сепаратор. Такий апарат поєднує високий тепломасообмін і відносно невеликий гідравлічний опір. Але раціональні параметри контактних повітроохолоджувачів визначено тільки для номінального режиму роботи турбокомпресора при нормальних початкових умовах, тому необхідні додаткові дослідження для встановлення параметрів контактних повітроохолоджувачів при режимах відмінних від номінальних.

В подальшому планується проведення досліджень які полягають у визначенні раціональних параметрів контактного повітроохолоджувача для всіх режимів роботи турбокомпресора, та удосконаленню конструкції контактного повітроохолоджувача.

Список літератури

1. **Трегубов В.А. Замыцкий О.В.** Оценка энергопотерь от нарушений температурных режимов турбокомпрессорных установок. Гірнича електромеханіка та автоматика 2. Дніпропетровськ.1999. № 61. С. 130-132.

2. **Мурзин В. А., Цейтлин Ю. А**. Рудничные пневматические установки. Недра.1965. 312 с.

3. **Мурзин В. А., Цейтлин Ю. А.** Турбокомпрессоры в горной промышленности. Госгортехиздат. 1962. 72 с.

4. **Мурзин В. А., Цейтлин Ю. А.** Определение экономически целесообразной периодичности очистки промежуточных воздухоохладителей шахтных турбокомпрессоров. Горная электромеханика и автоматика.1980. Вып. 36. С. 65–68.

5. **Мурзин В. А., Цейтлин Ю. А.** Упрощенный пересчет характеристик турбокомпрессоров при промышленных испытаниях их. Изв. вузов МВ и ССО. Энергетика. 1962. № 11. С. 21-25.

6. **Мурзин В. А., Цейтлин Ю. А.** Рудничные пневматические установки. Недра. 1965. 312 с.

7. **Степанов А. И.** Центробежные и осевые компрессоры, воздуходувки и вентиляторы. Пер. с англ.– М.: Машгиз, 1960.–342 с.

8. **Борохович А. И., Борохович Б. А., Закиров Д. Г.** Оптимальный срок очистки промежуточных пленочных холодильников поршневых компрессоров от осадков. Изв. вузов. Горный журнал. 1985. № 2. С.61–65.

9. Центробежные компрессорные машины. **Ф. М. Чистяков** и др.; под ред. Ф. М. Чистякова. Машиностроение, 1960. 327 с.

10. **Рис В. Ф**. Центробежные компрессорные машины. Машгиз. 1951. 245с.

11. **Носырев Б. А., Рыбин А. А.** Математическое моделирование систем охлаждения шахтных компрессорных установок. Изв. вузов. Горный журнал. 1992. № 1. С. 92–95.

11. **Мишин Д. С., Прасс И. Г., Пунтусов А. П.** Термодинамический анализ работы концевого холодильника компрессора К250-61-1. Труды ЛПИ им. Калинина. Центробежные компрессорные машины. Энергомашиностроение. 1962. № 221.С. 106–109.

12. **Шерстюк А. И.** Компрессоры. Госэнергоиздат, 1959. 191 с.

13. . **Куцепаленко В.Ф., Кабаков А.И., Тихонов Б.А.** Повышение эффективности охлаждения сжатого воздуха в компрессорах. Известия Томского ордена октябрьской революции и ордена трудового красного знамени политехнического института имени С.М. Кирова.1972. № 227.С. 119-124.

14. **Замыцкий О.В.** Анализ способов охлаждения при производстве сжатого воздуха для горных машин. Горный информационно-аналитический бюллетень. МГГУ. 2001. №10. С.67-70

15. **Замыцкий О. В.** Контактное охлаждение сжатого воздуха в турбокомпрессорах. Вісник Криворізького технічного університету.2005. №17. С. 285-288.

16. **Замыцкий О. В.** Моделирование характеристик центробежных турбомашин. Сб. научн. тр. Национальной горной академии Украины. Том 3. Дніпропетровськ: Навчальна книга, 2002. № 13.С.33–36.

