Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Of Computer Information Systems and Software Engineering
(Full name of faculty)
Computer science Department
(Full name of department)

QUALIFYING PAPER

For the degree of

bachelor
(Degree name)

topic: Development of an information security system
in the local computer network in the enterprise

Submitted by: fourth year student, group ICH-42
Specialty: 122 Computer science
(Code and name of specialty)

		Olajuwon Bankole Emmanuel
	(signature)	(Surname and initials)
Supervisor		Holotenko O.S.
	(signature)	(Surname and initials)
Standards verified by		
	(signature)	(Surname and initials)
Head of Department		Bodnarchuk I.O.
	(signature)	(Surname and initials)
Reviewer		
	(signature)	(Surname and initials)

Ternopil
2023

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Of Computer Information Systems and Software Engineering
(Full name of faculty)

Department Computer science Department
(Full name of department)

APPROVED BY

Head of Department

Bodnarchuk I.O.

(signature) (Surname and initials)

« » 2023 p.

ASSIGNMENT

for QUALIFYING PAPER

for the degree of *bachelor*
(Degree name)

specialty *122 Computer science*
(Code and name of the specialty)

student **Olajuwon Bankole Emmanuel**

1. Paper topic: Development of an information security system in the local computer network in the enterprise

Paper supervisor: Holotenko Oleksandr Serhiyovych,, PhD, Assoc. Prof.
(Surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of «___» _____ 2023 №____.

2. Student's paper submission deadline 10/07/2023

3. Initial data for the paper *Development of an information security system in the local computer network in the enterprise development environment for PC, assessment of the relevance of infrastructure threats, crypto provider in the data protection system.*

4. Paper contents (list of issues to be developed) *1. Analysis the methods of information protection in local area networks. 2. Protection of information in llc "oilgroup". 3. Occupational safety and health.*

5. List of graphic material (with exact number of required drawings, slides) 1. *Relevance of the work. 2. The main purpose of work, the object of study, subject of research. 3. Tasks of the work.*

4. System components. 5. Threat and dangers in local area Network. 6. Channels of information leakage. 7. Basic Security Service. 8. Protection of information in LLC "OILGROUP". 9. Analysis of the vulnerability of the enterprise. 10. Potection solution Recommendation. 11. Crypto provider in the data protection system. 12. Occupational Health and Safety. 13. Conclusions.

6. Advisors of paper chapters.

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
Occupational safety and health			

7. Date of receiving the assignment.

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
	Analysis of technical task		
	Analysis of characteristics of the object		
	Analysis methods of information protection		
	Information resources and services		
	Assessment of the relevance of infrastructure threats		
	Development of crypto provider in the data protection system		
	Occupational safety and health		
	Graphic materials		
	Preparation to the qualification work presentation		
	Qualification work presentation		

Student _____ Olajuwon Bankole Emmanuel
(signature) (surname and initials)

Paper supervisor _____ Holotenko O.S.
(signature) (surname and initials)

ABSTRACT

Development of an information security system in the local computer network in the enterprise //Qualifying paper // Olajuwon Bankole Emmanuel // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, group ICH-42 //Ternopil, 2023 // p. - 50, fig. - 14, tabl.- 4, bibliogr. - 15.

Keywords: Ethernet, physical topology, network equipment, switching, routing, sharing services, system, IoT, smart technologies.

In this diploma thesis developed a "Smart Office" project based on the Internet of things (IoT) technologies. Basic documentation has been prepared: subsystem operation algorithm, the basic electrical scheme, functional scheme, ccomparison of data providers. A programming language and appropriate development tools have been chosen, the structural elements of the subsystem and its web interface in configuration mode have been developed. The created subsystem fully satisfies the requirements and successfully accomplishes all assigned tasks.

TABLE OF CONTENT

INTRODUCTION 6

1 ANALYSIS THE METHODS OF INFORMATION PROTECTION IN LOCAL AREA NETWORKS 8

1.1 Threats and dangers in a Local Area Network 8

1.1.1 Unauthorized Access and Information Leakage: 8

1.1.2 Destructive Software Tools. 11

1.2 Methods and Means of Information Protection: 14

1.2.1 Methods and Approaches to Information Protection 14

1.3 Basic Security Services 16

1.3.1 User Identification and Authentication 16

1.3.2 Access control 21

1.3.3 Logging and auditing 21

1.3.4 Cryptography 22

1.3.5 Screening 23

2 PROTECTION OF INFORMATION IN LLC "OILGROUP" 25

2.1 Composition of information exposed to threats 25

2.2 The enterprise network and software 26

2.3 Analysis of the vulnerability of the enterprise 27

2.3.1 Possible ways of implementing threats in OILGROUP 27

2.3.2 Assessment of the relevance of infrastructure threats 28

2.4 Protection Solution Recommendations 30

2.4.1 Firewall Installation 30

2.4.2 Installing a crypto provider in the data protection system 32

2.4.3 Installation of intrusion detection and antivirus 37

3 OCCUPATIONAL SAFETY AND HEALTH 41

3.1. General characteristics of the room and workplace 41

3.2 Analysis of potentially dangerous and harmful production factors in the workplace 44

Conclusions 47

REFERENCES 49

INTRODUCTION

The issue of information protection has been significant since the inception of writing. Certain information has always needed to be safeguarded and people have employed various methods to protect it. Throughout history, encryption techniques such as cryptography have been utilized. In today's era of widespread computerization, the well-being and even the lives of many people rely on the security of computer systems that process information, as well as the control and management of various entities. These entities encompass telecommunications systems, banking systems, nuclear power plants, air and land transportation control systems, and systems for processing and storing classified and confidential information. To ensure the normal and secure functioning of these systems, it is crucial to maintain their safety and integrity.

At present, there are numerous possibilities for compromising information security, including:

Eavesdropping on conversations indoors or in vehicles using pre-installed "radio bugs."

Monitoring and controlling telephones, fax lines, and radio stations.

Remotely extracting information from various technical devices, particularly over a local network, including monitors and printing devices of computers and other electronic equipment.

Laser-induced radiation of window glasses within a room.

To counteract the abundance of data collection methods, numerous organizational and technical measures, often referred to as "special protection," are employed.

The problems related to information protection in local computer networks (referred to as LANs) are consistently in the focus of attention not only for specialists involved in the development and utilization of these systems but also for a wide range of users.

Information protection involves employing special means, methods, and measures to prevent the loss of information within LANs. The extensive and widespread use of computing technology has significantly increased the vulnerability of information stored, stored, and processed within LANs. Therefore, ensuring information security is an urgent task when employing information and communication technologies.

The research is focused on the information processes taking place at the "OILGROUP" enterprise, and the subject of the study is the methods of protecting information within the corporate computer network.

The objective of the final qualification work is to enhance the level of information security at the OILGROUP enterprise by developing recommendations for ensuring data protection within the LAN and proposing solutions to prevent unauthorized access to official and classified information.

To achieve the set goal, the following tasks need to be addressed:

Identify the software and hardware components involved in processing, storing, and transmitting information within the enterprise.

Conduct an analysis of the company's vulnerabilities, including identifying potential threats, evaluating scenarios of their realization, and assessing the significance of these threats.

Develop recommendations for information protection within the enterprise.

The practical significance of this work lies in the possibility of implementing a unified security policy at the enterprise, which ensures an appropriate level of protection for official information.

1 ANALYSIS THE METHODS OF INFORMATION PROTECTION IN LOCAL AREA NETWORKS

1.1 Threats and dangers in a Local Area Network

In the context of Local Area Networks, there are two distinct aspects of information vulnerability that have been recognized:

Unauthorized Access: This refers to the risk of unauthorized individuals gaining access to information within the LAN, potentially leading to the unauthorized viewing or modification of sensitive data. Unauthorized access can compromise the confidentiality and integrity of information stored within the network.

Destructive Software Actions: This pertains to the activities of malicious software tools that can cause harm within the LAN. Such tools, often referred to as malware or destructive software, can disrupt normal network operations, compromise the availability of resources, and cause damage to the network infrastructure and data.

1.1.1 Unauthorized Access and Information Leakage:

The LAN architecture and its operational technology provide opportunities for attackers to discover or deliberately create vulnerabilities that enable covert access to information. The wide range of known malicious actions strongly suggests the existence or potential creation of numerous such vulnerabilities. Figure 1.1 illustrates various methods of unauthorized access to information.

Unauthorized access to information within the LAN can occur through two primary means:

Indirect access. This type of access does not require physical interaction with LAN elements.

Direct access. This type of access involves physical contact with LAN elements.

