Formulation And Solution the Tasks of Protection the Information from Unauthorised Access

Konstantin Scheglov, Andrey Scheglov, Tatiana Markina
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint Petersburg, Russian Federation
{ska, info}@npp-itb.spb.ru, markina@cs.ifmo.ru

Abstract—**We introduce vulnerability threats classification and formulate unauthorized access prevention problem in general terms. This problem consists of lowering conditional and unconditional threats, created by vulnerability threats in implementations including programming errors discovering and technological vulnerabilities. Informational security problem solving is dedicated to informational system intrusion prevention by use of defense against actual attack threats by methods of control and access policy for subjects (users and processes) to secured objects. We formulate problems which must be solved while designing and building informational security systems against unauthorized access dedicated to prevent intrusions into informational system. We describe general way for informational system security design. With practical problems of informational systems security against modern threats examples we illustrate suggested method abilities (for building informational security systems) and how such implementation influences to developed methods and information security tools. All described technical solutions are implemented, approved and patented.**

I. Introduction

In the paper [1]: using systems of information security from unauthorized access is directed at prevention receiving protected information by interested subjects in violation of the regulatory and legal documents (acts) or owners of information or rights of restricting access to protected information - in violation of the differentiation access policy. As a consequence, the basis of the implementation of the system of information security from unauthorized access is formed by control methods and access rights mediation of subjects (users) to the objects that implement the differentiation access policy.

In the paper [2] requirement is formulated for the design of modern systems of information security, as the security systems, aimed at the solution of the problem of protection against actual threats of attacks.

At first sight, this is different, in fact, in its formulation; the problem of information security is unrelated with protection against unauthorized access to information. As there are a number of conditions under which can unauthorized access implement to the information that is processed bypassing realized differentiation access policies. As an example: it allows us to identify vulnerabilities in operating systems and applications created by errors in software. However, the solution of the problem of protection against actual threats of attacks does not contradict the general formulation of the problem of information security from unauthorized access [1]. It's because of that it reduced the implementation of protection against unauthorized access to information carried out for the violation of the rights and (or) access rules. Therefore, the problem of protection against actual threats of attacks can be positioned as the task of protecting information from unauthorized access. Another thing is how to solve a given interpretation? We will answer this key question in this paper. This question is key, because the answer to this question will allow to formulate a statement of the problem of protection from unauthorized access in general and to identify approaches to its solution.

II. Tasks and Methods of Implementation of the Differentiation Access User Policy to Protected Resources of the Information System

Today in practice, the implementation of a differentiation policy of access of subjects (as subjects - users) to protected resources of information system (objects) is based on using of one of the corresponding abstract models of access control [3,4]. Today the most widely used models of discretionary access control (used in modern universal OS) and mandatory access control. Discretionary (sometimes also called as selective) access control (DAC) based on implementation of the model «Harrison-Ruzzo-Ullman» [3]. In this case the basis of the construction of the differentiation access policy is the task for administrator to create access matrix (a list of rules for access of subjects to objects, or conversely - to the objects of the subjects that is realized transposition access matrix).

Discretionary access control method can be implemented with random, or forced control the flow of information for members (depending on whether the non-privileged user is as the «owner» of the created object or not) [5]. Mandatory access control (MAC) is based on the realization of an abstract model of «Bella – LaPadula» [4]. This is an access control with forced control the flow of information. It is based on the formalization of the rules using security labels (mandates) - numerical values that reflect the appropriate levels of security actors (access levels) and objects (levels of privacy) in a given hierarchy. A certain level of security is assigned for each subject and object of the system; it is assigned to a security label. The implementation of a differentiation policy of access involves arithmetic comparison of the marks and is based on the initially specified rules.

With a view to the implementation of a differentiation access policy, which is based on the application of the discretionary access control method and/or mandatory access control methods, we can use role-playing [6] and in-session [7] access control models. Role-Based Access Control model (RBAC) is used to generate user-mode process information as part of their role in the information system in order to provide to the user with access rights that are only to the necessary facilities. Session access control model is used for the formation and separation treatment regimens on the one machine (in general case - in the information system) with the same user the information of different levels of confidentiality, to protect against the leakage of confidential information by processing them on the on machine in a completely other (less secure) open mode or a lower level of confidentiality of information (separation modes of information processing are implemented in order to protect from lower categories of confidentiality of information processed by means of the transfer of her one way or another less secure processing mode - in the mode of processing less sensitive information). As you can see, in the formulation and solution the problems of implementation the differentiation access policy from subjects to objects are no question about protection against actual threats of attacks.