17. **Замыцкий О.В.** Выбор параметров контактных воздухоохладителей рудничных турбокомпрессоров. Вісник Криворізького технічного університету: Зб. наук. пр. Вип. 6. Кривий Ріг: КТУ, 2005. С.85-88

Рукопис подано до редакції 10.11.2021

UDC 004.056.53

N.O. KARABUT[·], O.H. RYBALCHENKO, I.O. DOTSENKO, Senior lecturers
Kryvyi Rih National University

PROTECTION TECHNOLOGY OF DATA PROCESSED IN DISTRIBUTED INFORMATION SYSTEMS

Purpose. To solve the problem of protecting information from unauthorized access in any information system which is based on control and delimitation of access rights of subjects to protected objects, primarily to file objects designed to store processed data.

Research methods. The implementing access control is to use one of the abstract models like discretionary, mandated and role-based access control.

Scientific novelty. An innovative approach to protecting data processed in distributed information systems through the methods of access control to the objects being created – to the file objects and to the clipboard. Those allow to exclude the access object from the delimiting policies because of automatic markup of created objects.

Practical significance. Practical implementation of this approach, provided that the markup (created attributes) directly in the created file allows to identify and solve the problem of implementing the delimiting policy of access to data processed in a distributed information system by considering different ways of data exchange between components of a similar system. This implements data flow management within the system.

Results. The considered data protection technology in the information system based on the use of access control methods allows: to get a new property of delimiting access policy in a distributed information system by using different methods of data exchange between components/computers; to increase the efficiency of the information security system by managing data flows in the system.

Key words: distributed information system, data protection, unauthorized access, control and delimitation of access rights, delimiting policy, object created, data flow management.

doi: 10.31721/2306-5451-2021-1-53-112-118

Problem statement. Protecting information from unauthorized access in any information system is based on control and delimitation of access rights of subjects to protected objects (access control), primarily to the file objects, since they are designed for storage of processed data. There are different ways of exchanging data - files- between the components (computers) of the distributed information system.

This determines the urgency of managing data flows in a distributed system, when transferring a file from one computer information system to another the access rights to the file are transferred with it. As a result, the other computer has the rights set by the delimiting access policy to files transferred between computers. The delimiting access policy should be set within the system, not a single component (computer) of the distributed information system. Since encryption is the widely used method in the practice of additional protection of data processed in the information system, it applies to cryptographic data protection aimed at managing encrypted data flows in a distributed information system.

Analysis of the recent research and publications. Principles of access control to the created objects.

Access control is to use one of the relevant abstract models [1, 2].

Currently, the most widely used models are discretionary, mandated and role-based access control.

Discretionary Access Control (DAC) implies the Happison-Puzzo-Ullman model [3]. The basis for constructing a delimiting access policy is the task of the administrator of the access matrix including the rules of subject-to-object/object-to-subject access. The task is implemented by transposing the access matrix. The DAC method can be arbitrary or forced for users to manage data flows depending on whether the unprivileged user is included as the "owner" of the created object in the administration scheme [4].

Mandatory Access Control (MAC) is based on the abstract Bella-LaPadula model [5]. The access control with forced management of information flows is based on the formalization of the task, rules under security labels (mandates) - numerical values that reflect the corresponding security of subjects (access levels) and objects (privacy levels) in a hierarchy. Each subject and object of the system is assigned a certain security - a security label. The delimiting access policy involves an arithmetic comparison of the labels based on the original specified rule.

The idea of *Role-Based Access Control* (RBAC) [1] lies in the maximum approximation of the logic system to the real division of personnel functions in the organization. The method defines roles in the system as a set of actions and responsibilities associated with the activity. In fact, the role model is discretionary access control in implementing the relevant group access policy (delimiting policy for user groups). The advantages of this model include the possibility of a certain formalization of roles, hence, the possibility of setting and further replicating some typical delimiting access policies for the respective roles. Thus, the basic ones include abstract models of discretionary and mandated methods of access control.