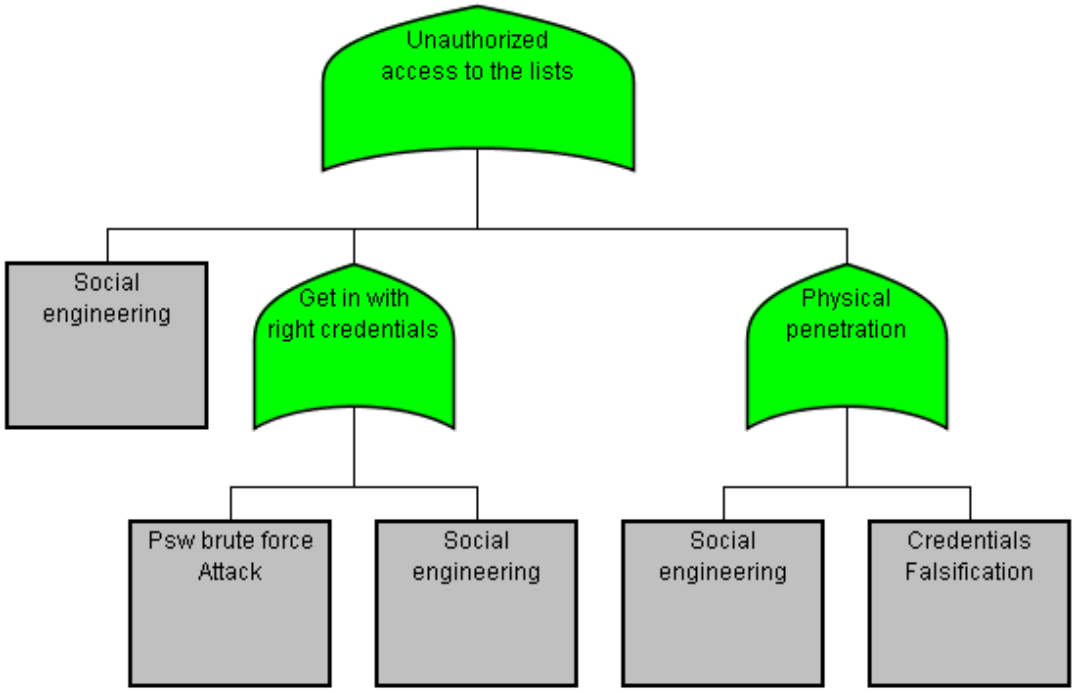


Figure 1.1 - Methods of Unauthorized Access to Information

There are several channels through which unauthorized individuals can obtain information without proper authorization. These channels include:

- Eavesdropping devices. Unauthorized individuals use listening devices to intercept and capture sensitive information.
- Remote photography. Unauthorized capture of information through remote surveillance techniques.
- Electromagnetic radiation interception. Intercepting and deciphering information by capturing electromagnetic signals emitted by network devices.
- Theft of information carriers and industrial waste. Unauthorized individuals steal physical storage devices or dispose of discarded materials containing sensitive information.
- Reading data in arrays of other users. Unauthorized access to information stored in the memory arrays of other users within the LAN.
- Copying information carriers. Unauthorized duplication of information stored on physical storage devices.

- Unauthorized use of terminals. Illegitimate utilization of user terminals to gain access to confidential information.
- Masquerading as a registered user. Stealing passwords and other credentials to impersonate a legitimate user and bypass access restrictions.
- Software traps. The use of deceptive software elements to trick users into revealing sensitive information or performing unauthorized actions.
- Obtaining protected data using authorized requests. Exploiting loopholes in authorized system requests to gain access to protected data.
- Exploiting programming language and operating system vulnerabilities. Taking advantage of weaknesses in programming languages or operating systems to gain unauthorized access.
- Intentional inclusion of Trojan horse blocks in program libraries. Deliberately inserting malicious code disguised as harmless software components.
- Illegal connection to equipment or communication lines. Illicit physical connections to network equipment or communication lines to gain unauthorized access.
- Malicious disabling of protection mechanisms. Actively disabling or bypassing security measures to gain unauthorized access.

An information leakage channel consists of an information source, a material medium or a transmission medium carrying the information signal, and a means to extract the information from the signal or medium.

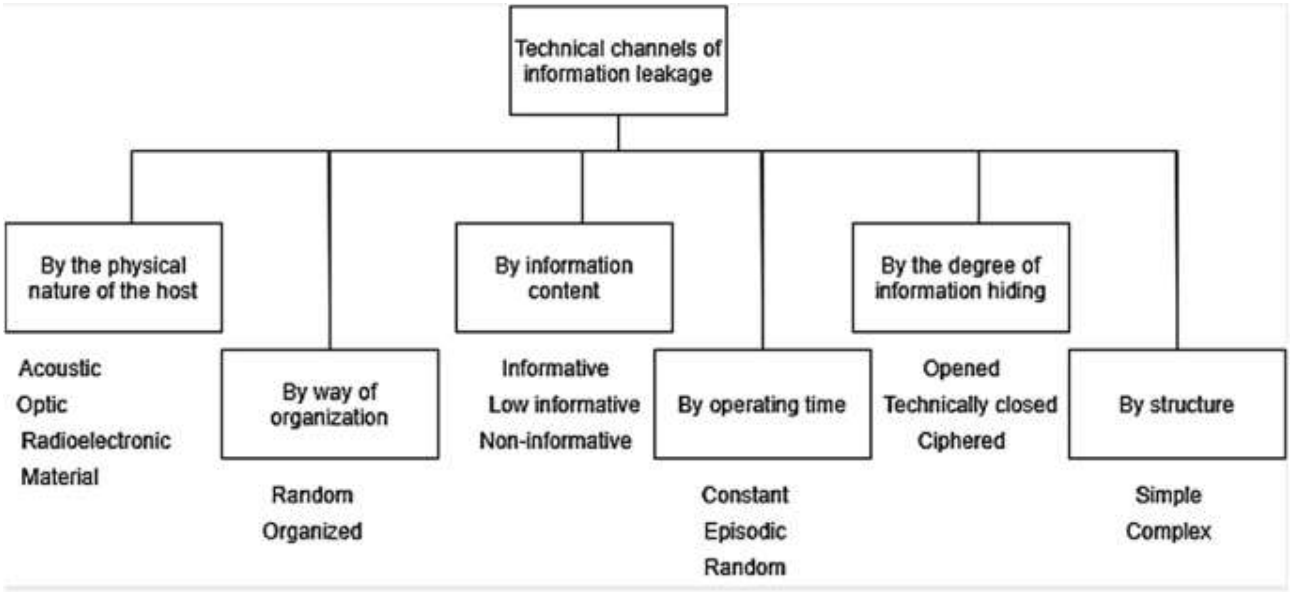
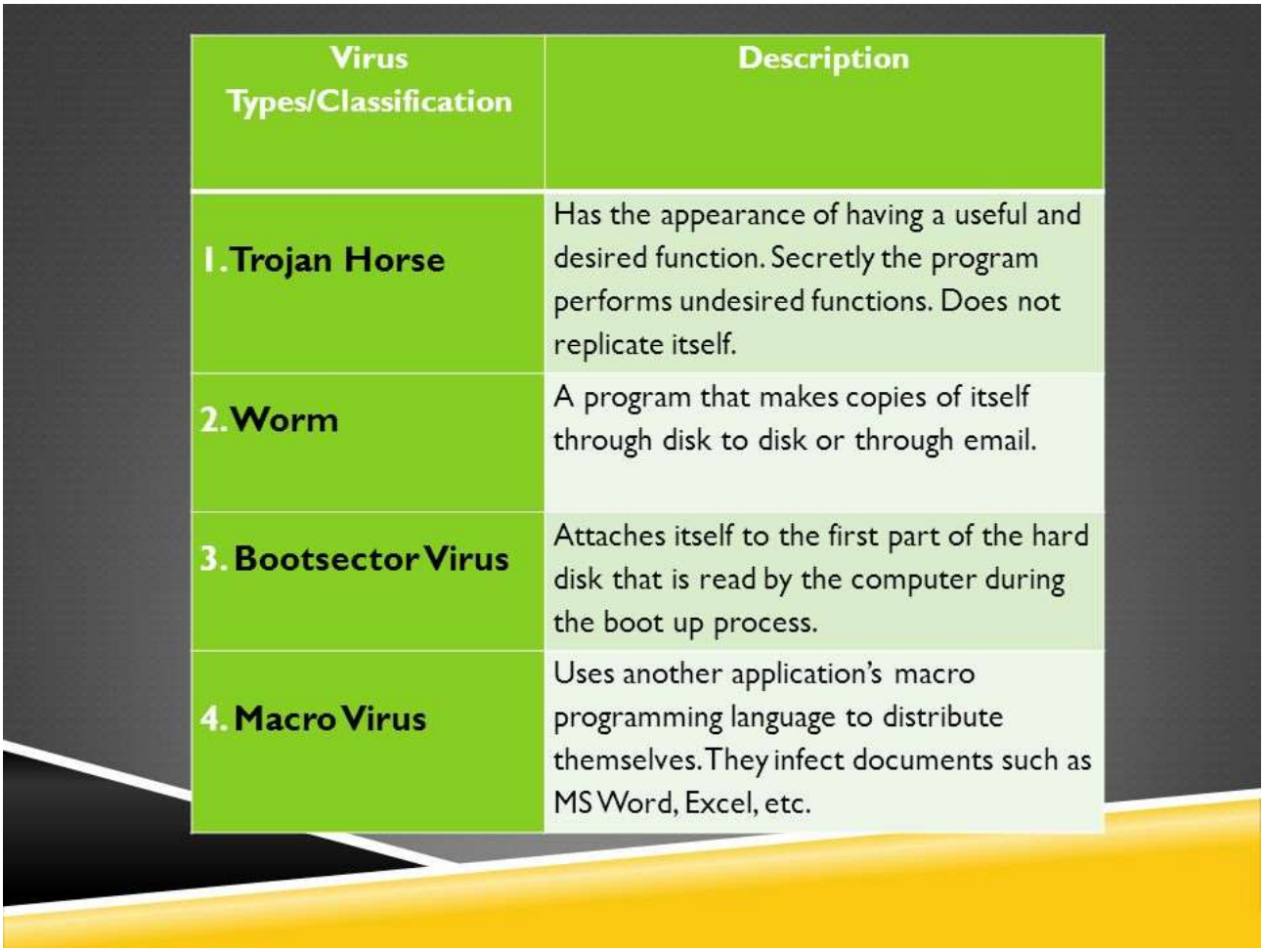


Figure 1.2 - The main channels of information leakage

1.1.2 Destructive Software Tools.

Computer viruses, Trojan horses (also known as bookmarks), and methods of penetrating remote systems through local and global networks belong to a category of destructive software tools, referred to as RPS (Figure 1.3).

