https://orcid.org/0000-0002-8047-7647

UDC 004.772

Yu.Yu. YURCHENKO*

IMPLEMENTATION OF THE ELEMENTS OF THE ENTERPRISE PROTECTION SYSTEM

*State University of Trade and Economics, Kyiv, Ukraine

Анотація. *У статті визначено головні завдання та особливості корпоративних інформаційних мереж, проаналізовано специфіку корпоративної мережі, реалізованої в медичному центрі. Запропонована система захисту даних на підприємстві розроблена на основі моделі Белла-Ла Падула, оскільки ключовими положеннями даної моделі є призначення усім учасникам процесу обробки даних, що захищається, і документам, в яких вона міститься, спеціальних рівнів безпеки. Визначені рівні безпеки впорядковані за допомогою встановленого відношення домінування, контроль доступу здійснюється залежно від рівнів безпеки взаємодіючих сторін, що дозволяє застосовувати технічні рішення служби каталогів Active Directory. Одним із елементів для забезпечення захисту даних реалізовано використання за відповідним розкладом Тіньової копії даних. Важливою складовою забезпечення захисту даних є індивідуальний процес налаштування групових політик та перевірка реплікації з іншими серверами, на яких працюють служби каталогів Active Directory медичного центру. У результаті впровадження елементів системи захисту даних підприємства вдалось значно підвищити рівень захисту, налаштувати сервер резервного копіювання, на якому створено відповідні папки, в які буде проводитись резервне копіювання за розкладом. Дана функція дає можливість зберігати історію змін будь-якого файла за певний період. Запропоновані елементи системи безпеки можуть бути застосовані для аналізу системи захисту, контролю доступу, забезпечення цілісності даних тощо. Служби каталогів Active Directory були впроваджені в медичному центрі, та виконано налаштування реплікації даних на резервний сервер. Враховуючи специфіку підприємства, а саме медичного центру, впроваджені елементи системи захисту даних забезпечують розмежування рівнів доступу, реалізують профілі захисту та убезпечують особові дані пацієнтів.*

Ключові слова: *комп'ютерні мережі, корпоративні мережі, захист компонентів.*

Abstract. *The article defines the main tasks and features of corporate information networks and analyzes the specifics of the corporate network implemented in a medical center. The proposed data protection system at the enterprise is developed on the basis of the Bella-La Padula model since the key provisions of this model are the assignment of special security levels to all participants in the protected data processing process and to the documents in which it is contained. The specified security levels are arranged using the established dominance relationship, and the access control is carried out depending on the security levels of the interacting parties, which allows the application of technical solutions of the Active Directory service. One of the elements to ensure data protection is the use of a Shadow Copy of data according to the appropriate schedule. An important component of ensuring data protection is the individual process of setting up group policies and checking replication with other servers running the Active Directory directory services of the medical center. As a result of the implementation of elements of the company's data protection system, it was possible to significantly increase the level of protection and set up a backup server, on which appropriate folders were created, to which backup copies would be made according to the schedule. This function makes it possible to save the history of changes in any file for a certain period. The proposed elements of the security system can be used to analyze the security system, control access, ensure data integrity, etc. The Active Directory directory services were implemented in the medical center, and data replication to a backup server was configured. Taking into account the specifics of the enterprise, namely the medical center, the implemented elements of the data protection system ensure the delimitation of access levels, implement protection profiles and secure the personal data of patients.*

Keywords: *computer networks, corporate networks, component protection.*

ISSN 1028-9763. Математичні машини і системи. 2023. № 2

DOI: 10.34121/1028-9763-2023-2-75-81

1. Introduction

A modern corporate network is not only a data transmission network but a complicated complex using which the following tasks are successfully solved:

• increasing the efficiency of the company's work (quick and high-quality decision-making, the possibility of flexible distribution of work among employees, etc.);

• ensuring the possibility of joint use of resources;

• improving communications;

• the provision of prompt access to corporate information;

• greater freedom in the territorial placement of computers.

A corporate network is often viewed as a complex system consisting of several interacting levels. When designing a corporate network, the following requirements are met:

• extensibility – the possibility of relatively simple addition of individual network components (users, applications, services, etc.), increasing the length of network segments and replacing existing equipment with more powerful ones;

• scalability – the possibility of adding new nodes, increasing the length of connections without degrading network performance;

• compatibility – the ability of the network to contain various software and hardware;

• productivity complicated – ensuring the necessary values of performance parameters of the network nodes and communication channels: data transfer speed, response time, and transmission delay;

• controllability – the provision of centralized management capabilities, network development planning, and network condition monitoring;

• reliability – ensuring the uninterrupted operation of the network nodes and communication channels, coherence, storage, and delivery of data without changes and errors to the destination node;

• security – ensuring data protection against unauthorized access.