Objectives of the article. Here, both the existing abstract models of access control and technical solutions that implement them use two equal entities - the subject and object of access. The purpose of the rules involves what access rights subjects to objects (or vice versa) have. The subjects of access in the delimiting policy are users identified by accounts in relation to users to the rules set, the actions that might cause harm.

Presentation of the main research and results. The tasks of data processed protection in the information system include the protection of user-generated objects (files and clipboard), since the objects are to store data processed in the system. This focus on the completely new approaches and new methods of access control that eliminate the shortcomings of known methods for solving this problem. [6].

The proposed principles of access control to the created objects [6] are based on their automatic markup when creating or modifying an object. Also, they eliminate the essence of access object from the delimiting access policy. They are as follows:

the "object" is excluded from the access control scheme, when the delimiting policy uses two entities: the subject identifier (account information) created by the object, and the subject identifier requesting access to the created object;

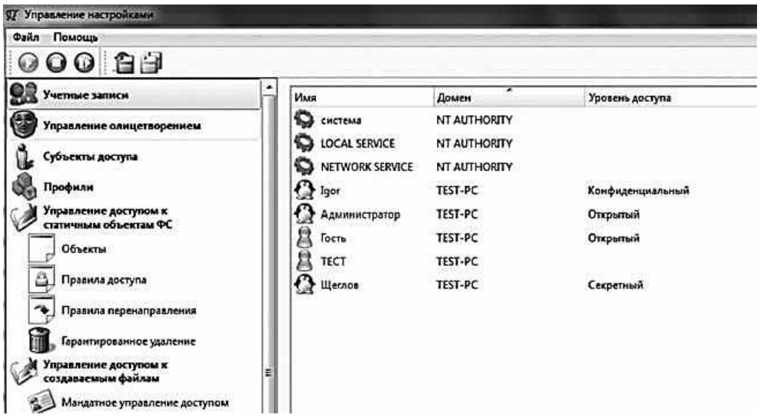
access rules are established between: access subject (account information) requesting access to the object, and access subject (account information) that created this object;

when creating /modifying the subject of the object, the object gets the account information of the access subject, who created this object - the object is marked (account information of the subject is stored in the attributes of the object created);

when requesting access to any object, the access manager (a key element) receives the markup of the object, reading its attributes, and analyzes the request for irreversibility of the specified access rules, resulting in the requested entity access to the object or refuses it.

Thus, the delimiting policy is implemented (access rules are set) between access subjects to objects created by them, not subjects to objects.

The access control to created objects. The Mandatory Controls Access method to created files. The security labels (access levels) or mandates are assigned exclusively to (interactive) users [8]. The access level can be set /selected for any user entered the system. However, only file creators receive security labels, access to which is controlled and delimited (data processed by the users is to be protected).



Имя	Домен	Уровень доступа
система	NT AUTHORITY	
LOCAL SERVICE	NT AUTHORITY	
NETWORK SERVICE	NT AUTHORITY	
Igor	TEST-PC	Конфиденциальный
Администратор	TEST-PC	Открытый
Гость	TEST-PC	Открытый
ТЕСТ	TEST-PC	
Щеглов	TEST-PC	Секретный

Fig.1. The delimiting access policy of the Mandatory Access Control method to the created files

Note that the configuration of the delimiting access policy does not require the assignment of security labels to the file objects that causes the key gaps of the MAC method (special challenges in inclusion in the system object control scheme).

Consider the Access Manager.

Security labels are assigned to controlled users creating files which require delimiting access rights. The access manager automatically marked a file created by any user: the attributes of the file automatically include the account information of the entity (access level - the mandate) created the file. Similarly, the previously unmarked file is marked when modifying a controlled user.

Accessing the file created during the system operation, the access manager analyzes markup in the file; if it is available (access rights are not delimited), the manager analyzes the compliance of the request with the mandate rules of file access and the file got from the user.