A computer virus is a form of malicious software that can replicate itself and insert copies of itself into the code of other programs, system memory areas, boot sectors, and spread those copies through various communication channels. Viruses thrive on the universal interpretation of information in computer systems. They can interpret infected programs as data during the infection process and as executable code during execution. This fundamental principle is based on the von Neumann architecture used in modern computer systems.



Virus Types/Classification	Description
1. Trojan Horse	Has the appearance of having a useful and desired function. Secretly the program performs undesired functions. Does not replicate itself.
2. Worm	A program that makes copies of itself through disk to disk or through email.
3. Bootsector Virus	Attaches itself to the first part of the hard disk that is read by the computer during the boot up process.
4. Macro Virus	Uses another application's macro programming language to distribute themselves. They infect documents such as MS Word, Excel, etc.

Figure 1.3 - Types of Destructive Software

According to F. Cohen's traditional definition, "a computer virus is a program that can infect other programs by modifying them and adding its own, possibly altered, copy." The key criterion in defining a virus is its ability to self-replicate, distinguishing it from other programs. However, the "copies" of a virus can differ structurally and functionally from one another.

The current landscape is marked by two factors: the emergence of polymorphic viruses and virus generators (constructors). Polymorphic viruses pose challenges for traditional detection algorithms as each new copy bears no resemblance to its parent. This is achieved through encrypting the virus body and utilizing a decryptor that varies with each instance. Virus generators enable the creation of new viruses by specifying propagation methods, induced effects, and harm parameters to the generator program. Viruses continuously expand their "habitat" and introduce novel algorithms for infection and behavior.

A Trojan horse is a program that contains a destructive function that activates when specific triggering conditions are met. These programs are typically disguised as useful utilities. Trojan horses carry out actions related to security breaches and destructive activities. Instances of creating such programs to facilitate virus propagation have been observed.

Program bookmarks also include a hidden function that can harm a computer system. However, these functions aim to remain inconspicuous to avoid detection, as the longer a bookmark goes unnoticed, the longer it can operate.

Examples of destructive functions implemented by Trojan horses and program bookmarks include:

- Information destruction
- Information interception and transmission
- Purposeful modification of program code

While viruses and Trojan horses cause damage through self-propagation or overt destruction, destructive software operating within computer networks focuses on hacking targeted systems to breach security and integrity. This process can be automated using a specific type of destructive software known as a network worm.

Worms are viruses that spread across global networks, impacting entire systems rather than individual programs. They represent the most dangerous type of virus as they can target information systems on a national or global scale. With the advent of the global Internet, network worms pose the greatest security threat, as any of the millions of connected computers can become vulnerable to them at any given time.

1.2 Methods and Means of Information Protection:

1.2.1 Methods and Approaches to Information Protection

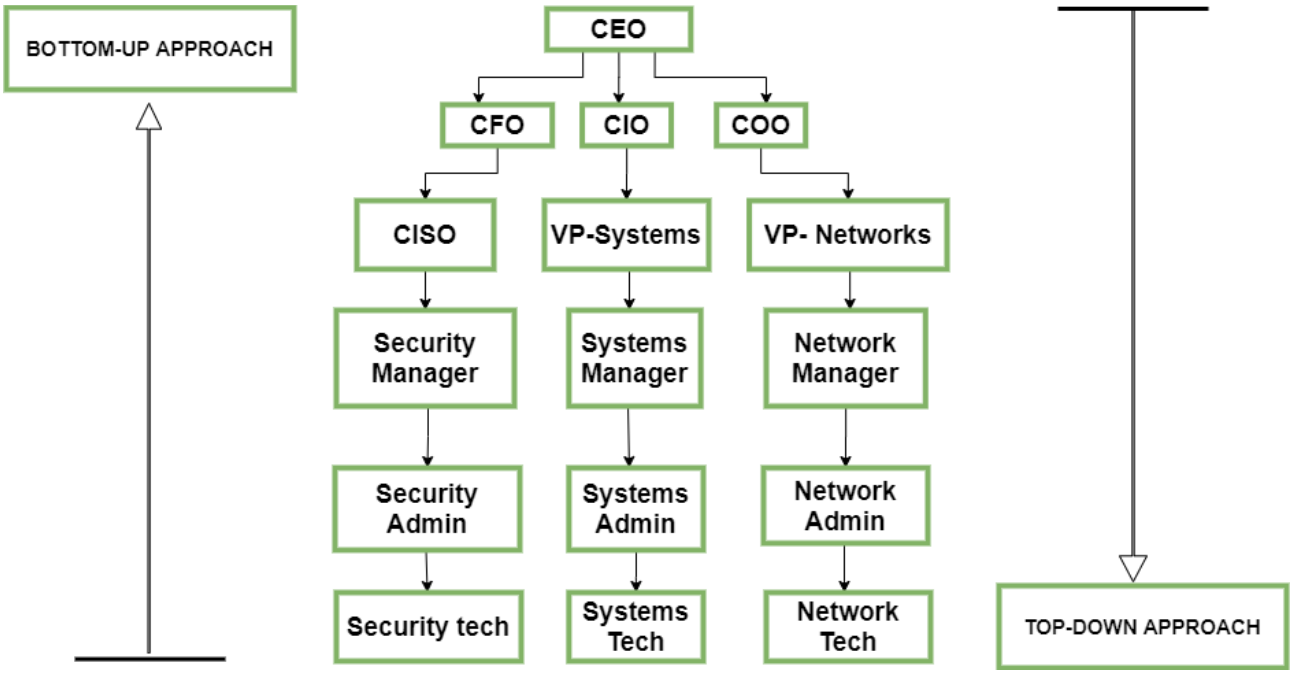


Figure 1.4 - Methods and Approaches to Information Protection in the LAN

Protecting information within a LAN involves several key elements:

1. Obstacle: This physical barrier hinders an attacker's access to protected information by securing the premises and equipment, as well as information carriers.

2. Access Control: This method regulates the use of system resources, including technical, software, and data elements. Access control incorporates several security functions, including:

- User and resource identification, assigning unique identifiers such as names, codes, and passwords to users, personnel, and system resources.
- Authorization checks to ensure compliance with regulations regarding the day of the week, time of day, requested resources, and procedures.
- Establishing and creating appropriate working conditions within established regulations.
- Logging activities related to protected resources.

- Prompt response (e.g., delaying work, refusing access, disconnection, signaling) in case of unauthorized requests.

3. Encryption: This method protects information within the LAN through cryptographic transformation. Cryptographic encryption is crucial when transmitting information over long-distance communication lines, providing reliable protection against unauthorized access.

4. Regulation: This approach involves developing and implementing measures that minimize the possibility of unauthorized access to protected information within the LAN. Effective protection requires strict regulation of the LAN's structural construction (building architecture, equipment placement), as well as organization and supervision of personnel engaged in information processing.

5. Enforcement: LAN users and personnel are compelled to comply with rules regarding the processing and use of protected information, backed by the threat of material, administrative, or criminal consequences.

These information protection methods are implemented using various means, including technical, software, organizational, legislative, and moral and ethical measures.

Organizational Means: These measures are implemented during LAN creation and operation to ensure information protection. They encompass all structural elements, from premises construction and system design to equipment installation, testing, inspections, and ongoing operation.

Legislative Means: These include legal acts that regulate the use and processing of information with restricted access, as well as define measures of responsibility for violating these rules.

Moral and Ethical Means: These encompass norms developed within a specific country or society, establishing behavioral standards for information processing and usage. While not enforceable by law, non-compliance often leads to loss of authority and prestige.

1.3 Basic Security Services

1.3.1 User Identification and Authentication

Identification and authentication serve as the foundation for information system protection, as all protection mechanisms operate based on named subjects and objects within the system. Identification involves assigning a personal identifier to access subjects and objects and comparing it with a given list. It establishes authenticity, determines the authority of the subject upon system admission, controls established privileges during the session, and enables action logging. Authentication, on the other hand, involves verifying the identity of the access subject and confirming its authenticity.

Figure 1.5 illustrates the general procedure of user identification and authentication when accessing the system. Once the subject's authenticity is established during authentication, the information protection system must determine their set of rights or privileges for subsequent control and access delimitation.

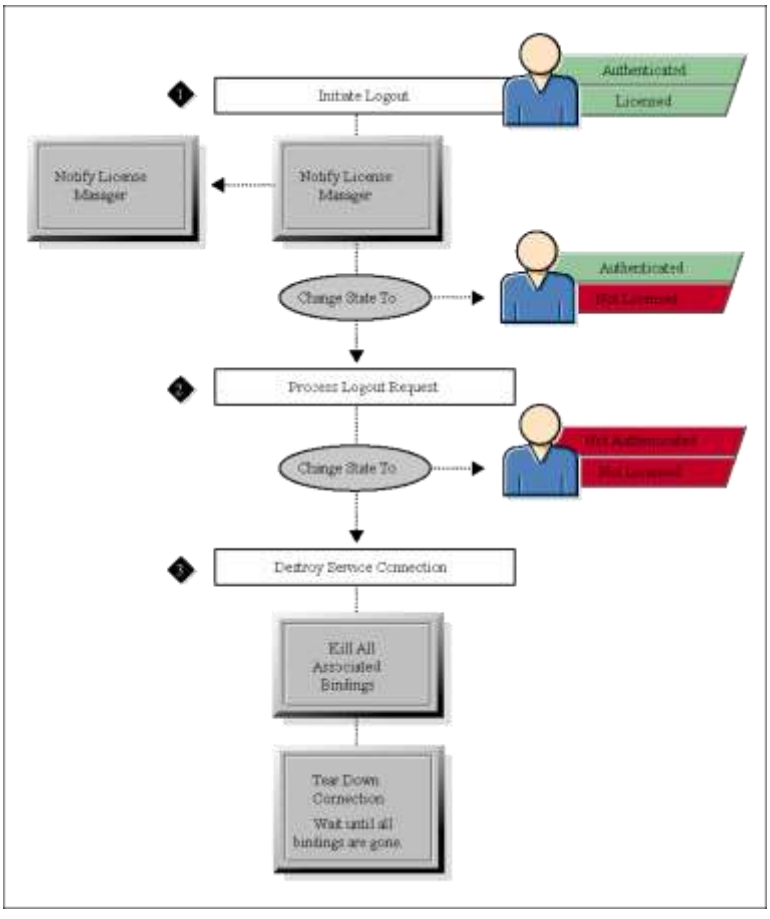


Figure 1.5 - Classic identification and authentication procedure

Authentication methods can be categorized based on the controlled component of the system. Communication partner authentication is used to establish and periodically verify connections during a session, preventing threats like masquerade and session replay. Data source authentication, on the other hand, confirms the authenticity of a specific data source.

