https://orcid.org/0000-0001-8624-5778
https://orcid.org/0000-0002-8047-7647

UDC 004.772

S.S. SHKILNIAK[*]**, Yu.Yu.YURCHENKO**[**]

METHODS OF ENSURING THE SECURITY OF COMPUTER NETWORKS

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

Анотація. *Метою статті є аналіз питань безпеки сучасних комп'ютерних мереж для розробки технічних рішень, що використовуються при створенні корпоративних мереж, та представлення практичного застосування для забезпечення захисту інформації на підприємстві. Однією з найважливіших частин інформаційної інфраструктури сучасних підприємств та багатьох державних організацій є корпоративні мережі. Оскільки функціонування корпоративних систем може проходити у відкритому середовищі, вихід із ладу такої системи чи спотворення підсистеми доступу до інформаційних ресурсів фактично означає припинення функціонування підприємства. У статті розглядаються питання методологічних та технічних аспектів захисту інформації на підприємстві. Розглядаються питання застосування мережевих технологій для реалізації політики безпеки та рівнів доступів до інформації. Розглядаються й аналізуються питання безпеки та доступу до інформації на різних рівнях, з урахуванням технічного та кадрового забезпечення. Визначено принципи побудови, що використовуються під час планування мережі та прийняття рішень. Розглянуто структуру корпоративної мережі та методологію її створення. Наведено способи реалізації корпоративної мережі підприємства з урахуванням питань безпеки та захисту інформації. Запропоновано теоретико-методологічні основи проєктування корпоративної мережі забезпечення інформаційної безпеки підприємства. У статті наведено технології, що застосовуються при створенні корпоративних мереж. Розглянуто методологію створення корпоративної мережі, а саме, які вимоги ставляться перед корпоративною мережею та технічні завдання корпоративної комп'ютерної мережі. В результаті дослідження було розроблено оновлену схему корпоративної комп'ютерної мережі (для реалізації комп'ютерної безпеки) та представлено систему безпеки корпоративної комп'ютерної мережі.*

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

Abstract. *The aim of the article is to analyze the security of modern computer networks for the development of technical solutions used in the creation of corporate networks and to present practical applications for information security in the enterprise. One of the most important parts of the information infrastructure of modern enterprises and many government organizations are corporate networks. Since the operation of corporate systems can take place in an open environment, the failure of such a system or distortion of the subsystem of access to information resources actually means the cessation of the enterprise. The article considers the issues of methodological and technical aspects of information protection it the enterprise. The issues of application of network technologies for the implementation of security policy and levels of access to information are considered. Issues of security and access to information at different levels are considered and analyzed, taking into account technical and personnel support. The principles of construction used in network planning and decision-making are defined. The structure of the corporate network and the methodology of its creation are considered. The methods of realization of the corporate network of the enterprise taking into account the issues of security and protection of information are given. Theoretical and methodological bases for designing a corporate network for the information security of the enterprise are proposed. The article presents the technologies used in the creation of corporate networks. The methodology of creating a corporate network is considered, namely, what are the requirements for the corporate network and the technical objectives of the corporate computer network. As a result of the research, an updated scheme of the corporate computer network (for the implementation of computer security) was developed and the security system of the corporate computer network was presented.*

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

DOI: 10.34121/1028-9763-2022-2-102-110

1. Introduction

The advent of local and global data networks has given computer users new opportunities for the rapid exchange of information. But at the same time, the development and complexity of tools, methods and forms of automation of information processing increase the dependence of society on the degree of security of information technology.

The urgency and importance of the problem of information security are determined by the following factors:

– modern levels and rates of development of information security tools lag far behind the levels and rates of development of information technologies;

– the high growth rate of the fleet of personal computers used in various fields of human activity;

– increasing the number of users who have access to information resources and data sets;

– the rapid growth of information accumulated, stored, and processed by computers and other automation tools;

– numerous vulnerabilities in software and network platforms;

– the rapid development of the global Internet which virtually does not prevent security breaches of information processing systems around the world.