Note that the primary advantage of this method, including simplifying administration, is the correctness of the mandate scheme of access control in the general case. In any folder and conditions, the created/modified file is clearly marked and subjects to the specified delimiting access policy for further requests.

The Discretionary Access Control method to the created files. The DAC method can address the most pressing current issues of information security: anti-malware protection (attacks to increase the privileges of running a malicious program with the systems and system rules).

Three entities identify the access subject [9]:

source user ID launching it;

effective user ID addressing the object;

process (full-track name of the process file) is specified within the interface.

When setting the user ID -primary and effective, a mask "*" can be used- "Any" (the specified rules apply to all users). The process name can be specified either by the full-track name of its processed file or by a mask (use environment variables). For example, the mask C: \ ProgramFile \ * covers all processed files, the mask "*" specifies that the rule applies to any process. The rules for accessing the created files are set by the administrator from the interface and are displayed in the interface.

Note that the assigned access rights do not include the " in response" right. By default, the ban on the created files execution is an effective protection against malware [10]. The task of the delimiting access policy is as follows. The controlled access subjects are set from the list of specified access subjects in the field "Select creators".

The file creator is assigned access rights to other subjects' files created for the selected controlled subject.

To this effect, they select the entity to which access rights belonged in the "Select access entities" field. The relevant access rights-read, text, delete, rename- are allowed or denied for the selected pair of subjects in the left and right fields of the interface. The specified rule is displayed in the corresponding line in the interface.

The access manager operates like in the mandatory method, except that the access rules for the request correctness analysis are selected from the appropriate access matrix. A key difference in creating files and not controlled by users is they must be marked/identified in order to prevent their further execution including system rights.

The specific feature of the control access method for creating files (according to the data) is the ability to isolate (according to the processed data) the operation of critical applications [11].

The MAC and DAC mechanisms can operate together when implementing the delimiting access policy to the created files. The request for access is authorized if it contradicts neither the mandate nor the discretionary rules of access. The access manager analyzes first the mandate rules of access, then discretionary.

These methods significantly cover a number of other methods of data protection including guaranteed deleting. Here, the rules of guaranteed deletion should be set for access subjects creating files, which in any folder should be deleted, not for folders in which saved files are automatically deleted [12]. To be sure, the simple administration and the correctness of the task protection is relevant. A guaranteed deletion rule for folders requires for setting it for all storage folders of temporary files created by most applications since they store protected data as residual information.

Encryption and control access method to the encrypted files being created. The MAC, DAC or both methods to the created files are to address the problem of forcible storage of information encrypted for access subjects. When setting up a file encryption policy, you need to specify access objects with MAC or security label - credentials. Encryption keys are also to be assigned to the entities. The open (not secret) account information of the subject stored as an attribute of the created/modified file is enough to select the encryption key to decrypt the file. The technical solution is patented [13].

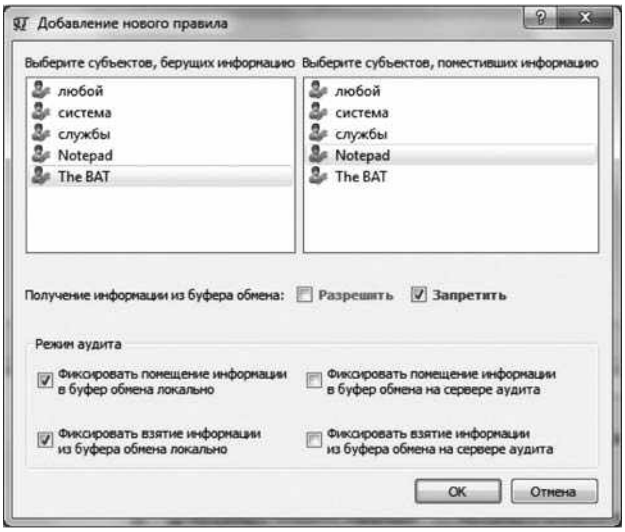
Clipboard access control. The clipboard is intended for temporary storage of data used to exchange data applications; when the administrator sets the delimitation access policy, we have not yet created this data. Control and delimitation of access to created objects written to the clipboard apply the above principles of control and delimitation of access rights.