Authentication can be classified as one-way (user proving authenticity to the system, such as during login) or two-way (mutual) authentication based on the direction of the process.

Authentication methods are commonly classified based on the means used, resulting in four groups:

1. Knowledge-based methods: These methods rely on secret information known to the authorized person, such as passwords.
2. Token-based methods: These methods use unique physical items like tokens or electronic cards.
3. Biometric-based methods: These methods measure physiological or behavioral attributes of a living organism, such as biometric parameters of a person.
4. User-associated information methods: These methods utilize information associated with the user, such as their coordinates.

The most common and familiar authentication methods are password-based methods, where the subject enters their password, which is compared to the stored encrypted password in the reference database by the authentication subsystem. If they match, access to the system's resources is granted.

Password methods can be classified based on the degree of password changeability:

- Methods using permanent passwords that are repeatedly used.
- Methods using one-time or dynamically changing passwords.

Most operating systems employ multiple-use passwords, where the user's password remains unchanged throughout a specific validity period set by the system administrator. While this simplifies administration procedures, it increases the risk of password compromise. There are various ways to crack a password, from shoulder

surfing to intercepting communication sessions. The probability of an attacker cracking a password increases if it carries a semantic load (e.g., a birthday or a person's name), is short, typed in a single case, has no expiration limitations, etc. It is crucial to consider whether the password is allowed only in dialog mode or if it can be withdrawn from the program, as the latter allows the launch of password-cracking programs.

A more secure approach involves using one-time or dynamically changing passwords. Various methods of password protection based on one-time passwords exist, including modifying simple password schemes, request-response methods, and functional methods.

In the first case, a user is provided with a list of passwords. During authentication, the system prompts the user for a password, the number of which in the list is determined randomly. The length and position of the initial character of the password can also be set randomly.

The "request-answer" method involves the system asking the user general questions, the correct answers of which are only known to the specific user.

Functional methods rely on special password conversion functions that change the user's passwords over time according to a specific formula. These methods minimize the transfer of any information that could be exploited by an attacker.

In some cases, it may be necessary for a user to verify the authenticity of a remote user or an operating system they are attempting to access. The "handshake" method is suitable for this purpose as it does not exchange any confidential information between the participants.

It should be noted that authentication methods based on one-time passwords also do not provide absolute protection. For example, if an attacker has the ability to connect to the network and intercept transmitted packets, they can send those packets as their own.

Combined methods of identification have become more prevalent recently, requiring both a password and the presence of a card (token) - a special device that confirms the subject's authenticity. Cards can be passive (with memory) or active (smart cards). Passive cards with a magnetic stripe are commonly used, where the user

enters their identification number and, if it matches the encoded electronic option on the card, they gain access to the system. This approach ensures reliable identification of the person accessing the system and eliminates unauthorized use of the card by intruders. This method is often referred to as two-factor authentication. In some cases, cards are used by themselves for physical access control, without requiring a personal identification number.

The advantage of using cards is that the authentication information processing is performed by a reading device without being transferred to computer memory, which eliminates the possibility of electronic interception on communication channels. However, passive cards are more expensive than passwords, require special reading devices, and involve specific procedures for secure accounting and distribution. Smart cards, on the other hand, have their own microprocessor and offer various options for password protection methods. They are multifunctional and can be used not only for security purposes but also for financial transactions. The drawback of cards, including smart cards, is their higher cost.

A promising development in card technology is their integration with the PCMCIA (PC Card) portable system expansion standard. These portable PC Card devices, inserted into a PC Card slot, eliminate the need for special reading devices. However, they are currently expensive.

Authentication methods based on the measurement of human biometric parameters provide almost 100% identification accuracy, addressing the challenges of lost passwords and personal identifiers. However, these methods cannot be used to identify processes or data objects due to ongoing development and challenges related to standardization and distribution, as well as the requirement for complex and expensive equipment.

Examples of biometric methods include fingerprint recognition, iris scanning, retina scanning, hand geometry, facial recognition, signature analysis, voice timbre analysis, and keyboard handwriting analysis. Biometric characteristics are also being used in intelligent payment cards, access tokens, and elements of cellular communication.

Authentication based on fingerprint scanning is universal, relatively inexpensive, and widely promoted by law enforcement agencies due to electronic fingerprint archives. Hand geometry devices are used when fingerprint scanners are impractical, such as in muddy or injured conditions, and have a lower biological repeatability. Iris scanning devices provide the highest accuracy, with a theoretical probability of shell coincidence of 1 in 10^78. Thermal imaging of the face allows for identification at a distance and is used in combination with database search for authorized person identification and outsider screening. Voice verification is convenient for telecommunication applications and has a relatively low probability of error. Keyboard input monitoring tracks speed and intervals between key presses. Signature digitizers are used to verify handwritten signatures.

A new trend is the use of location-based authentication, which utilizes space navigation systems like GPS (Global Positioning System). GPS equipment allows users to repeatedly send their coordinates to specific satellites. The authentication subsystem, aware of the satellite orbits, can determine the user's location with high accuracy. This authentication method is highly reliable due to unpredictable fluctuations in satellite orbits and constantly changing coordinates, making interception impossible.

Based on the level of information security, authentication tools can be classified into three categories: static authentication, stable authentication, and permanent authentication. Static authentication provides protection against unauthorized access in systems where intruders cannot read authentication information during the session. Examples of static authentication include traditional permanent passwords, where their effectiveness depends on the difficulty of guessing and their level of protection. Stable authentication utilizes dynamic authentication data that changes with each session, such as systems using one-time passwords and electronic signatures. Strong authentication protects against attacks where an attacker can intercept authentication information and attempt to use it in subsequent sessions. Permanent authentication provides identification for each block of transmitted data, safeguarding it from unauthorized modification or insertion. An example of permanent authentication is the

use of algorithms to generate electronic signatures for each bit of transmitted information.

1.3.2 Access control

Access control tools regulate the actions that user subjects and processes can perform on objects within the system. Logical access control, implemented through software, is the primary mechanism in multi-user systems for ensuring confidentiality, integrity, and availability by preventing unauthorized users from accessing resources. Access rights control is performed by various software components, such as the operating system core, additional security tools, databasemanagement systems, and intermediary software. When making access decisions, information such as subject identifiers (user identifiers, network addresses), entity attributes (security labels, user groups), location, time, and internal service limitations are typically analyzed.

1.3.3 Logging and auditing

Logging involves the gathering and accumulation of information concerning events occurring within the information system of a company. Each service within the system has its own set of potential events, which can be categorized as external events resulting from the actions of other services, internal events caused by the service itself, and client events triggered by users and administrators.

Audit refers to the analysis of the accumulated information, conducted either promptly in near-real-time or periodically. The implementation of logging and auditing serves several objectives:

Ensuring accountability of users and administrators: By recording all actions, it acts as a deterrent against illegal operations. Detailed logging can be employed when there is suspicion of dishonest behavior by a particular user, enabling investigation into potential security breaches and the ability to revert incorrect changes, thereby preserving information integrity.

Reconstruction of event sequences: This facilitates the identification of weaknesses in service protection, enables the detection of intruders, assessment of the extent of damage caused, and restoration of normal operations.

Detection of information security violations: Logging and auditing help identify requests that have violated information security policies, allowing for prompt action and mitigation of potential risks.

Provision of information for problem identification and analysis: By identifying bottlenecks and analyzing problems, the accessibility of the system can be improved. This may involve reconfiguring or adjusting the system, conducting performance measurements, and implementing necessary improvements.

In summary, logging and auditing play a crucial role in ensuring accountability, detecting security breaches, reconstructing event sequences, and improving system accessibility and performance..

1.3.4 Cryptography

Cryptography plays a crucial role in ensuring the confidentiality and integrity of information, serving as a fundamental component of various software and technical security measures. It acts as the final line of defense in protecting sensitive data.

There are two primary methods of encryption: symmetric and asymmetric. Symmetric encryption involves using the same key for both encrypting and decrypting messages. It offers highly effective encryption techniques, and a standard algorithm called "Information processing systems. Cryptographic protection. Algorithm of cryptographic transformation" exists for such methods.

However, symmetric encryption has a significant drawback. The secret key must be known to both the sender and the recipient, which introduces challenges in key distribution. Moreover, the recipient, upon receiving an encrypted and decrypted message, cannot prove that it originated from a specific sender since they could have generated the same message themselves.

