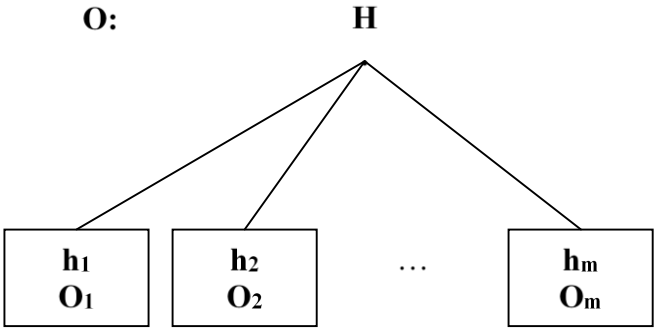


Fig.1(b).Ordered root tree

First, the network component corresponding to the root vertex of the $H$ graph $O$, is activated, then the components belonging to the second level of the hierarchy, etc. Moreover, the initialization of each network branch corresponding to one of the $O_i$, $i=\overline{1,m}$ subgraphs is carried out independently of all other network branches to which the subgraphs correspond, $O_j$, $j=\overline{1,m}$, $j \neq i$,.

Choose an arbitrary subgraph $O_i$. Choose any end vertex from the subgraph $O_i$. Denote it $h_k$. Consider a route, namely a simple target from the root vertex of a $h_i$ subgraph $O_i$ to the selected end vertex. Obviously, a simple goal is the only one. Any other route $h_i$ from $h_k$ to will contain at least one of the peaks and at least one of the edges at least 2 times, that is, such a route will not be a simple goal.

Then the considered problem of establishing $h_k \in O_i$ the security of an element corresponding to the end vertex is equivalent to the task of establishing the security of a network with a simple structure. This has been reviewed above.

Thus, to establish the security of an element $h_k \in O_i$, it is necessary to introduce special PP into the system. Moreover, the vertex will be determined for the system of PP under consideration $h_0$, and then the system with all possible connections can be represented in the form of an ordered root tree $G^1$ (Fig. 2).
At the same time, the security of the system will be monitored in accordance with the levels of the initialization hierarchy.

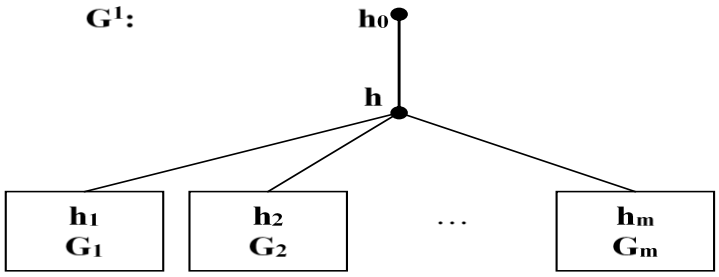


Fig.2. The levels of the initialization hierarchy

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

## IV. INITIALIZATION OF THE SYSTEM IS PERFORMED IN AN ARBITRARY ORDER

The process of such initialization is represented by a graph that contains all the vertices present in the tree $G$. Moreover, due to the arbitrary order of initialization of the system, it is impossible to talk about the presence of connections between all components - procedures. Therefore, in the general case, the statement regarding the presence or absence of any of the edges of the graph $O$ is impossible, i.e. we consider the graph $O$ to be disconnected.
Without loss of generality, suppose that several (n) sub branches are activated in the system. In the graph o, they correspond to the connected components, i.e. parts not connected to each other. Denote them $o_i$, $i=\overline{1,n}$. These components are connected graphs, namely, they have the structure of an ordered root tree. The initialization of the system branches corresponding to the connected components $o_i$, $i=\overline{1,n}$, is carried out sequentially at the hierarchy levels.
In this case, the task of monitoring the security of the system will be equivalent to the task of monitoring the security of all activated components of the system corresponding to the end vertices of the graph, i.e. end vertices of connected components $o_i \in O$, $i=\overline{1,n}$.

Itarbitraries choose one of the connected components $o_i$. Let $h_0^1$ - be the root vertex for the graph $o_i$. Then, according to the case considered in Section 1, in order to control the security of the sub-branch of the system corresponding to the graph under consideration, it is necessary to implement a special RF at the vertex $h_0^1$. Denote it by PP. Similarly, to control the security of all other connected components $o_i \in O$, $i=\overline{1,n}$, it is necessary to implement special PP in their root vertices $h_0^1$, $i=\overline{1,n}$,.
By virtue of the arbitrary choice of the connected components of the graph $O$, the following statement is valid for the placement of the PP in a system of arbitrary structure.

## V. CONCLUSION

In conclusion, it should be noted that the proposed model to increase the security of information and communication systems, taking into account the criterion of ensuring the competitiveness of the enterprise, allows to increase the state of protection against threats to violation of the information security of the enterprise.

## REFERENCES

[1] Saparova G.A., Gulomov Sh.R. Development of Specialized Method for Increasing the Level of Security on Information and Communication Systems. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2, December 2019. – P. 1821-1826
[2] Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
[3] Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016
[4] Joseph Migga Kizza. Guide to Computer Network Security (Computer Communications and Networks) (2015-02-10)
[5] Kazarin O., Shubinsky I. Reliability and security of software. Publisher: Yurayt. Year of publication: 2018
[6] Melnikov V. Information Security Textbook. Publisher: KnoRus. Year of publication: 2018

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

**AUTHOR'S BIOGRAPHY**

**Saparova Gaukhar** was born in September 25, 1983 in Nukus city, the Republic of Karakalpakstan. In 2006 graduated «Mathematics» faculty of Azhiniyaz Nukus State Pedagogical Institute. Has more than 30 published scientific works in the form of articles, journals, theses and tutorials in the field Computer networks and Cyber Security. Currently works of the department «Information Security» at the Tashkent University of Information Technologies of Nukus branch named after Muhammad al-Khwarizmi.