Here, the discretionary access control includes access process in the subject, but with some reservation.

Between the accounts, the system by default differentiates the clipboard access right. The delimiting applies to sessions of different users. If you start the process with the rights of another account in one session (without rebooting the system or changing the user), for example, using the utility "runas", the clipboard between accounts is not delimited - this case should be avoided.

As for implementing the DAC method to the clipboard, note that it is completely similar to the method of access control to the created files. Access rules - permission or ban on receiving information from the clipboard - from the interface are shown in Fig. 2. The access manager operates similarly.

Thus, the above methods as protection mechanisms implement completely isolated data processing as individual/grouped users and individual applications/application groups in the system.



Добавление нового правила

Выберите субъектов, берущих информацию

- любой
- система
- службы
- Notepad
- The BAT

Выберите субъектов, поместивших информацию

- любой
- система
- службы
- Notepad
- The BAT

Получение информации из буфера обмена: □ Разрешить ☑ Запретить

Режим аудита

☑ Фиксировать помещение информации в буфер обмена локально

□ Фиксировать помещение информации в буфер обмена на сервере аудита

☑ Фиксировать взятие информации из буфера обмена локально

□ Фиксировать взятие информации из буфера обмена на сервере аудита

Fig. 2. The rules for accessing the clipboard

Note that the use of the proposed access control methods to the created objects enable to consider data protection and system objects as completely different protection tasks, in its formulation changes the requirements for many security mechanisms - not only control access. This allows us to suggest a new technology for protecting data processed in the information system.

The problem of protection. Technology of data protection processed in distributed information systems.

Distributed information system involves several computers processing information within a single system and exchanging data between them. File data can be transferred both using external file drives and over the network. In both cases, the transferred file is an object to which the access rights of the subjects are to be differentiated on all computers in the distributed information system. The delimiting access policy is implied for the distributed information system, but not for an individual computer.

Each created file mapped to the account information of the creator of the access subject (the subject ID or security label, possibly both, depending on the method of control and access) allows control and delimitation of access rights. The manager uses the account information as an attribute of the file, when analyzing the request for consistency of the specified delimiting access policy. When implementing a delimited access policy for a distributed information system, file attributes stored directly in the file allow them to be transferred together with a similarly marked file between the information system computers.

Below are the possible delimiting access policies considering the control access methods implemented in the system to the created files.

A delimiting access policy based on security labels (access level) is quick to set up. The access levels (quantitative values) are posted as attributes in the files. A list of access levels and arithmetic comparison rules of security labels are created for the distributed information system. When creating a user on each computer, he is assigned an access level from the list specified for the system. Here, under the implemented technology of distributed information processing on individual computers of the system, information of not all levels of access can be processed. As a result, users on one of the system's computers may be assigned not all access levels from the full-list system.

How to ensure access control in this case. Any file, created during the system operation either on the computer of a creator or on the computer to which it is transferred over the network, receives a label security of the user who created it. Hence, access to it on any computer is possible only within the delimitating policy set for the information system. This extends to encryption - a user can decrypt a file with the appropriate level of access - security label, because the encryption keys are assigned to security labels, not specific users.

The clipboard access control as an object is necessary for inter-machine data exchange in the information system in files.

The possibility to modify the attribute of the file transferred to another computer naturally requires for the correct access control method. Below is the example how to meet the requirement. Let the data be transmitted over the network using e-mail through the application "The BAT". You need to allow this application to read only data written to the clipboard, which is configured from the interface (data transfer is possible only by transferring the appropriate file). The e-mail and the attached file transfer to the remote computer and are automatically saved by the application in the appropriate file. The markup of the newly created file marks the application is running; the further access to the letter is available for the user who has the level of access. Thus, we have a marked file which contains a letter including an attachment in the appropriate format received by mail from another computer. If you are about opening the file attached to the letter, "The BAT" application prompts the user to either save or open the file. If you are about saving the file, it is saved/created in the place selected by the user. As a result, the original markup of this file changes - its new markup shows the security label of "The BAT" user. We must prevent this change in attributes. If you open the file, "The BAT" application creates a temporary file, which will then be read by the application- the editor "Word". The markup of the source file changes, which in both cases is created on a remote machine by "The BAT" application

To solve this problem, you can prevent "The BAT" application to mark the attachment files (not e-mails) created in the appropriate service folder. The administrator should specify programs and folders that will be/will not be marked in these folders depending on the delimiting policy.