Asymmetric methods, on the other hand, utilize two keys: a non-secret key for encryption (which can be published along with the user's address) and a secret key for decryption (known only to the recipient). The RSA method (Rivest, Shamir, Adleman) is a widely used asymmetric encryption method based on operations involving large prime numbers and their products.

Asymmetric encryption methods enable the implementation of electronic signatures or electronic message verification. The sender sends two copies of the message - one in the open form and another decrypted with their secret key (which can be considered a form of encryption). The recipient can then encrypt the decrypted copy using the sender's public key and compare it with the open copy. If they match, the sender's identity and signature can be considered authentic.

However, a significant drawback of asymmetric methods is their relatively slow speed compared to symmetric methods. Therefore, they are often combined with symmetric encryption. It's worth noting that asymmetric methods are typically 3-4 orders of magnitude slower than symmetric methods. To address the key distribution problem, the message is first symmetrically encrypted with a random key, which is then encrypted with the recipient's public asymmetric key. The encrypted message and key are then transmitted over the network.

Cryptographic methods provide robust integrity control for information. Unlike traditional checksumming methods, which can only detect random errors, a cryptographic checksum (also known as a hash) calculated using a secret key practically eliminates the possibility of undetectable data modifications.

In recent times, various forms of symmetric encryption based on composite keys have gained popularity. The concept involves dividing the secret key into two separate parts that are stored independently. Each part alone does not allow decryption. If law enforcement agencies have suspicions about an individual and possess a certain key, they can obtain the key halves and proceed with symmetric decryption using standard techniques.

1.3.5 Screening

The concept of a screen refers to a mechanism that distinguishes the access of clients from one set to servers from another set within a network. It accomplishes this by controlling the flow of information between the two sets of systems.

A screen typically consists of two mechanisms: one that restricts the movement of data and another that facilitates it. In a broader sense, a screen can be represented as a sequence of filters, where each filter can either delay the data or immediately transfer

it to the other side. Some filters may even pass a portion of the data to the next filter for further analysis or processing on behalf of the intended recipient, returning the result to the sender.

In addition to access limitation functions, screens also implement information exchange protocols. Typically, a screen is not symmetrical, as it defines an "inside" and "outside" perspective. The goal of shielding is to protect the internal area from potentially hostile external sources. Firewalls, for example, are installed to safeguard the local network of an organization that has access to the open environment, such as the Internet. Another example of a screen is a port protection device that controls access to a computer's communication port independently of other system security tools.

In conclusion, this section has addressed the threats and risks associated with unauthorized access to information and has analyzed various methods and tools for protecting information within a corporate network.

2 PROTECTIONS OF INFORMATION IN LLC "OILGROUP"

2.1 Composition of information exposed to threats

The information resources within the infrastructure of LLC "OILGROUP" that are potentially vulnerable to threats include the following:

1. Target information: OILGROUP's commercial secrets, Personal data of employees of LLC "OILGROUP" and other individuals obtained during its activities
2. Technological information: Configuration data and other information about technologies, software, and technical means used for information accumulation, storage, processing, transmission, and protection Service information related to information security tools, such as identifiers, passwords, access restriction tables, cryptographic keys, security audit logs, etc.
3. Software: Software information resources of the information infrastructure of LLC "OILGROUP," including general and specialized software, software backup copies, and software related to information security tools.

Within the infrastructure of LLC "OILGROUP," the following information resources are present:

Information related to commercial secrets:

- Salary information
- Contracts with suppliers and buyers
- Production technologies

Protected information with restricted access:

- Employment contracts
- Employees' personal files
- Materials from the supply department
- Employees' personal records
- Content of accounting registers and internal accounting reports
- Other internal developments and documents

Open information:

- Information related to the firm's marketing activities
- Information on the firm's website and booklets
- Charter and founding documents
- Sales department information
- Production price list

2.2 The enterprise network and software

The enterprise network and software of LLC "OILGROUP" are based on standard network solutions. The local computing networks consist of the following components:

- Server equipment located in a separate rack (cabinet)
- Automated workplaces used by the employees
- General switching equipment and a structured cable system

Data exchange between LLC "OILGROUP" and external entities such as the tax service, pension fund, and Sberbank occurs through external networks. For cryptographic protection of accounting and reporting department data when transferring reports to the tax service and pension fund, LLC "OILGROUP" utilizes the Sprinter PC information security tool. Additionally, the Bicrypt KSB-S information security tool is used for cryptographic protection of accounting department data when transferring files to OJSC VitaBANK.

LLC "OILGROUP" employs certified, licensed, and freely distributed software in its operations.

Table 2.1 Certified soft

Software	**Quantity**
Windows 10 Pro	20
MS Office 2013	20
Windows server 2008 R2	3

As a result, the information infrastructure of LLC "OILGROUP" operates in a multi-user mode, where information processing is carried out with demarcated access rights. This mode of operation is governed by the existing laws, as well as the internal documents and official instructions of LLC "OILGROUP".

2.3 Analysis of the vulnerability of the enterprise

2.3.1 Possible ways of implementing threats in OILGROUP

During the examination of information security at the "OILGROUP" enterprise, it was determined that there are potential risks associated with unauthorized access. These threats include:

Unauthorized access to protected assets utilizing the internal infrastructure of OILGROUP.

Uncontrolled use, theft, or loss of infrastructure elements (such as printouts and information carriers) within OILGROUP.

Unauthorized visual access to protected information displayed on monitor screens or through printed documents.

Network traffic analysis, scanning of the computing network, denial-of-service attacks, identification of password information, manipulation of trusted network objects, and the imposition of false network routes using non-standard technical and software tools available to attackers.

Impersonation of infrastructure administrators within LLC "OILGROUP".

Compromise of password information for accessing the information resources of LLC "OILGROUP".

Interception of OS boot control.

The targeted and technological information, specifically commercial information, is identified as the type of resources that are potentially at risk. The violation of asset security pertains to confidentiality.

The potential consequences resulting from the realization of these threats would be unauthorized access to protected information.

2.3.2 Assessment of the relevance of infrastructure threats

Table 2.3 provides a comprehensive list of current threats to the infrastructure of LLC "OILGROUP" that were identified during the analysis of unauthorized access threats to information.

Table 2.3 - List of threats to the infrastructure of LLC "OILGROUP"

№	Угроза безопасности ПДн	Степень актуальности	Меры по противодействию угрозе	
			Технические	Организационные
1	Кража носителей информации	актуальная		Инструкция для персонала
2	Кража паролей	актуальная		Инструкция пользователя, учет паролей
3	Кражи, модификации, уничтожения информации.	актуальная	Настройка средств защиты, политика безопасности	Резервное копирование и инструкция пользователя
4	Несанкционированное отключение средств защиты	актуальная	Настройка средств защиты	Инструкция администратора безопасности
5	Действия вредоносных программ (вирусов)	актуальная	Антивирусное ПО	Инструкция по антивирусной защите
6	Недекларированные возможности ПО	актуальная	Настройка средств защиты	Сертификация
7	Установка ПО не связанного с исполнением обязанностей	актуальная	Настройка средств защиты, политика безопасности	Инструкция пользователя, инструкция администратора безопасности
8	Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная	Настройка средств защиты, политика безопасности	Инструкция пользователя
9	Выход из строя аппаратно-программных средств	актуальная	Резервное копирование	Охрана, Инструкция для персонала
10	Сбой системы электроснабжения	актуальная	Использование ИБП, резервное копирование	Охрана
11	Разглашение информации, модификация, уничтожение сотрудниками	актуальная	Настройка средств защиты, политика безопасности	Инструкция для персонала, подписка о не разглашении

12	Перехват в пределах контролируемой зоны	актуальная	Средства криптографической защиты, физическая зашита канала	Охрана
13	Угрозы удаленного запуска приложений.	актуальная	Межсетевой экран, Антивирусное ПО	
14	Угрозы внедрения по сети вредоносного ПО	актуальная	Межсетевой экран, Антивирусное ПО	
15	Угрозы утечки видовой информации	актуальная		Инструкция пользователя
16	Кража ПЭВМ	неактуальная		Пропускной режим, охрана, видеонаблюдение
17	Вывод из строя узлов ПЭВМ, каналов связи	неактуальная		Пропускной режим, охрана, видеонаблюдение
18	Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	неактуальная	Межсетевой экран	Инструкция пользователя, инструкция администратора безопасности

Therefore, based on the analysis of OILGROUP's infrastructure, the following conclusions can be drawn:

1. Computer theft is not a significant concern due to 24-hour access control, locked doors, and the requirement for special passes to remove computer equipment from the building.
2. Disabling computer nodes and communication channels is also irrelevant due to the access control measures and locked doors implemented in the building.
3. Actions aimed at intercepting PEMIN and acoustic information are deemed irrelevant as the majority of sensitive data is consolidated and stored on a separate database server within a controlled area, minimizing the probability of external intrusion or physical destruction of data.

To enhance the software and hardware complex for computer information protection, the following recommendations are proposed:

- Implement network perimeter protection by selecting an appropriate

firewall.

- Choose cryptographic means of protection against NSD (unauthorized access).
- Determine means of detecting intruders and implementing antivirus measures.

2.4 Protection Solution Recommendations

2.4.1 Firewall Installation

Regarding IP protection decisions, the installation of a firewall is recommended as one of the primary measures. Firewalls provide external protection against unauthorized access and are designed to safeguard computer networks or individual nodes from external attacks. In the case of OILGROUP, the UserGate Proxy & Firewall 5.2 F software firewall is recommended as an effective and cost-efficient solution for protecting confidential information and data within the corporate network.

The UserGate Proxy software offers comprehensive network security features and employs modern methods to combat Internet threats. It allows for secure network interaction, traffic accounting, and protection of the local network from external threats. The software has been certified as a network shielding and secure Internet access tool for protected systems.

