https://orcid.org/0000-0002-8047-7647
https://orcid.org/0000-0002-7829-0939

UDC 004.772

**V.E. KRASKEVICH[*], Yu.Yu. YURCHENKO[*]**

# SOFTWARE IMPLEMENTATION OF THE ENTERPRISE PROTECTION SYSTEM

[*]State University of Trade and Economics, Kyiv, Ukraine

***Анотація.*** *У статті запропоновано реалізацію специфічної інформаційної системи забезпечення інформаційної безпеки підприємства. Досліджено та проаналізовано особливості міжнародного стандарту ISO/IEC-15408, який є методологією завдань, оцінки та каталогом вимог безпеки IT. Визначено специфіку застосування загальних критеріїв безпеки та як приклад впровадження на підприємстві «Загальних критеріїв» запропоновано застосування служб Active Directory. Визначено переваги служби каталогів Active Directory в порівнянні з робочою групою (Workgroup). Запропоновано покрокову побудову відмовостійкої системи захисту даних підприємства. Особливістю запропонованої системи є відмовостійкість служби каталогів, яка забезпечується шляхом розгортання серверів-контролерів домену в кожному домені. Визначено головні завдання запропонованої системи захисту даних, до яких належить комплексність охоплення функцій управління; ефективність використання комп'ютерно-телекомунікаційного обладнання і програмного забезпечення; адаптивність функціональної та інструментальної структури системи до особливостей керованого об'єкта. Запропонована комплексна система захисту даних складається з ряду компонентів, взаємопов'язаних між собою. Обов'язковою складовою налагодження комплексної системи захисту є організація системи резервного копіювання критичних баз даних, що включає в себе планування розкладу резервного копіювання для різних серверів. Для керування правами доступу додано групи користувачів, враховуючи особливості роботи підприємства, а налаштування політик дає можливість обмежити доступ до даних на файлових серверах підприємства у відповідності за різними рівнями доступу до інформації. Впровадження матеріалів дослідження у практику вирішення прикладних завдань, спрямованих на впровадження системи захисту даних на підприємствах, підтверджене актами практичного застосування на підприємстві ТОВ Медичний центр «Консиліум Медікал».*

***Ключові слова:*** *системи захисту, стандарти, відмовостійкість, захист даних.*

***Abstract.*** *The article proposes the implementation of a specific information system for ensuring the information security of the enterprise. The peculiarities of the international standard ISO/IEC-15408, which is a methodology of tasks, assessments and a catalog of IT security requirements have been studied and analyzed. The specifics of the application of general security criteria have been defined and the use of Active Directory services has been proposed as an example of the implementation of General Criteria at the enterprise. The advantages of the Active Directory service in comparison with the Workgroup have been determined. Step-by-step construction of a fault-tolerant enterprise data protection system has been offered. A feature of the proposed system is the fault tolerance of the directory service, which is ensured by deploying servers – domain controllers in each domain. The article defines the main tasks of the proposed data protection system, including the comprehensive coverage of management functions, the efficiency of use of computer and telecommunications equipment and software, and the adaptability of the functional and instrumental structure of the system to the features of the managed object. The proposed complex data protection system consists of a number of interconnected components. A mandatory component of setting up a comprehensive protection system is the organization of a backup system for critical databases, which includes planning a backup schedule for various servers. To manage access rights, user groups have been added, taking into account the specifics of the company's work, and setting policies makes it possible to limit access to data on the company's file servers in accordance with different levels of access to infor-*

*mation. The implementation of research materials into the practice of solving applied tasks aimed at implementing a data protection system at enterprises has been confirmed by acts of practical application at the enterprise Medical Center Consilium Medical LLC.*
***Keywords:*** *protection systems, standards, fault tolerance, data protection.*

DOI: 10.34121/1028-9763-2022-4-62-67

## 1. Introduction

The problem of leaks of information from a variety of commercial and non-commercial enterprises is becoming a daily occurrence. The issue of data security is quite relevant in any enterprise. Ensuring information security at the enterprise comprises the development of a comprehensive information protection system and constant control over the sources of various potential threats, and the need to protect information in various ways (protection of programs against reading and copying, protection of copyrights to information, protection against unauthorized access, and launch of programs).