In networks with centralized management (dedicated server), the network OS is the main (or the only) system that manages server resources [1]. Such systems, of course, have high performance and functionality and use their own disk and file systems optimized for network operation.

The aim of the article is to study the analysis and implementation of elements of a complex data protection system using directory services.

2. Results of the research

A network operating system is a package of programs that provides network implementation and management and provides clients with the ability to use network services. The main tasks of the network operating system are ensuring the compatible use and distribution of network resources; provision of network service to clients; network administration; exchange of messages between network nodes; organization of processes in the network; ensuring reliable data storage and other tasks related to network operation. An important function of the network operating system is to provide a protection system, namely data storage confidentiality, delimitation of access rights to resources, password protection, detection of unauthorized access attempts, tracing of user actions, keeping logs of system events, etc. The software of the client part transforms the requests of the application program for the use of network resources into the appropriate network formats, ensures their forwarding through the transmission medium, and performs reverse conversions. The client part depends on the operating system installed on the workstation (DOS, Windows, Unix, Macintosh, etc.) and the types of networks. The most popular network operating systems today are Microsoft Unix/Linux and Windows Server. UNIX was created to ensure the survivability of

systems and support network equipment, and thanks to high performance and mobility, the UNIX operating system can be used on complex workstations. Linux is a version of UNIX adapted for Intel processors [2].

There are many requirements for corporate network operating systems. They are the following:

• scalability, i.e. the ability to provide work in a wide range of different quantitative characteristics of the network;

• compatibility with other products;

• the ability to work in a complex, heterogeneous network environment in plug-and-play mode;

• support for various end-user OSes (DOS, UNIX, OS/2, Mac, Windows);

• support of protocol stacks (TCP/P, IPX/SPX, NetBIOS, DECnet, AppleTalk, OSI);

• providing easy access to remote resources and convenient service management procedures;

• multi-server network support and effective integration with other operating systems;

• a developed system of services: file service, print service, data security and fault tolerance, data archiving, messaging service, various databases, calling remote RPC procedures, etc.;

• support of network equipment of various standards (Ethernet, Token Ring, ARCnet, FDDI), support of network management standards [3].

The growth of information volumes, information uncertainty, and the complexity of information management of business processes of the enterprise predispose to the use of modern information technologies. The use of models as simplified descriptions of important system components makes it possible to simplify the solution to the task of creating a protection system adequate to real threats [4].

3. Materials and methods

The issue of data protection, including personal data, is quite relevant in any enterprise. Medical institutions of different types of ownership are no exception and require the implementation of complex data protection systems. A feature of the design of information protection systems and the implementation of the Active Directory directory service at enterprises is individual settings for each object, and the delimitation of access levels depending on the type of enterprise activity.

The implementation of a complex data protection system in a medical center does not belong to typical technical solutions and requires the development of individual protection profiles, data virtualization, copy schedules for different servers and user instructions. The Bella-La Padula model was chosen as the basis for the construction of a complex system, which provides for the separation of security levels and allows the application of technical solutions of the Active Directory directory service.

At the time of the design of the existing data protection information system, the company was called “Ibn Sina + Medical Center” LLC. Accordingly, the old name of the enterprise will appear on the graphic material.

The existing data protection information system of the medical center consisted of the following components:

1. Domain controller (domain controller) – IbnSina.cnb domain.

2. File server (file server) – the storage of work data of employees.

3. Server of the medical information system “EMSIMED” – a specialized software for work in medical institutions.

4. Users’ personal computers and laptops.

A domain controller is a server running a centralized storage service for user accounts, computers, application installations, and more. It is necessary for the organization of a single authentication center and storage/provision of information about the company's land resources.

On the Windows Server platform, directory services are implemented using Active Directory, and on Linux – using Samba. For the fault tolerance of the system, it is possible to install secondary servers with the domain controller service (the division into primary and secondary servers will be conditional since they equally contain the necessary information and perform their tasks).