At the same time, today the necessity of solving the problem of protection against actual threats of attacks, there is no doubt, therefore, try to solve it. But they use completely different methods. For example, this has led to the emergence of so-called detection systems (detection and prevention) intrusion, IDS (will not be confused with the IDS - the intrusion is already the result of an attack)[8], They are based, in relation to our problem of protection, on an analysis of audit logs of system tools and applications in order to identify on definable rules log analysis of suspicious events, classified the relevant rules as a possible intrusion (or attacks by the heuristic analysis - analysis of pre-defined rules set of events, characterized as an intrusion).

The principal disadvantages of IDS are fairly obvious and known (it cannot be protected in real time - the intrusion prevented already on the fact their detection, high utilization of computing resources - the need to maintain the set of audit logs and analysis, and it could be the maximum operational, otherwise this approach to the protection does not make any sense, the complexity of the administration of the corresponding system of protection – it is boring to set the audit rules, the rules of their control, especially heuristic analysis, etc.). However, for lack of a better approach to solving this problem of protection, these systems are actively developing.

Another example is the so-called, DLP-solutions (Data Loss Prevention and Data Leak Prevention) [9]. These programs are addressed to solve the problem of protection against data loss. Here again, the methods of control (under appropriate their flaws) are solved actual problems of protection - in this case it is implemented protection against theft of information by authorized users (monitored for compliance with the rules given by) emanating from the protected computer information. However, over time, corresponding to the evaluation of the effectiveness of the approaches to the protection has led to a revision of the positioning of these systems. Now we are talking about applying them in the first place, to prevent leaks of information related to negligence of employees (authorized users), which is understandable to convert background information prior to its deliberate theft. Naturally, it is quite a different problem of information security.

III. Classification of threats vulnerabilities. Statement and general approach to the problem of protecting information against unauthorized access

We introduce a classification of threats vulnerabilities that pose a threat of attack.

Definition. Under the threat of technological vulnerabilities of information systems in general, we understand the technological disadvantages of its construction, including a lack of required functions of information security or incorrectness of their implementation, that do not allow to fully implement protection against unauthorized access - implement the necessary rights and (or) rules of the authorize access to information and (or) prevent access to the violation of the rights and (or) access rules.

Assume that the system has no such technological disadvantages. However, under these conditions, to some extent there is a threat to the security of information systems, but for other reasons. In this case, the attacker can already use the threats related to implementation errors (for example, programming errors, such errors allow to make a SQL-injection) system resources and applications.

As an illustration, consider some examples of actual attacks that exploit vulnerabilities threats. For example, the attack on elevation of privileges [10] is associated with the possibility of execution on a computer file created by interactive user with system privileges. Certainly, in the normal mode of operation (without creating appropriate conditions) - the nominal opportunity - the possibility of execution by the system user-created files cannot be regarded as a technological vulnerability - a mistake or incorrect implementation of protection, however, the detection (on condition) corresponding programming errors in system tools (in the relevant components of the system [11]), this possibility can already be seen as a threat of technological vulnerability.

Another example you can see. In modern systems, there is no possibility to set different access rights to objects of different processes run out of the same account (user) - all executable from the same account (user) inherits permissions to objects that account (user). Again, in the normal mode of functioning (without the occurrence of corresponding conditions) - the possibility cannot be considered as a processing vulnerability - as any error or incorrect security implementation. However, when it is detected (under condition) of the respective programming errors in this case primarily in applications [12]. This feature can already be seen as a threat of technological vulnerability.

Such examples are many, but common to them is that some property of the system or application that is not a technological vulnerability provided regular functioning of the system and applications, it becomes such a vulnerability in the event of certain conditions, including the detection (at condition detection) of the corresponding programming errors in the system tools and applications. It is important that, as we see, like technological vulnerabilities in these conditions can already be seen as disadvantages of implementation differentiation access policy. With that said, we can make the following very important conclusion.