*The aim of the article is* to conduct research and implement a comprehensive data protection system using protection profiles.

## 2. Results of the research

In the international standard ISO/IEC-15408, there are main subjects and objects of security [1]. This standard is the most successful result of the generalization of the experience of various states in the development and practical use of information technology (IT) security assessment criteria. The basic documents that formed the basis of the General Criteria and the connections between them are presented. When carrying out work on the analysis of the security of the enterprise, it is advisable to use the General Criteria as the main criteria that allow assessing the level of IP protection from the point of view of the completeness of the security functions implemented in it and the reliability of the implementation of these functions. The development of this standard had the following main goals:

- unification of national standards in the field of IT security assessment;
- increasing the level of trust in the assessment of IT security;
- reducing IT security assessment costs based on mutual recognition of certificates.

The new criteria were to ensure mutual recognition of the results of a standardized security assessment in the global IT market. The first part of the General Criteria contains definitions of general concepts, concepts, and a description of the model and methodology of IT security assessment. It introduces the conceptual apparatus and defines the principles of formalization of the subject area. The requirements for the functionality of protection tools are given in the second part of the General Criteria and can be directly used in the security analysis to assess the completeness of the security functions implemented in the IS. The third part of the General Criteria, along with other requirements for the adequacy of the implementation of security functions, contains a class of requirements for the analysis of vulnerabilities of protection means and mechanisms called Vulnerability Assessment. This class of requirements defines the methods that should be used to prevent, detect, and eliminate various vulnerabilities such as side channels of information leakage, errors in the configurations that lead to the transition of the system to a dangerous state, insufficient stability of security mechanisms, the presence of vulnerabilities in information protection tools that allow users to gain unauthorized access to information bypassing existing protection mechanisms. According to the level of systematization, completeness and possibilities of detailing the requirements, universality and flexibility in the application of general criteria, they represent the best of the currently existing standards. Moreover, what is very important, due to the peculiarities of its construction, it has practically unlimited opportunities for development, it is not a functional standard, but a methodology of tasks, assessments and a catalog of IT security requirements that can be expanded and refined [2].

As an example of the implementation of the General Criteria at the enterprise, the introduction of Active Directory has been used. Deployment of the Active Directory directory service in comparison with a workgroup (Workgroup) provides 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.

• *A single point of policy management*. In the network (workgroup) all computers are equal. None of the computers can control the other one, all computers are configured differently, and it is impossible to control compliance with uniform policies or security rules. When using a single Active Directory directory, all users and computers are hierarchically distributed across organizational units, to each of which uniform group policies are applied.

• *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. (these are not only applications for Microsoft Windows, but also Linux-based servers).

• *Unified application configuration repository*. Deployment of the Active Directory directory service is a prerequisite for the operation of Exchange Server or Office Communications Server, and the DNS domain name server configuration can also be stored in the directory service.

• *Increased level of information security.* The use of Active Directory significantly increases the level of network security, as it will be a single and secure storage of accounts.

• *Scalability and fault tolerance of the Active Directory directory service.* The hierarchical structure of domains allows flexible scaling of IT infrastructure to all branches and regional divisions of companies.

Fault tolerance of the directory service is ensured by deploying 2 or more servers – domain controllers in each domain. All changes are automatically replicated between the domain controllers. In the event of failure of one of them, network performance is not affected, because the remaining ones continue to work. An additional level of fault tolerance provides the placement of DNS servers on domain controllers in Active Directory, which allows each domain to have several DNS servers that serve the main zone of the domain. And in case of failure of one of the DNS servers, the remaining ones will continue to work, and they will be available both for reading and for writing, which cannot be ensured using, for example, the Linux-based BIND DNS server [3].

## 3. Materials and methods

It is advisable to start building a fault-tolerant data protection system by planning the structure of the domain and its components. Before installing the platform, it is necessary to prepare a suitable server with the necessary technical characteristics. The key parameter for ensuring fault tolerance of the server is the organization of disk space for the formation of the necessary operating systems or platforms. The next step is the preparation of the platform for the installation of the Active Directory service (installation and configuration of the servers have been carried out on the VMware ESX 6.5.0 platform, see Fig. 1 and Fig. 2).