The UserGate Proxy solution offers several benefits, including:

- Support for PPTP and L2TP protocols for connecting the VPN server with VPN clients within the local network, enabling remote access to network resources.
- Definition of Internet access policies and full control over Internet traffic usage within the company, with detailed statistics.
- Creation of rules to control data transmission speed between the local network and the Internet, limiting traffic volume and time spent on the network for users and groups.
- Simplification of network administration tasks.

Figures 2.1 to 2.3 demonstrate examples of the UserGate Proxy & Firewall's

functionality. The price of the product is 6,075$.

Note: It's important to mention that the information provided in the response is based on the context provided and should be verified and adapted to the specific needs and requirements of OILGROUP before implementation.

The UserGate Proxy & Firewall 5.2 F software complex has received Certificate No. 2076 dated April 19, 2010, issued by the Federal Service for Technical and Export Control (FSTEC) of Russia. This certificate confirms that the UserGate Proxy & Firewall 5.2 F software complex is compliant with ZB requirements and has been evaluated with a trust level of OUD2 for OK. Additionally, it meets the criteria of class 4 RD ME and level 4 RD NDV, making it suitable for use in creating Access Control (AC) systems up to and including class 1G.

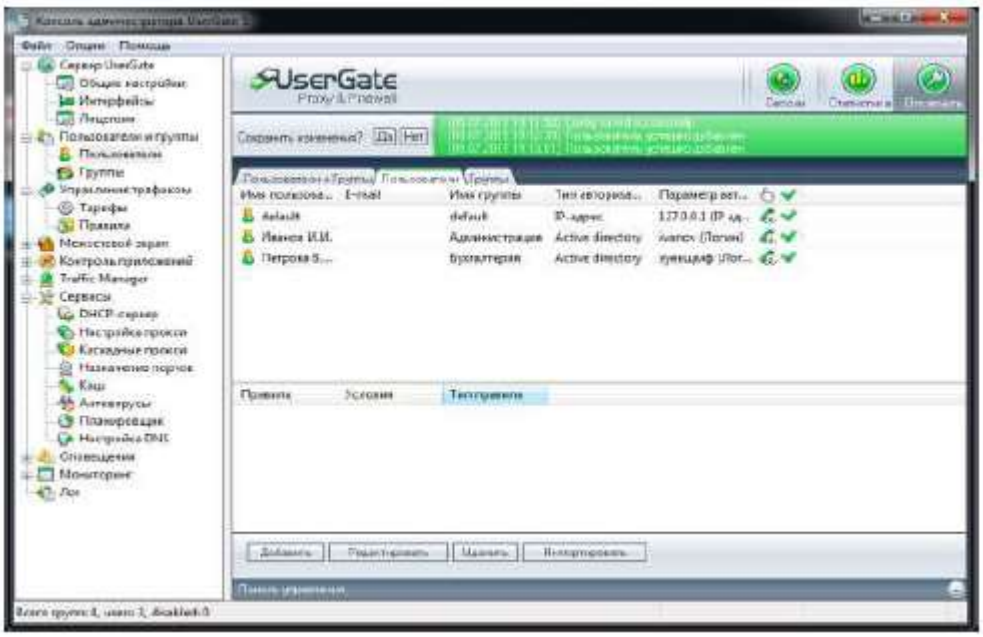


Figure 2.1 - Administrator interface in UserGate Proxy & Firewall

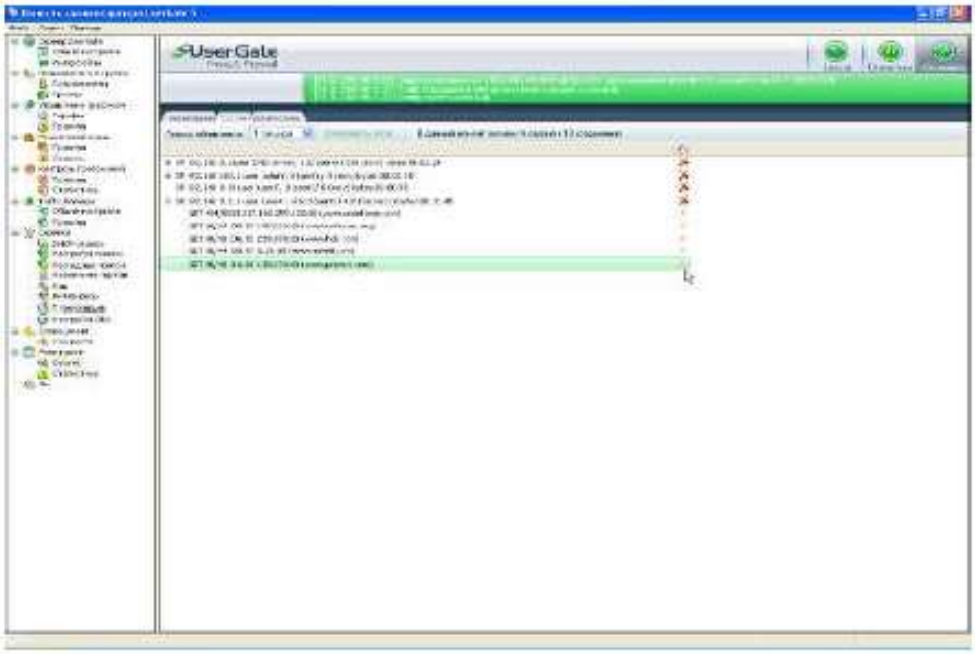


Figure 2.2 - Session control in UserGate Proxy & Firewall

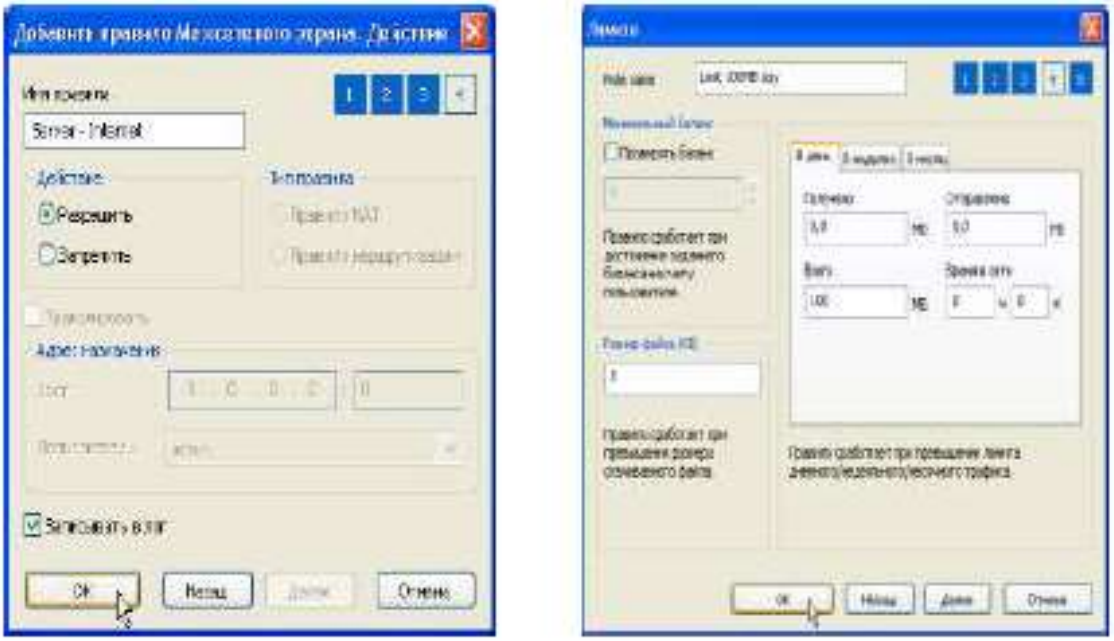


Figure 2.3 - Configuring traffic restrictions and network screening

2.4.2 Installing a crypto provider in the data protection system

Cryptographic means of protection against NSD should adhere to the following GOST standards on cryptography:

"Information technology. Cryptographic protection of information. Processes of formation and verification of an electronic digital signature."

"Information technology. Cryptographic protection of information. Hashing function."

"Information processing systems. Cryptographic protection. Cryptographic transformation algorithm."

One notable cryptographic protection tool is "ViPNet CSP," which is suitable for protecting information in Access Control systems up to 1B and Personal Data Information Systems up to 1 class inclusively. The features and capabilities of "ViPNet CSP" include:

1. Generating encryption keys and electronic signature keys, as well as data encryption and impersonation protection.
2. Ensuring the integrity and authenticity of information. "ViPNet CSP" can be used by state and commercial organizations, as well as individuals, by embedding it in application software.
3. Facilitating the storage and processing of personal data, confidential, official, commercial, and other non-state secret information, along with facilitating the exchange of such information and the legal significance of electronic document management.
4. Enabling the exchange of information in electronic form among government bodies, local self-government bodies, organizations, and individuals.

"ViPNet CSP" is not only designed for use in ViPNet software produced by OJSC "InfoTeKS," but it can also be integrated into application software developed by other manufacturers and delivered to end-users. It provides the following functionalities:

- Creation and verification of electronic signature keys according to the GOST R 34.10-2001 algorithm.
- Data hashing according to the algorithm.
- Data encryption and impersonation protection according to the algorithm. It includes the generation of random and pseudo-random numbers and encryption of session keys.

- Authentication and session key generation during data transfer using SSL/TLS protocols. Public key certificates can be stored directly in the key container.
- Support for various key storage devices such as eToken, ruToken, Shipka, etc.