With that said, we introduce the following definitions.

Definition. Under the threat of unconditional technological vulnerability we understand the threat of technological vulnerabilities presents in the system without incurring any additional conditions.

It was to prevent threats to undoubted technological vulnerabilities in the construction of secure information systems should be formulated requirements for the correct implementation of methods of protection of information (requirements for design of secure systems).

Definition. Under the threat of conditional technological vulnerability we understand the threat of technological vulnerability that occurs in the system in the event of certain additional conditions, without which corresponds to the nominal capacity of the system does not pose any security threat.

Note that conventional technological vulnerabilities can be related to the widely used practice of nominal possibilities of modern applications to extend their functionality by using macros, scripts, etc. The threat of these vulnerabilities is associated with the possibility of granting respective application harmful properties [13].

Definition. Under the threat of the vulnerability of implementation, we will realize the error in the implementation of the information system used in the media, or some nominal capability of the system and applications, creating conditions that carry the creation (development) conditional threat of technological vulnerability.

Definition. We say that the information system «completely unprotected» in the presence therein of at least one known unconditional technological vulnerability that allows unauthorized access to realize the processed information in it; that the information system «has a basic level of security» in the absence of her unconditional technology known vulnerabilities; we say that the system is «hypothetically perfectly protected» in the absence of her famous unconditioned and conditioned technological vulnerabilities (respectively known threats posed by vulnerabilities implementation).

Comment. It is hypothetically ideal because we can talk about the lack of known threats, vulnerabilities realization only at a particular time, including time on moment constructing information security systems.

Thus, in order to construct a secure information system («hypothetically perfectly protected») it must be neutralized threats as unconditional and conditional technological vulnerabilities.

Definition. Under neutralized threat of the technological vulnerabilities in general, we understand the implementation of technical measures to prevent any possibility of the creation of this threat vulnerability threat of attack or (if technical unrealizability such decision) to reduce the potential losses from the sale of the attack, operating this threat vulnerability.

Comment. Certainly, the level of vulnerability threat to the implementation of a system of information security is not possible - the correction of corresponding errors in software is the task of the developers of the software. Another thing is that neutralizing the conditional technological vulnerabilities are identified relevant threats to the implementation of vulnerability does not pose a threat to the implementation of the corresponding attacks.

As an example unrealizability of the neutralized threat of conventional technological vulnerability could cause the possibility of granting the application or system process as a result of harmful properties identified in this software means programming errors (threat vulnerability implementation). Reducing potential losses from the implementation of the attack, operating this threat vulnerability can be achieved implementation process model of access control [12,13], based on the implementation of a differentiation access policy to the subject of the access process, with access to critical processes defined using a probabilistic model of access control [12, 13], should be insulated. In particular, they must prevent access to confidential data - for objects created by other applications [14], in general, to protect system objects (file objects and registry objects of OS) [15].

All that said can be formulated in general terms the task of protecting information from unauthorized access.

Definition. The challenge of protecting information from unauthorized access can be solved in order to prevent obtaining protected information subjects concerned in breach of the regulatory and legal documents (acts) or owners of information or rights of differentiation access to protected information. In general, involves neutralization threats of unconditional and conditional technical vulnerabilities by system of protection against unauthorized access.

Pay attention to this key definition that follows from the above classification of threats introduced vulnerabilities. In fact, this formulation in general terms the task of building systems to protect information from unauthorized access in the present conditions, defining their purpose, outline the range of problems solved by them functional protection. Solution of the problem in this formulation allows building information security from threats of actual attacks.