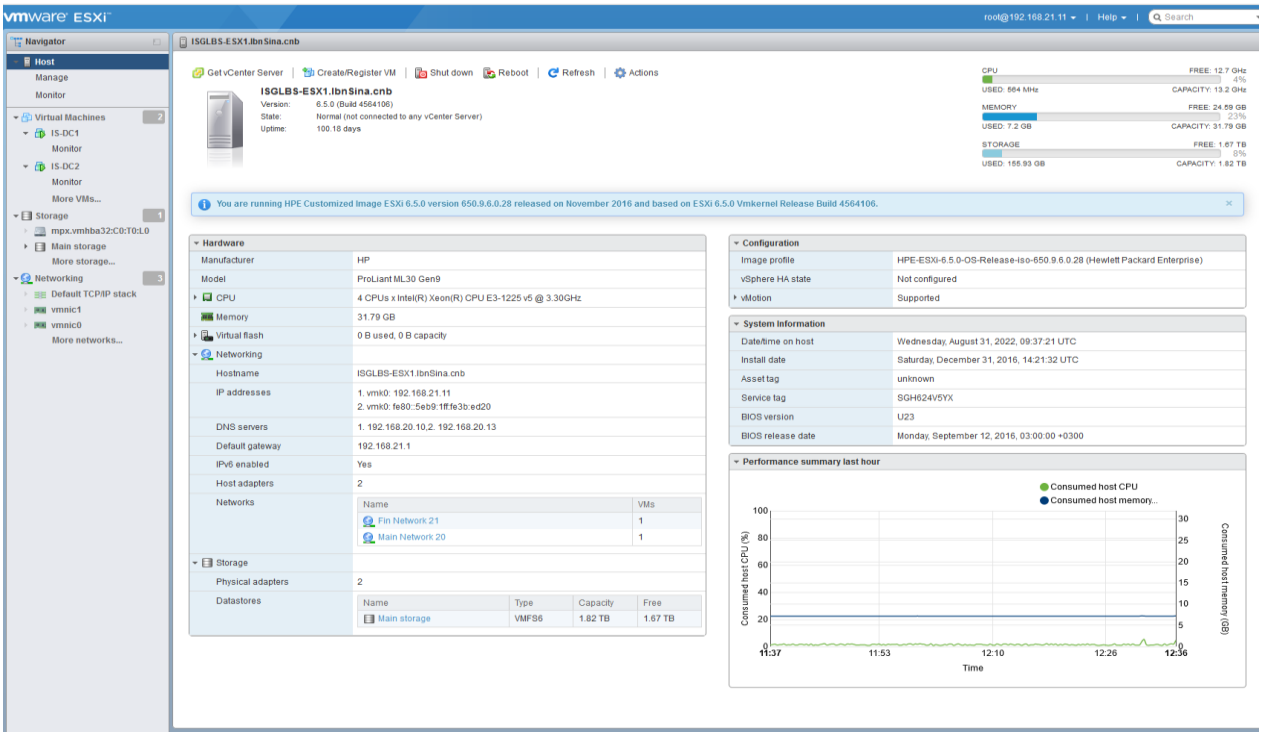


Figure 1 – Features of VMware ESX 6.5.0 Server

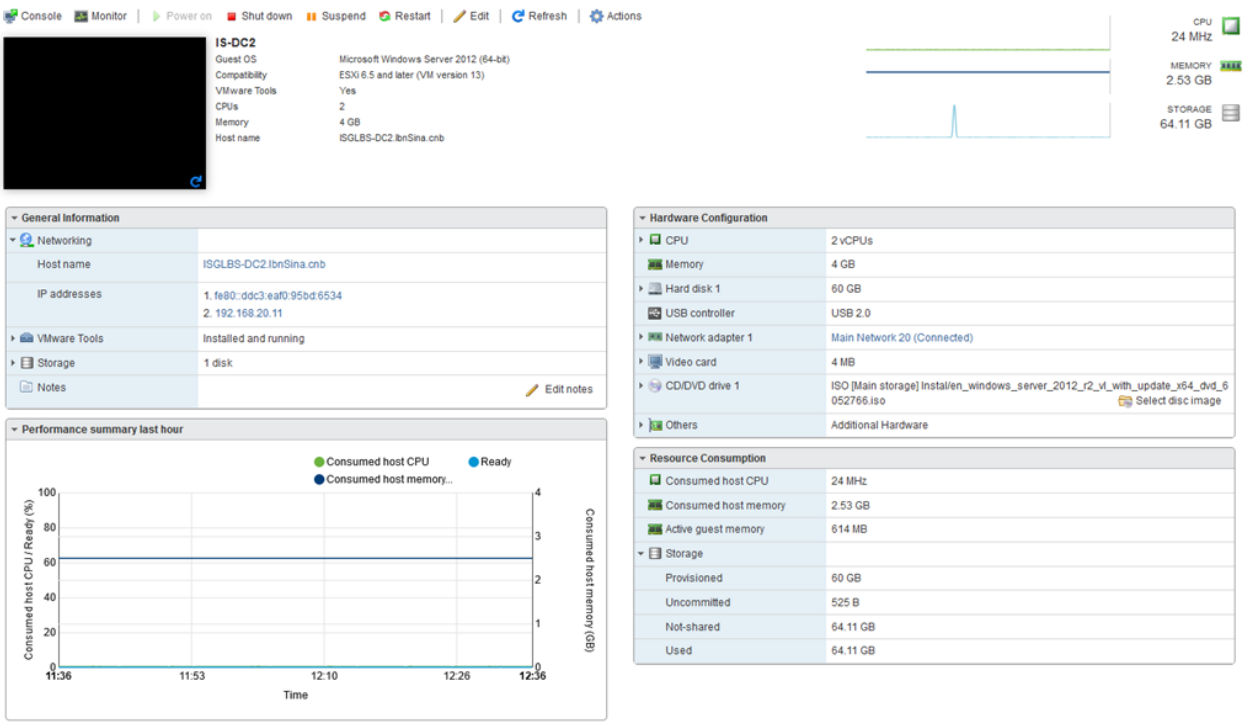


Figure 2 – Implementation of Windows Server 2012 R2 for Active Directory

After installing the platforms, install the directory service. It is advisable to install the service on three servers, so the first ISGLBS-server will be primary, and ISGLBS-DC2 and ISGLBS-DC3 will be in replication with it, and thus there will be backups. Running the script is done with the help of Windows PowerShell. For further preliminary unified configuration of servers and personal computers of users, it is necessary to develop instructions for the initial

configuration of servers and configuration of computers. The next step is to organize a comprehensive backup system for critical databases, and it starts with planning the backup schedule for the various servers.

In this case, the server backup schedule follows:

15:00 – Test Server (ISGLBS-TEST) – Every day
17:00 – Domain Controller 3 (ISGLBS-DC3) – Every day
17:30 – Domain Controller 1 (ISGLBS-DC1) – Every day
18:00 – Domain Controller 2 (ISGLBS-DC2) – Every day
19:30 – File Server (ISGLBS-FS1) – Every day
21:00 – MCMED Server (ISGLBS-MCMED1) – Every day
23:30 – Backup server (ISGLBS-BS1) – Every day
00:30 – File Server (ISGLBS-FS2) – Every day
01:30 – Terminal Server (ISGLBS-TS1) – Every day
04:30 – Terminal Server (ISGLBS-TS2) – Every day
06:00 – Terminal Server (ISGLBS-TS3) – Every day

After developing a backup schedule for various servers, you can proceed to the next stage of organizations of a comprehensive backup system of critical databases. It is advisable to use RAID data virtualization technology to install and configure the backup server. Since a comprehensive data protection system consists of a number of components that are interconnected, it is appropriate to consider each element necessary for functioning. First of all, it is necessary to enter the entire structure, groups of users, and users themselves. The very structure of the enterprise domain is presented in the form of a tree (Fig. 3).