For encryption and electronic signature verification, the cryptoprovider ViPNet CSP utilizes the public key contained in the recipient's certificate for the encrypted document or the sender's certificate for the document with the electronic signature. Decryption and creation of an electronic signature require the use of the user's private key (specified by the user). The process of sending a confidential Outlook message is depicted schematically in Figure 2.4.

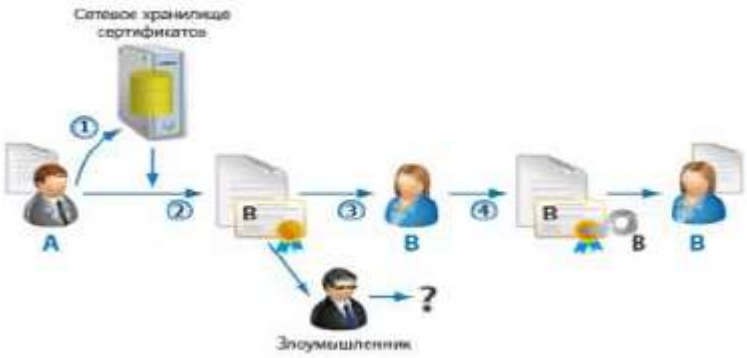


Figure 2.4 - Scheme of exchange of protected documents

To send a confidential Outlook message from User A to User B, the following steps are taken:

User A requests User B's public key certificate from the network storage and verifies it against User B's contact information in the Outlook program.

User A encrypts the document using User B's public key obtained from the certificate.

User A sends the encrypted message to User B.

User B decrypts the document using their private key.

As a result, User B receives the confidential message from User A.

If an attacker intercepts the message, they will be unable to read its contents since they do not possess User B's private key. If User B is unable to decrypt the message received from User A, it indicates that the message may have been altered or damaged during transit by unauthorized individuals. In such cases, User B can request User A to resend the message.

The process of creating and verifying an electronic signature is outlined below.

Figure 2.5 - The process of creating and verifying a document signature

User A intends to certify a document, such as an Outlook message, with an electronic signature to ensure that it cannot be altered by other users and that the authorship can be verified as User A. The process is as follows:

User A signs the document using their private key.

User A then distributes the signed document to all relevant parties, including users B, C, and D, or makes it publicly accessible.

User B, for example, requests User A's public key certificate from the Certificate Store.

User B verifies the document's authenticity by using User A's public key, which is stored in their certificate.

The "ViPNet CSP" cryptographic means of protection is designed to be compatible with IBM-compatible computers, including stationary, portable, and mobile devices. The recommended system configuration includes a processor with x86

or x86-64 architecture, at least 512 MB of RAM, and a minimum of 30 MB of free space on the hard disk.

To achieve a higher security class beyond K1, the use of devices certified by the FSB of Russia is necessary. These devices, such as the "electronic lock" (a hardware and software module for trusted boot), should be certified at a class no lower than 2B. The "Sable" electronic lock (version 2.0) is currently supported and meets these requirements.

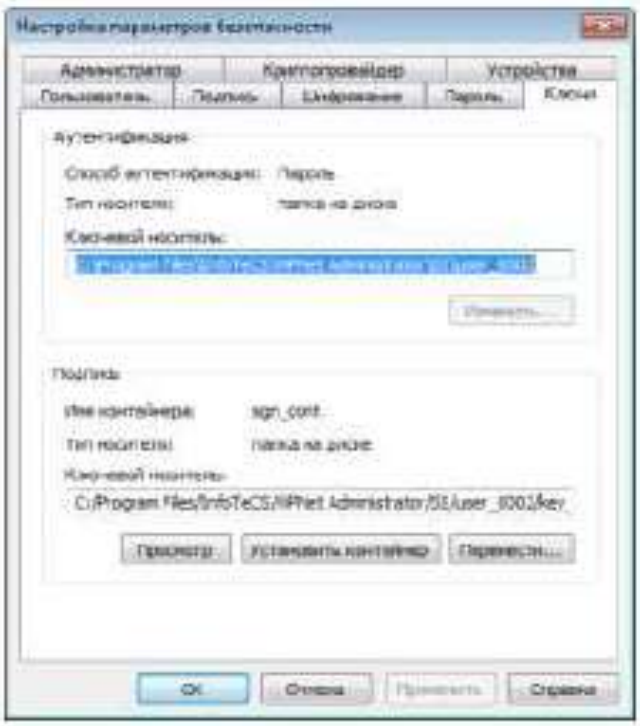


Figure 2.6 - Working with the key container in ViPNet CSP

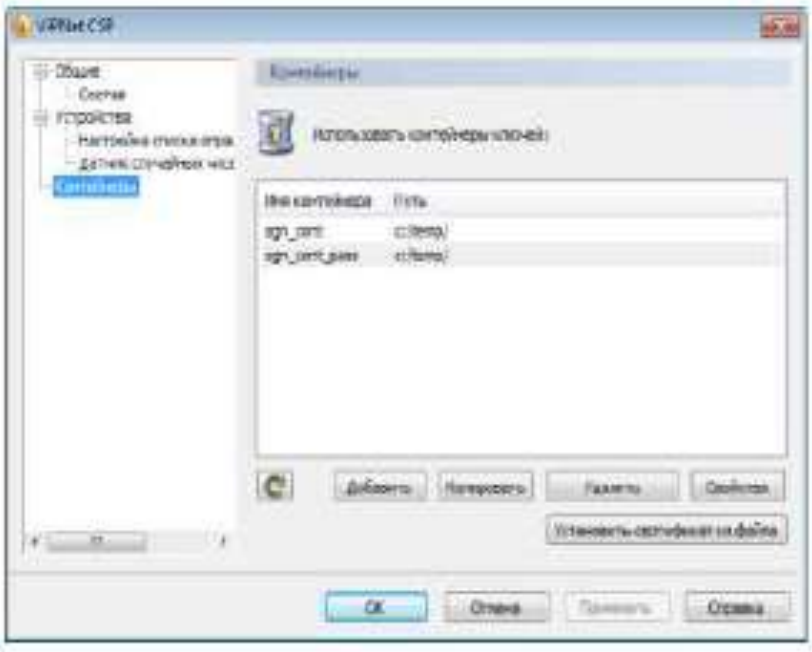


Figure 2.7 - Certificate enrollment procedure in ViPNet CSP

2.4.3 Installation of intrusion detection and antivirus

Security Studio Endpoint Protection 6.0 offers comprehensive computer protection by incorporating a firewall, antivirus, and intrusion detection capabilities. It is designed to facilitate secure and seamless Internet usage while effectively preventing any malicious software from infiltrating the computer and blocking unwanted network traffic.

The key features and benefits of Security Studio Endpoint Protection 6.0 include:

Safe network access: The software ensures secure access to network resources, allowing users to connect to networks without compromising their computer's security.

Protection against known viruses and spyware: It employs advanced antivirus technology to detect and eliminate known viruses and spyware, safeguarding the computer from common threats.

Protection from unknown threats: Security Studio Endpoint Protection utilizes sophisticated threat detection mechanisms to identify and defend against emerging or unknown threats, ensuring proactive protection.

Secure use of network resources and spam protection: The software enables safe utilization of network resources, ensuring that users can access shared files, printers, and other network assets without compromising security. Additionally, it provides protection against spam, reducing the risk of email-based threats.

Centralized management: Security Studio Endpoint Protection offers centralized management capabilities, allowing administrators to efficiently monitor and control the security of multiple computers within a network environment.

By utilizing the certified version of Security Studio Endpoint Protection, organizations can meet the data protection requirements outlined by FSTEC. Furthermore, when combined with NSD Secret Net's Information Security System (SZI), it provides a comprehensive solution for protecting automated workstations, ensuring enhanced security across the network infrastructure.

Figure 2.8 - Components of Security Studio Endpoint Protection

Components of Security Studio Endpoint Protection:

• Internet screen: This feature enables two-way traffic control, preventing unauthorized access requests from the local Internet network to the computer.

• Antivirus and antispyware: The software includes a fast and efficient scanner that combines antivirus and antispyware capabilities to detect and neutralize malicious software.

• Intruder detection tool: The "Attack Detector" module proactively prevents over 25 typical attacks, while the "Local Security" feature controls program interactions, protecting the system against unrecognized threats.

• Web control: SSEP monitors and controls the operation of interactive elements embedded in web pages, preventing potential harm to the computer and the leakage of confidential information.

• Centralized management: The SSEP "Administration Center" provides centralized installation and updates, remote configuration of protection mechanisms, and monitoring of security events.

Advantages and benefits of Security Studio Endpoint Protection:

• The intruder detection tool is a highly advanced solution for countering information leaks and ensuring data security.

• Support for working in parallel with other antivirus software from different manufacturers.

• Compatibility with Secret Net, allowing for the implementation of a comprehensive security solution.

• Recommended for installation in the entire infrastructure of OILGROUP for all workstations.

Based on the design solution developed to protect information from unauthorized access in the corporate network of OILGROUP, the following security systems are recommended for installation:

• Cryptographic means of protection against NDS: SKZY "ViPNet CSP".

• Firewall: UserGate Proxy & Firewall 5.2 F.

• Intruder detection tool and antivirus: Security Studio Endpoint Protection (SSEP).

Variant of the location of information protection means in the corporate network LLC "OILGROUP" is depicted in Figure 2.9.