All of the above makes it possible to determine the general approach to the construction (not the design, it is assumed mandatory use of mathematical modeling) systems to protect information from unauthorized access in this formulation of their tasks of protection:

- Analysis of the architectural features of the system and the software used in the protected information system, to identify the unconditional and conditional processing of potential vulnerabilities. Potential conditional technological vulnerabilities - a property of the system and applications, with the potential (under certain conditions - in this case, it does not matter under what conditions) may be used by an attacker to implement the attack on the protected system. Development of methods and means of control and access rights differentiation, aimed at neutralization the technological vulnerabilities identified;

- Analysis of the threats identified vulnerabilities implementation used in the implementation of successful attacks unauthorized access (for this purpose can be used by relevant statistics, continuously waged against identified threats vulnerabilities), to determine the conventional technology vulnerabilities, which were in this case (if the identified vulnerabilities implementation) used by an attacker to carry out a successful attack on an information system. Development of methods and means of control and access rights differentiation, aimed at neutralization identified technological vulnerabilities.

Important in solving the problem of information protection from unauthorized access to the proposed its formulation is that, since the intrusion of an information system priori possible only with the use of a particular technology vulnerability solution to the problem of neutralization the technological vulnerabilities is intended to protect against intrusion into an information system (note not on Intrusion Detection, namely to protect against intrusion), as protection from actual threats of attacks.

IV. Examples of building protection system for solving the problem of protection against its unauthorized generally

As noted, the task of neutralization the unconditional technological vulnerabilities is the formation and execution of the construction of systems of information protection from unauthorized access to formulate requirements for the implementation of a differentiating policy of access to part of the construction of a secure system. This approach to the construction of systems of information protection a brief look at the example of the formation of the requirements in the implementation of access control session. In [7] there is justification for the fact that as a subject access demarcation policy should serve the essence of «User» - user names (accounts) should be assigned a security label, not some virtual entity «session» - for the staff in the different modes it We have created different accounts (if for the formation of modes of information processing in different sessions use the same account, there is a need to separate between sessions - for a single account, all file objects, in which the rights of the user mass is recorded configuration and data, and other necessary them for information applications). It is clear that it is almost an impossible task. Questions of formation of modes of information processing of different levels of confidentiality, including implementation issues key to the correct solution of the problem of protection method of mounting local devices of users and issues (conflict) destination secure labels of devices (the conclusion that the abstract model of [4] is applicable only to file objects) are studied in [16]. Questions of correct implementation of separating the access policy (separation sessions - modes of information processing of different levels of confidentiality) are studied in [17], resulting in the conclusion that for the solution of the problem of protection the best is to use the method of mandatory access control to created file, as in its implementation of any file created, including created and nonshared by system and application directories automatically inherit the security label of the account to which it was created (including, it applies to the configuration files created by applications). In [18,19] the requirements to the implementation of a differentiating policy of access, including the correctness analyzed mandated access control rules to create the file, shows that the correct (called in [19] «consistent») is typically non-hierarchical processing (comparison solely on equality / inequality) hierarchical (appointed by taking into account the hierarchy level of confidentiality of processed information) security labels. Such research can continue, but at this stop, because it is important in this paper is not a review of the requirements for building a secure system for solving a problem of information security, and illustrate the need for this. Do not perform any of the claims review process poses a threat to the unconditional technological vulnerability of the execution is intended to neutralize such threats.

Certainly, the correct (in terms of implementation of the relevant requirements for the construction of protected system) implementation of the session access control to prevent leakage of confidential information, including, and its intentional theft, as the information of each level of confidentiality will be treated in its operation, with a positive user-controlled system Protection of information flows in each session and between sessions. By the way, look at how, in practice, often implemented mandatory access control - not that any requirement to build secure systems developers are not formed, but in general it is not clear why it is implemented in the system of protection as on the formation, and especially about the division of modes of information processing of different levels of confidentiality it is not carried out, as the absence of the in-session access control model [7], as such.

Now, let's speak about the task of neutralization threats conditional technological vulnerabilities. Again, we can give a few examples.