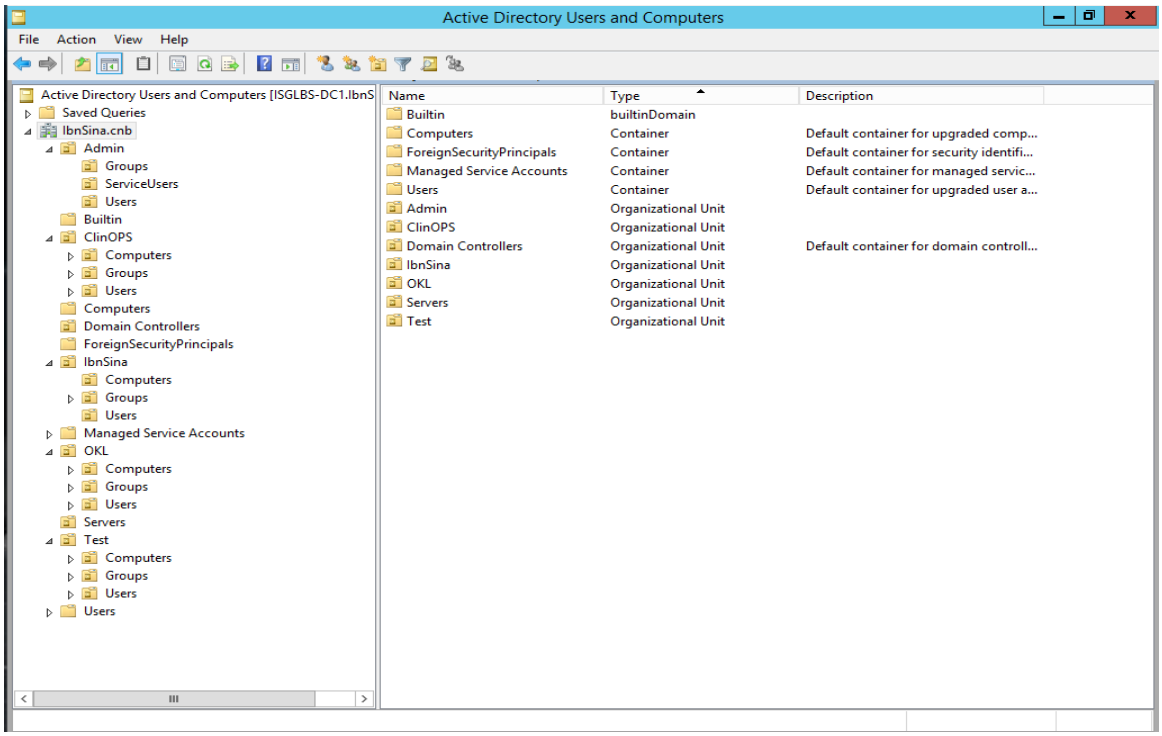


Figure 3 – The structure of the enterprise domain

For flexible management of access rights, it is advisable to add user groups, taking into account the specifics of the enterprise. The next step is to configure group policies and verify replication with other servers running the enterprise's Active Directory directory services. The stage of policy setting is also individual and provides an opportunity to limit access to data on the company's file servers in accordance with different levels of access to information. The last stage of the implementation of a comprehensive data protection system is the configuration and

organization of automated backup of the company's servers. It is also necessary to install and configure a backup server, on which it is necessary to create appropriate folders to which backups will be made according to a previously developed schedule. All automated processes will be launched with the help of service users (accounts entered into the domain structure for the purpose of performing automated tasks).

## 4. Conclusions

The growth of information volumes, information uncertainty, and the complexity of information management of business processes of the enterprise determine the use of information technologies. Prevention and neutralization of any threats, both internal and external, is possible due to the use of a new comprehensive data protection system using protection profiles. The introduction of a new comprehensive data protection system using protection profiles makes it possible to increase the level of protection to the required level, monitor and control the network traffic of the enterprise's corporate network, and track any actions to the end computer and the user.

## REFERENCES

1. Common Criteria Services – ISO 15408.
2. Диогенес Ю., Озкайя Е. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020. 1008 с.

*Стаття надійшла до редакції 27.09.2022*