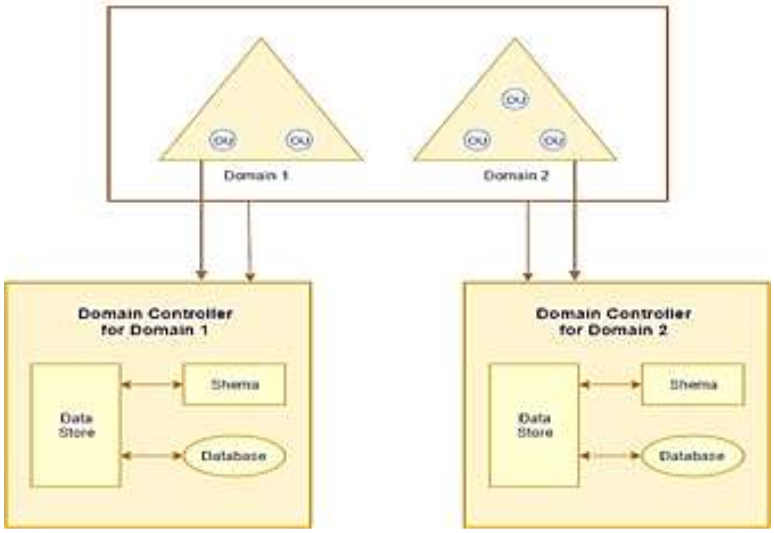

Figure 1 – An example of an Active Directory organization

The deployment of the Active Directory directory service (Fig. 1) in comparison with the workgroup (Workgroup) gives the following advantages.

Single point of authentication. When computers work in a workgroup, they do not have a single-user database, each computer has its own. Therefore, by default, none of the users has network access to another user's computer or server [4]. In the workgroup, on each computer or server, you will have to manually add a complete list of users who need network access. If one of the employees suddenly wants to change their password, then it should be changed on all computers and servers. When using an Active Directory domain, all user accounts are stored in one database, and all computers refer to it for authorization. All users of the domain should be included in the group, for example, “Accounting”, “HR”, “Finance Department”, etc. It is enough to set permission for certain groups once, and all users will have the appropriate access to documents and applications. If a new employee joins the company, an account is created for him, which is included in the appropriate group, and that's it! After a couple of minutes, the new employee gets access to all network resources to which he should be allowed access, on all servers and computers. If an employee is fired, it is enough to block or delete his account, and he will immediately lose access to all computers, documents, and applications [2].

A single point of policy management. When using a single Active Directory directory, all users and computers are hierarchically distributed across organizational divisions, each of which is subject to uniform group policies. Policies allow you to set uniform security settings and parameters for a group of computers and users. When a new computer or user is added to the domain, it automatically receives settings that meet the accepted corporate standards. Also, with the help of policies, you can centrally assign network printers to users, install necessary applications, set Internet browser security parameters, configure Microsoft Office applications, etc [4].

Integration with corporate applications and equipment. A great advantage of Active Directory is compliance with the LDAP standard, which is supported by hundreds of applications, such as mail servers (Exchange, Lotus, Mdaemon), ERP systems (Dynamics, CRM), proxy servers (ISA Server, Squid), etc. Moreover, these are not only applications for Microsoft Windows but also Linux-based servers. The advantages of such integration are that

there is no need for users to remember many logins and passwords to access one or another application since in all the applications they have the same credentials because their authentication takes place in a single Active Directory. In addition, there is no need for employees to enter their login and password several times, it is enough to turn on the computer and log in once, and in the future, users will be automatically authenticated in all applications. Windows Server provides the RADIUS protocol for the integration with Active Directory supported by a large number of network equipment. Thus, it is possible, for example, to ensure the authentication of domain users when connecting to a CISCO router via VPN [2].

A single application configuration repository. Some applications (such as Exchange Server or Office Communications Server) store their configuration in Active Directory. Deployment of the Active Directory directory service is a prerequisite for the operation of these programs. You can also store the DNS domain name server configuration in the directory service. Storing the application configuration in the directory service is advantageous in terms of flexibility and reliability. For example, in the event of a complete failure of the Exchange server, its entire configuration will remain intact because it is stored in Active Directory, and to restore the functionality of a corporate mail, it will be enough to reinstall the Exchange server in a recovery mode.

Increased level of information security. Using Active Directory significantly increases the level of network security. First of all, it is a single and secure repository of accounts. On the network, user credentials are stored in a local account database (SAM) that can theoretically be compromised by taking over a computer.