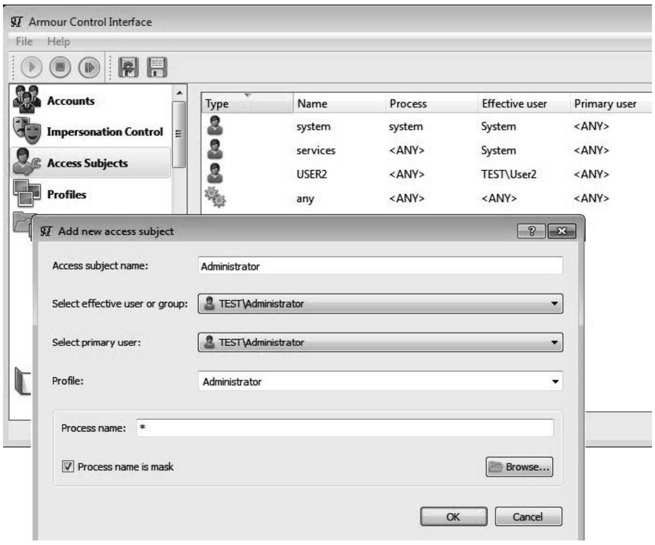
First of all, let us consider a simple example, how to identify such threats vulnerabilities. To do this, we turn again to consider the threat to privilege enhancement attacks [10]. As noted, the implementation of this attack involves the introduction of a computer with the rights of an interactive user malware (unconditional technological vulnerability), implies the existence of a specific vulnerability in the system component [11] - the threat of the vulnerability of implementation (a programming error in the system software), which allows to run with the system the rights of malicious program - that this is a threat to the conventional process of vulnerability. Thus, the task of identifying conventional technological vulnerabilities is to analyze implemented attacks (such information publicly available is sufficient) to use the threat of vulnerabilities implementation, including the identified programming errors, in order to determine the manner in which itself was implemented unauthorized access (identified vulnerabilities implementing some way must be used), and thereby it was not prevented by the protection system. In the above example - is the inability to differentiate access rights for execution creates an interactive user file system (for regular users).

To implement the process model of access control that let to isolate the work of the system-critical applications [14] (this problem was considered earlier). As the subject of access to the differentiation policy should be used entity of the «process» to allow the one remedy - a differentiating access policy implement and role, and process model of access control - the entity of «user process» [20]. With a view to the neutralization the threat of obtain the access to protected resource under a different user [21] - the entity of «the original user, process, the effective user» [22]. If we talk about neutralization the actual threat received by the user rights of a user on the system, including, in order increasing benefits, must be addressed to protect individual task - control and access rights to services impersonation. [23] To protect against the threat of executing malicious software, including executing with system privileges (protection from the threat of privilege elevation using identified vulnerabilities implementation in system components) must implement the requirement to prohibition the execution to create interactive user files [24], to protect from modification legal files for the purpose of granting malware properties, executed files should automatically mark up, after which it must prevent write/modify/rename/delete access that implemented the technical solution [25]. As a serious threat carries an investment applications malicious properties when they read the relevant malware file (such as an applet), illegally installed on the protected computer, like installing the appropriate files can be prevented [26].

This list of resolved tasks to protect information from unauthorized access, in terms of neutralizing it threats of conditional technological vulnerabilities can be continued, but focus on the examples above. We focus our attention on the task of neutralization the threat of vulnerability as the problem of protection from intrusion. Naturally, when the threat of technology vulnerabilities is neutralized, intrusion system - Implementation an attack is not possible by using this vulnerability. However, not all vulnerabilities may neutralize the threat. First of all, such threats include application vulnerabilities created by errors detected in these programming. Implementation of the protection of information from unauthorized access, you can reverse the effects of the implementation of such threats. You can realize it for such applications process model of access control, deciding in its implementation of the following tasks of protection - prohibit execution of created files, prohibit access to files (including a configuration files and files that are generated in other applications), prohibit access to the relevant system objects (file and registry objects of OS), etc. However, the fact of intrusion will be presented. In the result «infected» application can be used more than once in order to implement any of attack, and repeatedly attempting to implement various attacks. The fact of the intrusion («infection» of applications) will be registered by auditing system of protection at the first attempt the implementation of the attack (the process will be denied appropriate unauthorized access). But to prevent detected intrusion, in this case, as an additional (optional to audit) it will be automatic response to detection of intrusion - to forcibly terminate «infected» process (a process that has made unauthorized access) [27].