Here, the DAC method is implemented similarly, the only variance reflects the content of the attributes of the files created, including the transferred files between computers, and, the method of analyzing access rules. The delimiting access policy in the distributed information system significantly expands possibilities for the "computer ID" (name) to be included in the subject of access. Thus, the users registered on different computers of the system with the same names/accounts can uniquely identify in the delimiting access policy. A delimiting access policy in the distributed information system is far more difficult than in the mandated access control, however, substantially broadens practical possibilities due to the delimitation of access rights between applications used in the distributed information system.

Conclusions and direction of further research. The data protection technology in the information system with the use of access control methods enables- the new property of the delimiting access policy in a distributed information system by using different methods of data exchange between components/ computers; -the efficiency of the information security system by managing data flows in the system.

The data protection technology is to be realized in terms of different operating systems. The paper covers the tested hands-on application [14], which implements data protection technology within the operating system of the Microsoft Windows family.

References

1. **Девянин П. Н.** Модели безопасности компьютерных систем. М.: Издательский центр "Академия"', 2019.
2. **Цирлов В. Л.** Основы информационной безопасности автоматизированных систем. Р.: Феникс, 2019.
3. **Harrison M., Ruzzo W., Ullman J.** Protection in operating systems // Communication of the ACM. 1976. V. 19, N. 8. P. 461—471
4. **Щеглов А. Ю.** Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2019.
5. **Bell D. E., LaPadula L. J.** Security Computer Systems: Uni- fied Exposition abd MULTICS Interpretation. Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.
6. **Щеглов К. А., Щеглов А. Ю.** Принцип и методы контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. 2012. № 7. С. 43—47.
7. **Щеглов А. Ю., Щеглов К. А.** Система контроля доступа к файлам на основе их автоматической разметки. Патент на изобретение № 2524566. Приоритет изобретения 18.03.2013.
8. **Щеглов К. А., Щеглов А. Ю.** Реализация метода мандатного доступа к создаваемым файловым объектам // Вопросы защиты информации. 2013. Вып. 103, № 4. С. 16—20.
9. **Щеглов К. А., Щеглов А. Ю.** Практическая реализация дискреционного метода контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. 2013. № 4. С. 43—49.
10. **Щеглов К. А., Щеглов А. Ю.** Защита от вредоносных программ методом контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. 2012. № 8. С. 46—51.
11. **Щеглов К. А., Щеглов А. Ю.** Защита от атак на уязвимости приложений // Информационные технологии. 2014. № 9. С. 34—39.
12. **Щеглов К. А., Щеглов А. Ю.** Принципы реализации дополнительной защиты информации при контроле доступа к создаваемым файловым объектам на основе их автоматической разметки // Вопросы защиты информации. 2014. Вып. 104, № 1. С. 29—34.
13. **Щеглов А. Ю., Щеглов К. А.** Система контроля доступа к шифруемым создаваемым файлам. Положительное решение на выдачу патента на изобретение по заявке № 2013129406/ 08(043781) от 26.06.2013.
14. **Щеглов А. Ю., Щеглов К. А., Павличенко И. П., Корнетов С. В.** Комплексная система защиты информации "Панцирь+" для ОС Microsoft Windows. Свидетельство о регистрации программы для ЭВМ № 2014660889 от 17.10.2014. Правообладатель ЗАО "НПП "Информационные технологии в бизнесе".

Рукопис подано до редакції 10.11.2021