Scalability and fault tolerance of the Active Directory directory service. Microsoft Active Directory is highly scalable. More than 2 billion objects can be created in the Active Directory forest, which allows you to implement the directory service in companies with hundreds of thousands of computers and users. The hierarchical structure of domains allows flexible scaling of the IT infrastructure to all branches and regional divisions of companies. A separate domain can be created for each branch or division of the company, with its own policies, users, and groups. Administrative powers can be delegated to local system administrators for each child domain. At the same time, child domains still obey the parent domains.

In addition, Active Directory allows you to configure trust relationships between domain forests. Each company has its own forest of domains, each of which has its own resources. However, sometimes it is necessary to provide access to your corporate resources to employees from partner companies. For example, when participating in joint projects, employees with a partner company may jointly need to work with common documents or applications. To do this, trust relationships can be set up between the forests of organizations, which will allow employees from one organization to log in to the domain of another.

4. Designing

Fault tolerance of the directory service is ensured by deploying two or more servers – domain controllers in each domain. All changes are automatically replicated between domain controllers. In the event of failure of one of the domain controllers, the network performance is not affected, because the remaining ones continue to work [5].

The Active Directory directory service was implemented in the medical center (Fig. 2), but this service was configured on one server, on which data replication to the backup server was not configured.

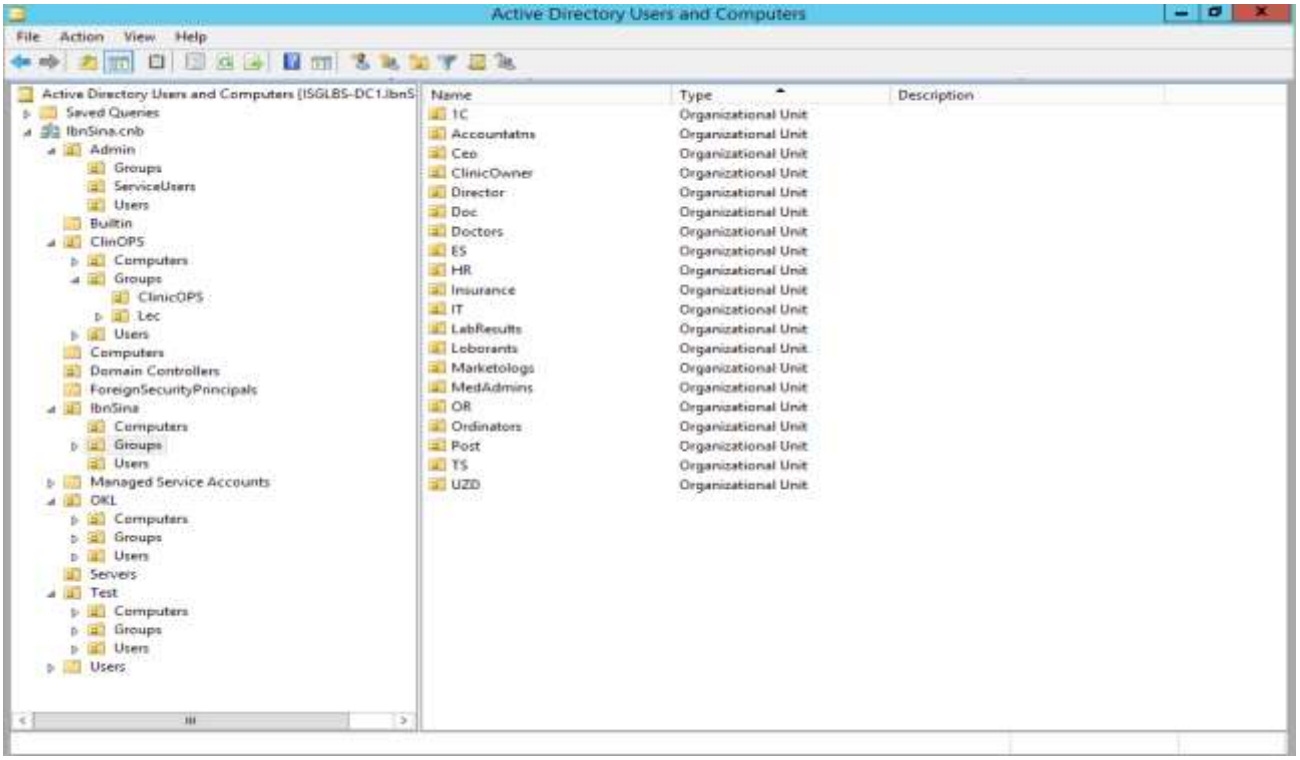

Figure 2 – Implementation of the Active Directory directory service

In addition, the Shadow Copy of the data function is implemented as an element to ensure data protection according to the appropriate schedule. This function makes it possible to save the history of changes in any file for a certain period (Fig. 3). That is, you can view a version of a file, for example, a week or a month old.