Modern methods of accumulation, processing, and transmission of information have contributed to the emergence of threats related to the possibility of loss, misrepresentation, and disclosure of data addressed to users.

The aim of the article is to provide the analysis and development of the corporate computer network scheme and to present the security system of the corporate computer network.

2. Results of the research

Security threat is a possible danger (potential or actual) of committing any act (action or omission) directed against the object of protection (information resources), causing harm to the owner or user, which is manifested in the danger of distortion, disclosure or loss of the information. The realization of the threat will be called an attack.

Realization of one or another security threat can pursue the following purposes:

– breach of confidentiality of information as the information stored and processed in the corporate network can be of great value to its owner;

– violation (partial or complete) of the corporate network (availability violation). Failure or incorrect change of modes of operation of the components of the corporate network, their modification or substitution may lead to incorrect results, failure of the corporate network from the flow of information or service failures. Refusal to flow information means non-recognition by one of the interacting parties of the fact of transmission or reception of messages. Given that such messages may contain important reports, orders, financial approvals, etc., the damage, in this case, can be quite significant.

Corporate networks are distributed computer systems that perform automated processing of information. The problem of information security is key for such computer systems. Ensuring the security of the corporate network involves the organization of prevention of any unauthorized intrusion into the operation of the corporate network and attempts to modify, disable or destroy its components, i.e., protection of all components – hardware, software, data, and personnel.

Let’s consider the current image of information security in the enterprise. Research company Gartner Group identifies 4 levels of maturity of the company in terms of information security.

Level 0:

– Nobody is involved in the information security of the company.

– No resources are allocated.

– Information security is simply a delimitation of access to resources and services.

A typical example is a company with a small staff engaged, for example, the one which deals with buying or selling goods. The network administrator is often a student, and the main thing in such a company is that everything works.

Level 1:

– Information security is considered as a technical case, there is no single concept for the development of information security of the company.

– Funding is provided within the general IT budget.

– Information security is implemented by means of Level 0 plus the means of backup, anti-virus means, firewalls, and means of the organization of VPN (traditional means of protection).

Levels 2 and 3:

– Information security is considered by the management as a set of different measures, there is an understanding of the importance of information security for production processes, and a program of information security system development of the company is approved by the management.

– Funding is provided within a separate budget.

Information security is implemented by means of Level 1 plus the means of the strengthened authentication, means of the analysis of mail messages and web content, IDS (intrusion detection systems), means of the security analysis, one-time authentication tools means, public key infrastructure, and different organizational actions.

Level 3 differs from Level 2 in the following way:

– Information security is a part of the corporate culture.

– Funding is provided within a separate budget, which according to the research of the analytical company Datamonitor in most cases is not more than 5% of the IT budget.

– Information security is implemented by means of Level 2 plus IS management systems, IS Incident Response Team, Service Level Agreement.

Thus, a serious approach to IS issues appears only at Levels 2 and 3. According to the provided classification, at Level 1 and partially at level 0 there is a so-called “fragmentary” approach to providing IS. The partial approach is aimed at counteracting clearly defined threats in given conditions [1]. Examples of such an approach are individual access control tools, stand-alone encryption tools, specialized anti-virus programs, etc.

3. Materials and methods

The complex approach is based on the decision of a complex of private tasks under the uniform program. This approach is currently fundamental to creating a secure information processing environment in enterprise systems, bringing together disparate threat management measures. These include legal, moral and ethical, organizational, software, and technical means of information security. An integrated approach has made it possible to integrate a number of autonomous systems by integrating them into integrated security systems.

Further development of an integrated approach or its maximum form is an integrated approach based on the integration of various security subsystems and communication subsystems into a single integrated system with common hardware, communication channels, software, and databases. An integrated approach is aimed at achieving integrated security. The main meaning of the concept of integrated security is the need to ensure a state of the corporation, in which it is reliably protected from all possible types of threats during the entire continuous production process. The concept of integrated security implies mandatory continuity of the security process both in time and space (throughout the technological cycle of activity) with mandatory consideration of all possible types of threats (unauthorized access, removal of information, terrorism, fire, natural disasters, etc.) [2].