It should be noted that the task of neutralization threats from conditional technological vulnerabilities is a radically new in its formulation, the problem of information security from unauthorized access (which cannot be said about the task of neutralization unconditional technological vulnerabilities - it is the task of constructing the correctness of information security system in its classical formulation). As a consequence, for solution of this problem it is necessary fundamentally new methods of protection. To illustrate this, we have given the appropriate links on the patented technical solutions.

Subject to the complexity of solving such problems the key task is developing protection methods aimed at simplification the administration of security systems. Also the solution of this problem leads to a fundamental changes of approaches of the implementation of protection. Let us illustrate this in example. The subject, set by the three entities, for example in the security system [28] you can create it in the interface Fig.1.



Type	Name	Process	Effective user	Primary user
	system	system	System	<ANY>
	services	<ANY>	System	<ANY>
	USER2	<ANY>	TEST\User2	<ANY>
	any	<ANY>	<ANY>	<ANY>

Access subject name: Administrator

Select effective user or group: TEST\Administrator

Select primary user: TEST\Administrator

Profile: Administrator

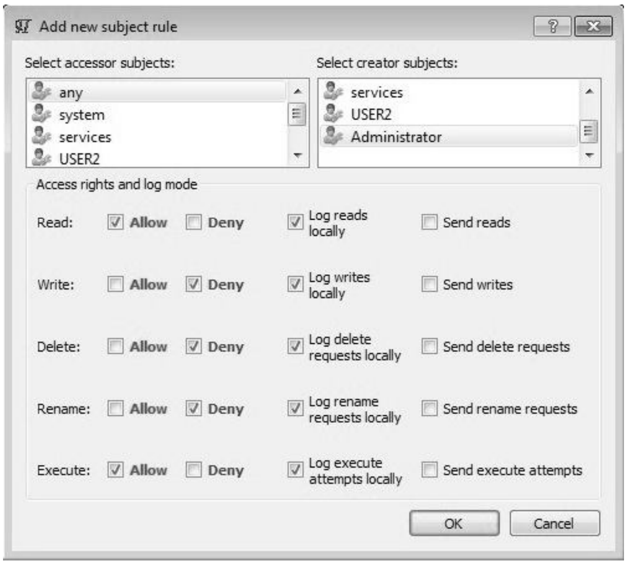
Process name: *

☑ Process name is mask

Fig.1. The interface of access subjects

Configuration the differentiation access policy like in Fig.1 is rather difficult [15]. This required the development of a fundamentally new method of access control method to the created objects (file objects and data temporarily placed into the clipboard). The gist of the method is that when an object is created it user account information (the corresponding identifier of the subject defined by three entities, see Fig.1) is automatically placed into object (the object is marked) [29, 25]. As a result, in the differentiation access policy is specified not which subject to which object has permissions, but which subject to created by which subject whom permissions has. The interface of the differentiation access policy to file objects is shown in Fig.2 [28].

The interface of the differentiation access policy to data temporarily placed into the clipboard, in Fig.3 [28].



Add new subject rule

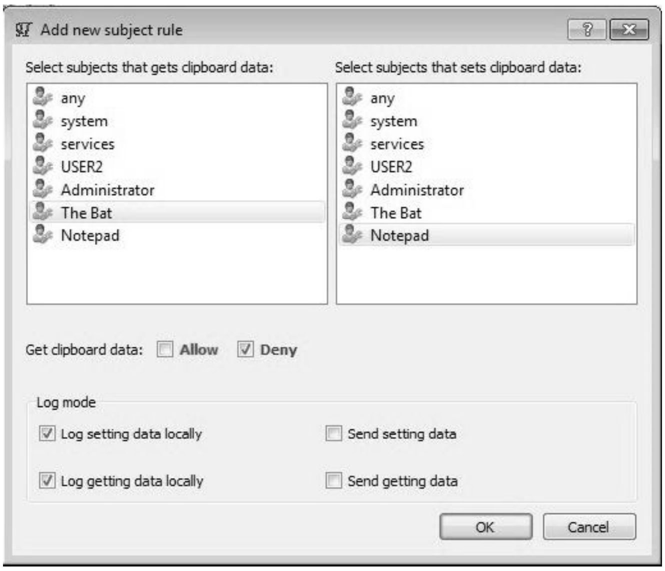
Select accessor subjects: any, system, services, USER2