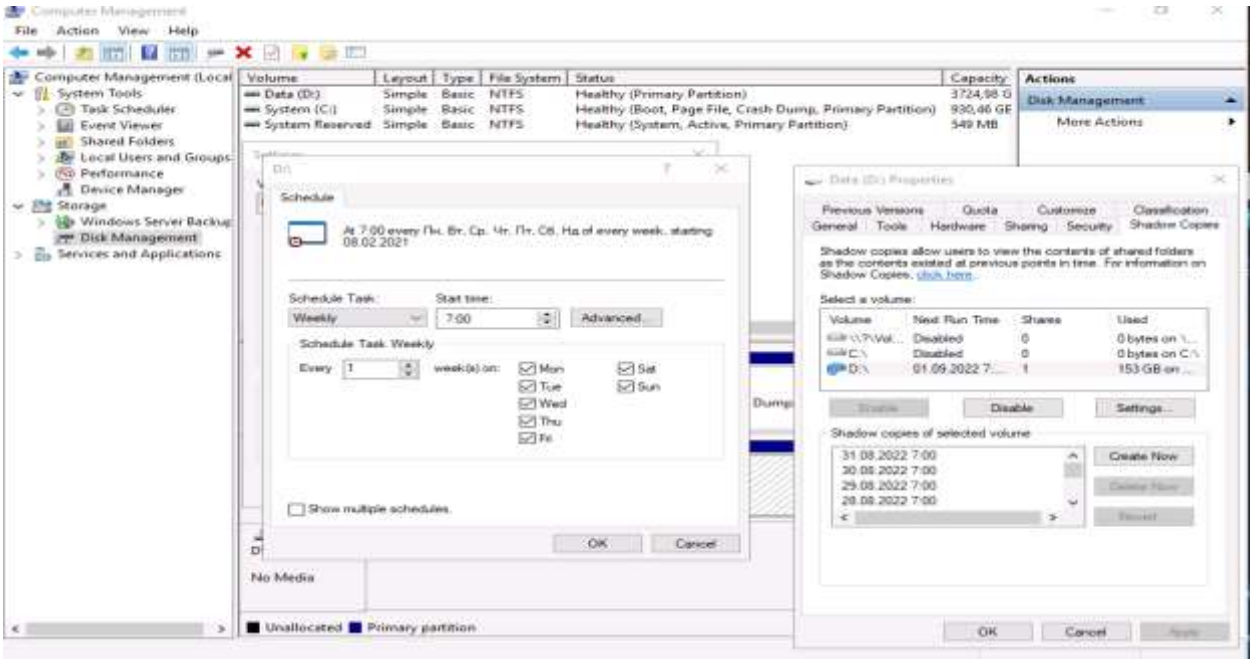

Figure 3 – The adjusted parameters of the Shadow Copy function

5. Conclusions

The article defines the main tasks and features of corporate information systems, which include the comprehensive coverage of management functions; efficiency of use of computer and

telecommunications equipment and software; adaptability of the functional and instrumental structure of the system to the features of the managed object, etc. Information for the implementation of elements of the data protection system was taken from the results of a comprehensive survey of the organization for which the development of the information system was carried out. As one of the additional elements of data protection, the Shadow copy of the data function is implemented according to the appropriate schedule. This function makes it possible to save the history of changes in any file for a certain period.

REFERENCES

1. Диогенес Ю., Озкайя Е. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020. 1008 с.
3. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: навч. посіб. К.: Видавнича група BHV, 2014. 608 с.
4. Kraskevich V.E., Yurchenko Yu.Yu. Software implementation of the enterprise protection system. *Mathematical machines and systems.* 2022. N 4. P. 62–67.
5. Samoylenko H.T., Yurchenko Yu.Yu. Conceptual model of enterprise security in the information environment. *Mathematical machines and systems.* 2023. N 1. P. 112–117.

Стаття надійшла до редакції 03.04.2023