Whatever the form of an integrated or integrated approach, it is always aimed at solving a number of private problems in their close relationship with the use of common hardware, communication channels, and software. For example, in relation to information security, the most obvious of these are the tasks of restricting access to information, technical and cryptographic closure of information, limiting the levels of parasitic radiation of technical means, security and alarm. However, there are needed solutions to other tasks which are no less important. For example, the disabling of business leaders, members of their families or key employees should call into question the very existence of the business. This can be facilitated by natural disasters, accidents, terrorism, etc. Therefore, the objective ensuring of the complete security of information can only be with integrated security systems, indifferent to the type of security threats and provide the necessary protection continuously, both in time and space, throughout the process of preparation, processing, transmission, and storage of information. The corporate network is territorially distributed, it unites offices, divisions and other structures which are at a distance from each other. Usually, the nodes of the corporate network are located in different cities and sometimes even countries. The principles on which such a network is built are very different from those used in creating a local area network. The key difference is that geographically distributed networks use rather slowly. When creating a local network, the main costs are spent on the purchase of equipment and cable laying, respectively, in the territorially distributed networks, a key essential element of the cost is the rent for the use of channels. This limitation is key, and when designing a corporate network you need to use all measures to minimize the amount of data transmitted.

Before uncovering the basics of the methodology of building corporate networks, it is necessary to reveal the comparative analysis of technologies that can be used in corporate networks. Data transfer technologies can be classified according to data transfer methods. In the general case, there are three main methods of data transmission:

– channel switching;
– message switching;
– packet switching.

Other methods of interaction are their evolutionary development. For example, if you imagine the technology of data transmission in the form of a tree, the branch of packet switching will be divided into frame switching and cell switching. First packet switching technologies are X.25 and IPs were designed with the ability to work with poor quality communication channels. As the quality improved, it became possible to use a protocol such as HDLC to transmit information, which found its place in Frame Relay networks. The need for greater productivity and technical flexibility prompted the development of SMDS technology, the capabilities of which were then expanded by standardization. Comparison of technologies can also be made according to the following criteria – the effectiveness of the addressing scheme or routing methods. Packet routing on the network can be performed statically. Examples of standardized solutions are OSPF or RIP dynamic routing protocols for the IP protocol. The best option for a private network is to create communication channels only in those areas where it is necessary. It is a return to leased lines but there are technologies for building data networks that allow organizing channels within them, which are performed only when necessary. These channels are called virtual. A system that combines remote resources through virtual channels is called a virtual network. There are two main technologies of virtual networks – circuit-switched networks and packet-switched networks. The first ones include the regular telephone network, ISDN and a number of other, more atypical technologies. Packet-switched networks are represented by Frame Relay and X.25. Channel-switched networks provide the user with several communication channels with fixed bandwidth for each connection. ISDN (digital network with integrated services) is an example of a virtual network with circuit switching. ISDN provides digital channels (64 kbit/s) which can transmit both voice and data. Limitations on the number of concurrently available resources imposed by ISDN make it convenient to use this type of communication as an alternative to telephone networks. In systems with a small number of nodes, ISDN can be used as the main network protocol [3].

During the construction of a geographically distributed network, there can be used all the technologies described above. The easiest and most affordable way to connect remote users to use VPN networks. In most cases, global data networks are used to connect network nodes. Connecting the corporate network to the Internet is justified access to relevant services. The use of the Internet as a data transmission medium is possible only when other methods are not available and financial considerations outweigh the requirements of reliability and security. If to use the Internet only as a source of information, it is better to use the technology of “connection on demand” (dial-on-demand). This dramatically reduces the risk of unauthorized intrusion into the network from the outside. The easiest way to provide such a connection is to use a call to a web-site over a telephone line or, if possible, through ISDN. Another, more reliable way to provide on-demand connections is to use a dedicated line and X.25 protocol or Frame Relay. Widespread methods of connection using PPP or HDLC do not allow this. A good solution is to use a single Internet connection point for the entire geographically distributed network, whose nodes are connected to each other by using X.25 or Frame Relay virtual channels. In this case, access from the Internet is possible to a single node, while users in other nodes can access the Internet through a connection on request.