Select creator subjects: services, USER2, Administrator

Access rights and log mode

Read:	☑ Allow	□ Deny	☑ Log reads locally	□ Send reads
Write:	□ Allow	☑ Deny	☑ Log writes locally	□ Send writes
Delete:	□ Allow	☑ Deny	☑ Log delete requests locally	□ Send delete requests
Rename:	□ Allow	☑ Deny	☑ Log rename requests locally	□ Send rename requests
Execute:	☑ Allow	□ Deny	☑ Log execute attempts locally	□ Send execute attempts

Fig.2. The interface of the rules of access to created files



Add new subject rule

Select subjects that gets clipboard data: any, system, services, USER2, Administrator, The Bat, Notepad

Select subjects that sets clipboard data: any, system, services, USER2, Administrator, The Bat, Notepad

Get clipboard data: □ Allow ☑ Deny

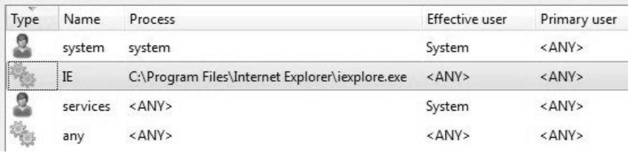
Log mode

☑ Log setting data locally □ Send setting data

☑ Log getting data locally □ Send getting data

Fig.3. The interface of the rules of access to data placed into the clipboard

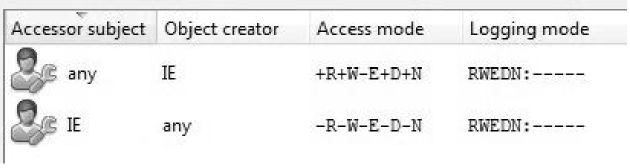
Consider using this method of protection for isolation the operation of any applications. It is illustrated in Fig.4, Fig.5. There only two rules in politics are isolated the access to the processed data on the computer and to the Internet browser [14].



Type	Name	Process	Effective user	Primary user
	system	system	System	<ANY>
	IE	C:\Program Files\Internet Explorer\iexplore.exe	<ANY>	<ANY>
	services	<ANY>	System	<ANY>
	any	<ANY>	<ANY>	<ANY>

Fig.4. The created subjects

As you can see, as a result of implementation of the proposed approach to design of information security system from unauthorized access in a general the method of access control is developed. This method is fundamentally differed from known methods.



Accessor subject	Object creator	Access mode	Logging mode
any	IE	+R+W-E+D+N	RWEDN:-----
IE	any	-R-W-E-D-N	RWEDN:-----

Fig.5. The access rules

VII. Conclusion

In conclusion, we note that the main result of this work is the formulation of the task of protecting information from unauthorized access in general. It is aimed at solving the problems of neutralization threats of unconditional and conditional processing vulnerabilities solution which enables fundamentally enhance the ability of systems to protect information from unauthorized access, for means of implementation of protection from actual threats of attacks, including threats posed by attacks vulnerabilities in the system and application software, and that fundamentally changes the approach to the construction of such systems of information protection. Finally, we note also that all the methods of protection, which are described, are implemented and tested in the construction of commercial systems of information security from unauthorized access [28].

References

[1] GOST 50922-96. Data protection. Basic terms and definitions.

[2] Methods of determining the actual threat of personal data security at their processing within the information systems of personal data. FSTEC Russia, 2008.

[3] M. A. Harrison, W. L. Ruzzo, J. D. Ullman, *Protection in operating systems,* Communication of ACM, 1976.

[4] D.E. Bell, L.J. LaPadula, *Secure Computer Systems: Unified Exposition and Multics Interpretation*. Rev. 1. US Air Force ESD-TR-306. MTR-2997. MITRE Corp. Bedford, MA. March 1976.

[5] A.U. Shcheglov, *Protecting the computer from unauthorized access.* St. Petersburg: Science and Technology, 2004.

[6] R. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, “Role-Based Access Control Models”, *IEEE Computer (IEEE Press)*, 29 (2), Aug. 1996, pp. 38-47.

[7] K.A. Shcheglov, A.U. Shcheglov, “Method session control access to file objects. Questions of practical implementation”, *Herald of computer and information technologies,* No. 8, 2014, pp. 54-60.

[8] James P. Anderson, *Computer Security Threat Monitoring and Surveillance*, James P. Anderson Co., 1980.

[9] PCWEEK official website, V. Vasiliev, DLP market is experiencing a crisis of confidence, Web: http://www.pcweek.ru/security/article/detail.php?ID=135206.

[10] K.A. Shcheglov, A.U. Shcheglov, “Protection against attacks on privilege escalation”, *Herald of computer and information technologies,* No. 1, 2015, pp. 36-42.

[11] HABRAHABR official website, The results of the 2013: the threat of exploitation and Windows, Web: http://www.habrahabr.ru/company/eset/blog/209694/.

[12] K.A. Shcheglov, A.U. Shcheglov, “Protection against attacks on vulnerable applications. Access control model”, *Problems of information security,* vol. 101, No. 2, 2013, pp. 36-43.

[13] K.A. Shcheglov, A.U. Shcheglov, “Protection against attacks from applications vested malicious functions. Access control mode”l, *Problems of information security,* vol. 99, No. 4, 2012, pp. 31-36.

[14] K.A. Shcheglov, A.U. Shcheglov, “Technology isolated data critical applications”, *Questions of information security,* vol. 108, No. 1, 2015, pp. 15-22.

[15] K.A. Shcheglov, A.U. Shcheglov, "Access control to a static file objects", *Questions of information security*, vol. 97, No. 2, 2012, pp. 12-20.

[16] K.A. Shcheglov, A.U. Shcheglov, "The method of mounting devices for users", *Herald of computer and information technologies*, No.8, 2015, pp. 40-45.

[17] K.A. Shcheglov, A.U. Shcheglov, "Practical implementation of mandatory access control to files created", *Herald of computer and information technologies,* No. 6, 2014, pp. 50-54.

[18] K.A. Shcheglov, A.U. Shcheglov, "Models and rules of mandatory access control", *Herald of computer and information technologies,* No. 5, 2014, pp. 44-49.

[19] K.A. Shcheglov, A.U. Shcheglov, "A consistent model of mandatory access control", *Bulletin VUZov. Instrument,* vol. 57, No. 4, 2014, pp. 12-15.

[20] A.U. Shcheglov, K.A. Shcheglov, "Access control to resources of a computer system with a subject access "user process"", Patent for the invention No. 2534599.

[21] K.A. Shcheglov, A.U. Shcheglov, "Methods for identification and authentication of the user when accessing the file objects", *Herald of computer and information technologies,* No. 10, 2012, pp. 47-51.

[22] A.U. Shcheglov, K.A. Shcheglov, "Access control to resources of a computer system with the subject "source user, effective user, the process"", Patent for the invention No. 2534488.

[23] K.A. Shcheglov, A.U. Shcheglov, "The method of control and allocation of access rights to services impersonation", *Herald of computer and information technologies,* No. 3, 2015, pp. 48-54.

[24] K.A. Shcheglov, A.U. Shcheglov, "Protection from malicious software method to control access to the created file objects", *Bulletin of computer and information technology*, No. 8, 2012, pp. 46-51.

[25] K.A. Shcheglov, A.U. Shcheglov, "System of access control to files based on their automatic markup", Patent for the invention No. 2524566.

[26] T. A. Shibaeva (Markina), A.U. Shcheglov, A. A. Ogoluk, "Protection implementation and launch malicious programs", *Questions of information security*, vol.93, No. 2, 2011, pp. 26-35.

[27] K.A. Shcheglov, A.U. Shcheglov, "Detection system and intrusion prevention-based access control to resources", Patent for the invention No. 2543564.

[28] A.U. Shcheglov, I. P. Pavlichenko, S. V. Kornetov, K. A. Shcheglov, "Comprehensive system of information protection "Armor+" for Microsoft Windows", The Certificate for computer program No. 2014660889.

[29] K.A. Shcheglov, A.U. Shcheglov. "Principle and methods of access control to newly created file objects", *Bulletin of computer and information technology,* No. 7, 2012, pp. 43-47.