Virtual channels of packet-switched networks should also be used for data transmission within the corporate network. Both X.25 and Frame Relay can be used as a virtual network when building a corporate information system. The choice between them is determined by the quality of communication channels, the availability of services at connection points, and financial considerations. Today, the costs of using Frame Relay for long-distance communication are several times higher than for X.25 networks. Higher data rates and the ability to transmit data and voice at the same time can be crucial arguments in favor of Frame Relay. Frame Relay technology is better in areas of the corporate network where leased lines are available. In this case, it is possible to connect local networks and connect to the Internet, as well as use those applications that traditionally require X.25. Besides, on the same network telephone communication between nodes is possible. For Frame Relay, it is better to use digital communication channels, but even on physical lines or tone channels, you can create a very efficient network by installing the appropriate channel equipment. Good results are obtained by using Motorola 326x SDC modems which have unique capabilities of correction and compression of data in a synchronous mode. Due to this, it is possible to significantly raise the quality of the communication channel and achieve an effective speed of up to 80 Mbps and above. Short-range modems that provide fairly high speeds can also be used on short physical lines. However, high line quality is required here, as short-range modems do not support any error correction. Widely known short-range RAD modems, as well as PairGain equipment, allow reaching a speed of 2 Mbps on physical lines about 10 km long. X.25 network access nodes, as well as proprietary communication nodes, can be used to connect remote users to the corporate network. In the latter case, you need to allocate the required number of telephone numbers (or ISDN channels) which can be too expensive. If you want to connect a large number of users at the same time, the cheaper option may be to use access nodes of the X.25 network even in one city.

Computer network developers and network administrators always strive to meet three basic network requirements, namely: scalability, productivity, and controllability. Good scalability is necessary so that both the number of users working in the network and the application software can be changed without much effort. High network performance is required for the normal operation of most modern applications. Finally, the network must be easy enough to manage so that it could be reconfigured to meet the ever-changing needs of the organization. These requirements reflect a new stage in the development of network technologies – the stage of creating high-performance corporate networks [4]. In modern conditions for the correct design of the network, its development and maintenance, professionals must take into account the following issues:

- change of organizational structure – during the project implementation, it is not necessary to "separate" software and network specialists. It is a case when developing networks and the system as a whole requires a single team of specialists of different profiles;
- use of new software – it is necessary to get acquainted with the new software at an early stage of network development in order to be able to make timely adjustments to the planned use of the tool;
- study of different solutions – it is necessary to evaluate different architectural solutions and their possible impact on the future network;
- inspection of networks – it is necessary to test the whole network or its parts at the early stages of development;
- choice of protocols – to choose the right network configuration, you need to evaluate the capabilities of different protocols. It is important to determine how network operations that optimize the performance of one program or software package can affect the performance of others;
- calculation of critical time – it is necessary to determine the allowable response time of each program and the possible periods of maximum load. It is important to understand how emergencies can affect the performance of the network, and to determine whether a reserve is needed to organize the continuous operation of the enterprise;
- analysis of options – it is important to analyze different options for using software online. Centralized storage and processing of information often create additional workload in the center of the network, and distributed computing may require the strengthening of local area networks of working groups [5].

Today there is no ready-made, well-established universal methodology, following which it is possible to automatically carry out a full range of measures to develop and create a corporate network. This is essential that there are no two exactly alike organizations. In particular, each organization is characterized by a unique leadership style, hierarchy, and business culture. Before starting to build a corporate network, it is necessary to first determine its structure, functional and logical organization and take into account the existing telecommunications infrastructure.

The structure of the network is the basis of the technical task for creating a network. It should be noted that the structure of the network differs from the network design. For example, it does not define the exact schematic diagram of the network and does not regulate the location of network components. The structure of the network, for instance, determines whether some parts of the network will be based on Frame Relay, ISDN or other technologies.

The network design must contain specific instructions and parameter estimates, such as the required bandwidth value, the actual bandwidth, the exact location of the communication channels, etc. In the structure of the network, there are three aspects, three logical components: the principles of construction, network templates, and technical positions. The principles of construction are used in network planning and decision-making. Principles are a set of simple instructions that describe in sufficient detail all the issues of building and operating a network deployment over a long period of time. As a rule, the basis for the formation of principles is corporate goals and basic methods of doing business in the organization. The principles provide the primary link between corporate development strategy and network technology. They are used to develop technical positions and network templates. When developing a technical task for the network, the principles of building a network architecture are set out in the section that defines the overall objectives of the network. The technical position can be considered as a target description that determines the choice between competing alternative network technologies. This position specifies the parameters of the selected technology and gives a description of a single device, method, protocol, service provided, etc. The number of technical positions is determined by a given degree of detail, the complexity of the network, and the scale of the organization [5].

The structure of the network can be described by the following technical aspects:

– Network transport protocols. What transport protocols should be used to transmit information?

– Network routing. What routing protocol should be used between routers and switches?

– The quality of service. At the expense of what the possibility of a choice of quality of service will be reached?

– Addressing in IP networks and addressing domains. What address scheme should be used for the network, including registered addresses, subnets, subnet masks, forwarding, etc.?

– Switching in local networks. What switching strategy should be used in local networks?

– A combination of switching and routing. Where and how switching and routing should be used; how should they unite?

– Organization of the city network. How should the branches of the enterprise, say, in one city, communicate?

– Organization of a global network. How should branch offices communicate with the global network?

– Remote access service. How do remote branch users access the enterprise network?

The first step in building a corporate network describes the intended functional structure. The quantitative composition and status of offices and branches are determined. The necessity of deployment of own private communication network is substantiated or the choice of the service provider which can satisfy the requirements. The development of the functional structure is carried out by taking into account the financial capabilities of the organization, long-term development plans, the number of active network users running applications, and the required quality of service. The development is based on the functional structure of the enterprise.

The second step determines the logical structure of the corporate network. Logical structures differ from each other only by the choice of technology (ATM, Frame Relay, Ethernet) to build the backbone which is the central link of the corporation's network. Consider the logical structures built on the basis of cell switching and frame switching. The data bus must meet two main requirements: the ability to connect a large number of low-speed workstations to a small number of powerful, high-speed servers, and an acceptable response rate to customer inquiries. The ideal backbone should have high reliability of data transmission and a developed control system. The control system should be understood, for example, as the ability to configure the highway, taking into account all local features and maintaining reliability on the level, that even if some parts of the network fail, the servers remain available. The cell-switched logical structure is used in networks with real-time multimedia traffic (video conferencing and high-quality voice transmission). It is important to assess the need for such an expensive network and, if necessary, to take as a basis the logical structure of the network with switching frames. The logical switching hierarchy, which combines two levels of the OSI model, can be represented as a three-level scheme:

– the lower level is used to connect local Ethernet networks;

– the middle layer is either a local area network, or a MAN network, or a WAN backbone network;

– the upper level of this hierarchical structure is responsible for routing.

The logical structure allows the identification of all possible communication routes between individual sections of the corporate network.

4. Designing an existing corporate LAN in 10-Strike: Network Scheme software

When developing a corporate network and a security system for it, it is necessary to build an existing network and consider its main components, namely their functions and roles in the structure of the local network. In order to analyze the functions and roles of network elements, we use the software 10-Strike: Network Scheme. It is designed to build network diagrams for Windows and allow scanning the network topology and finding all connected devices. All detected computers, switches and routers are placed on the circuit. If the switches support SNMP, the program will determine the network topology and draw connections between devices automatically. Trace route and LLDP protocol are also supported. It is convenient to refine the network topology scheme with the help of the built-in editing tools, complete connections, apply inscriptions, draw areas, and fill them with different colors and textures. The program contains a large library of vector icons of network devices. There can be distinguished the following stages of designing an existing corporate LAN:

1. Opening 10-Strike: Network Diagram and click on the toolbar File, Create Network Map.

2. Choosing the method of detecting computers on the network. In this window, we must choose one of three detection methods:

• scanning the range of IP addresses (recommended) allows detecting the maximum number of devices, identifying their type, OS version, other properties, and if there are switches, building a network diagram;

• import from a network environment is a quick way but not all devices can be detected;

• tracing allows building a scheme of connecting hosts to the Internet.

3. Setting the start and end IP addresses.

4. Setting the scanning method and parameters.

5. Search for and selection of computers for placement on the map. Selection of the required devices with ticks.

6. Saving the map to a file. Selection of the required parameters with ticks.

The result will be the following network diagram (Fig. 1).

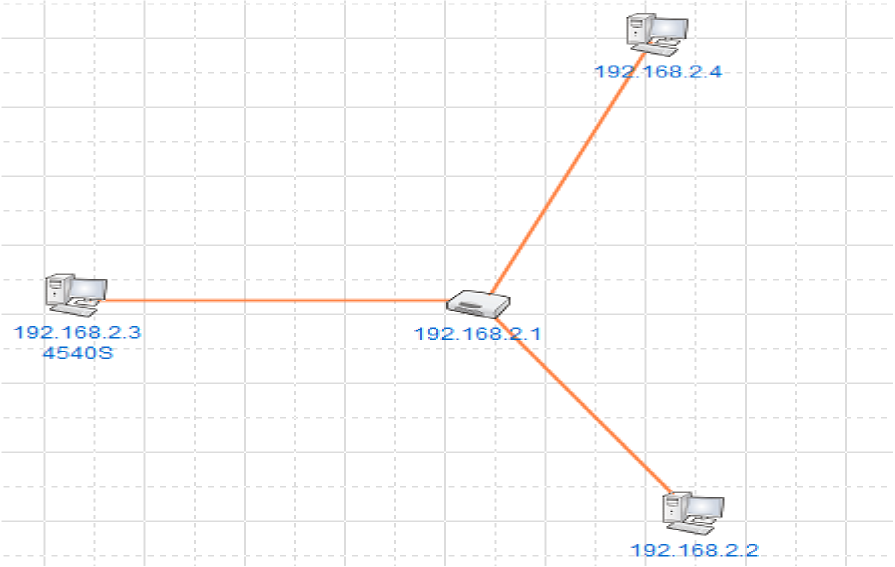

Figure 1 – An example of a network diagram obtained after using the program

In the process of building the existing network structure (scheme), the program builds logical connections between equipment and identifies the type of equipment (switch, computer, printer, etc.), so to fully understand the network structure, additional identifiers were applied to the equipment and namely to those who work with a particular computer (a specified position). Based on the obtained scheme of the corporate computer network, it is advisable to design new security systems and modern technologies for corporate network organization.

5. Conclusions

Systems and security of corporate computer networks play an important role in the process of organizing the protection of information resources of a company or organization. The organization of safe operation of corporate networks in an open environment is an urgent task. Solving this problem requires the use of mutually agreed comprehensive measures, the selection and implementation of which the article is devoted. The main tasks and features of corporate networks are determined, to which it is possible to distinguish the complexity of the coverage of management functions, efficient use of computer and telecommunications equipment and software, adaptability of the functional and instrumental structure of the system to the features of the controlled object, etc. In addition, a scheme of a corporate computer network and means of ensuring its security are proposed.

REFERENCES

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.

2. Эделман Дж., Лоу С.С., Осуолт М. Автоматизация программируемых сетей / пер. с англ. А.В. Снастина. М.: ДМК Пресс, 2019. 616 с.

3. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020. 1008 с.

5. Диогенес Ю., Озкайя Е. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.

Стаття надійшла до редакції 11.04.2022