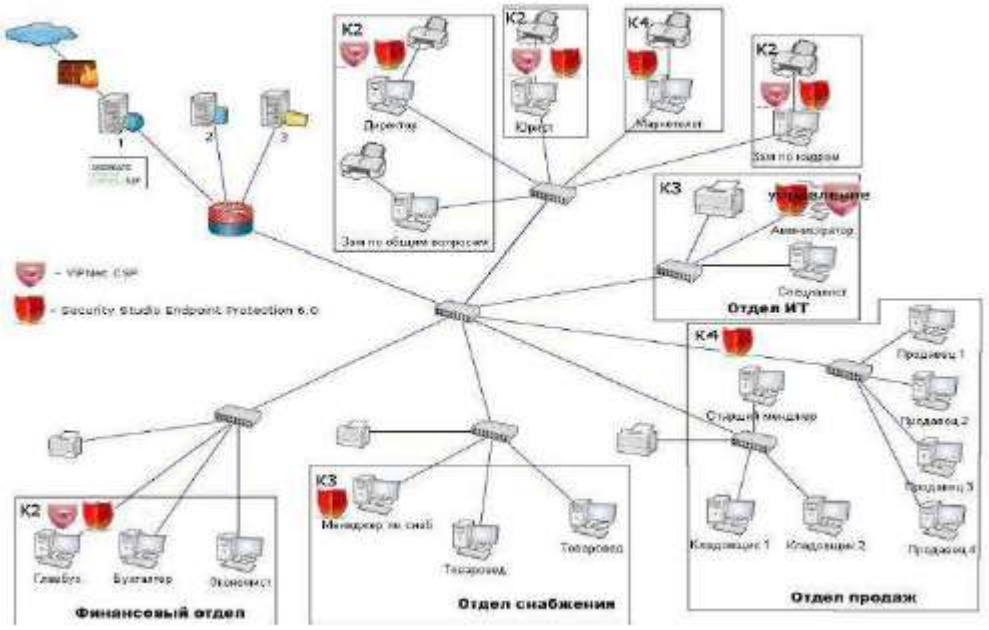


Figure 2.9 - Variant of placement of SZY in the corporate network of the LLC "OILGROUP"

Conclusions on section two: During the analysis of the enterprise's network and software, a comprehensive assessment of information security vulnerabilities was conducted, identifying the potential risks and threats faced by OILGROUP's LAN. Based on this assessment, several measures have been proposed to mitigate these threats and enhance information security within the LAN of OILGROUP. These

measures aim to protect the integrity, confidentiality, and availability of information resources, ensuring a secure and reliable network environment for the organization. By implementing these measures, OILGROUP can effectively prevent and address potential threats to information security in its LAN.

3 OCCUPATIONAL SAFETY AND HEALTH

Occupational safety and health issues are considered for the design and development phase of climate data analysis and visualization system.

Occupational safety is a system of legal, socio-economic, organizational and technical, sanitary and hygienic and treatment and prevention measures and tools aimed at preserving human life, health and ability to work. Working conditions at the workplace, safety of technological processes, machines, mechanisms, equipment and other means of production, condition of collective and individual protection means used by the employee, as well as sanitary and living conditions must meet the requirements of the law. An employee has the right to refuse the assigned work if a work situation has arisen that is dangerous to his life or health or to the people around him, or to the work environment or the environment. He must immediately notify his immediate supervisor or employer. The existence of such a situation is confirmed, if necessary, by labor protection specialists of the enterprise with the participation of a representative of the trade union of which he is a member or a person authorized by employees on labor protection (if the trade union was not established), as well as an insurance expert [12]. The task of labor protection is to minimize injuries and illnesses of the employee while ensuring comfort with maximum productivity. The main objectives of labor protection are the formation of specialists with the necessary knowledge and practical skills on legal and organizational issues of labor protection, industrial sanitation, safety, fire safety.

3.1. General characteristics of the room and workplace

The development of the analysis and visualization system is performed in a room located on the fourth floor of an eight-storey building with general and local lighting. The room has one-sided lighting, the windows are oriented to the east, the windows have shutters. White ceiling with a reflection coefficient of 0.7, light brick walls with a reflection coefficient of 0.5. There are 4 people working in the room, in accordance

with this we obtain input data for the analysis of potentially dangerous and harmful production factors, which are given in table. 4.1.

Table 3.1

Incoming data

Room parameters	**Value**
Length x width x height	6.6 x 6.1 x 2.7 m
Area	40.26m²
Volume	108,70 m³
Workplace number	**Specifics of work**
I workplace	Front-end programmer (web application client development specialist)
II workplace	Back-end programmer (specialist in the development of the server part of web applications and database design)
III workplace	Business analyst (also acts as a product manager)
IV workplace	UI-UX web designer
Technical means (quantity)	**Name and characteristics**
Monitor (4 pcs.)	HP 22Xi / 21.5 "/ 1920x1080px / IPS
Computer (4 pcs.)	HP ProBook 440 G6, 14 "IPS screen (1920x1080) Full HD, Intel Core i7-8565U (1.8 - 4.6 GHz) / RAM 16 GB / SSD 256 GB
Floor cooler (1 piece)	CRYSTAL YLR3-5V208
Air conditioner (1 piece)	DEKKER DSH105R / G / 26m2 / 2,65kW- 2.9 kW / 25x74.5x19.5 cm / 9 kg
General purpose luminaries (3 pcs.)	The lamp raster built-in 4x18W
Local lamps (4 pcs.)	Delux Decor TF-05/1 x 40W

According to NPAOP 0.00-7.15-18, the area S 'allocated for one workplace with a personal computer must be at least 6 m2 and the volume - at least 20 m3. There are 4 workplaces in the room, which fully meets the required standards.

We calculate the actual values of these indicators by dividing the volume of the room and the total area by the number of employees.

Therefore, based on the results obtained in terms of area and volume, the room meets the standards.

Table 3.2

Workplace characteristics

№	The name of the parameter	Value	
		in fact	Normative
1.	Height of a working surface, mm	780	680 – 800
2.	Width of a working surface, mm	1500	not less than 600
3.	Depth of a working surface, mm	750	not less than 600
4.	Height of space for legs, mm	750	not less than 600
5.	Width of space for legs, mm	800	not less than 500
6.	Depth of space for legs, mm	750	not less than 450
7.	Seat surface height, mm	480	400 – 500
8.	Seat width, mm	500	not less than 400
9.	Seat depth, mm	500	not less than 400
10.	Height of a basic surface of a back, mm	550	not less than 300
11.	Width of a surface of a back, mm	470	Not less than 380
12.	Length of armrests, mm	300	not less than 250
13.	Width of armrests, mm	60	50 – 70
14.	Distance from eyes to the screen, mm	650	600 – 700

It is possible to draw a conclusion that the sizes of a workplace of the programmer correspond to the established norms, proceeding from the set parameters.

3.2 Analysis of potentially dangerous and harmful production factors in the workplace

When creating a system of analysis and visualization, the work is performed sitting without physical effort, so it belongs to the category of light Ia.

Premises for work must be equipped with heating, air conditioning or supply and exhaust ventilation in accordance with DBN B.2.5-67: 2013. Normalized parameters of the microclimate, ionic composition of air, content of harmful substances meet the requirements of LTO 3.3.6.042-99, GN 2152-80, GOST 12.1.005-88, DSTU GOST 12.0.230: 2008 and DSTU GOST 12.4.041: 2006. Ventilation is understood as a set of measures and means designed to ensure meteorological conditions and cleanliness of the air environment that meet hygienic and technical requirements at permanent places and service areas. The main task of ventilation is to remove polluted, humid or heated air from the room and supply clean fresh air.

The sources of noise in the room are the fan of the system unit, laptop and air conditioner. The sound generated by the fan and air conditioner can be classified as constant.

According to DBN B.2.5-28: 2018 the work belongs to the category of visual works. The use of natural, artificial and mixed lighting is envisaged.

The computer is a single-phase consumer of electricity powered by 220V AC from a network with grounded neutral. IBM PC refers to electrical installations up to 1000V closed version; all conductive parts are in the casings. According to the method of protecting a person from electric shock, computers and peripherals must meet 1 class of protection.

Technical methods of protection against electric shock is reduced to the use of current of safe voltage, protection in case of accidental touching current-carrying parts and against excessive currents, protection in case of voltage transfer to non-current-carrying metal parts of the installation.

Safe voltage is obtained from the high voltage grid (110-120 V) by means of step-down transformers.

Protection against contact with live parts of the installation is achieved by means of insulation, fencing off the use of blocking safety devices and inaccessibility of the location of the installations.

Switchboards are placed in closed metal casings-boxes.

Safety alarm is used in the form of posters and inscriptions. The best light alarms are double, which in the presence of voltage lights a red light, and in its absence - green.

Protection against excessive currents - short circuits and overload currents, which can cause insulation to ignite, is provided by fuses and circuit breakers, and protection against voltage transfer to live parts by means of protective earthing and protective disconnection.

Fire prevention is achieved by eliminating the formation of sources of ignition and combustible environment.

Fires of the following classes are possible in this room: A - combustion of solids, E - combustion of live electrical installations.

CONCLUSIONS

During the design process, the following tasks were successfully accomplished:

An in-depth analysis of the object of protection was conducted, considering its specific requirements and characteristics.

Clear requirements for the protected system were defined, taking into account the levels of privacy and authorized user access.

Existing means of protection against unauthorized access were carefully evaluated and considered.

Based on the analysis and requirements, appropriate information security tools from NSD were selected and recommended for installation in the infrastructure of NGMA LLC.

The analysis revealed that the object of protection, which consists of multiple workstations, handles information with varying levels of privacy. Access to certain information is restricted only to authorized users, while others have limited access rights.

Certain threats related to unauthorized access were identified as irrelevant in the context of the implemented protection measures:

Theft of PCs is considered irrelevant due to the 24-hour access control to the controlled area.

Failure of PC nodes and communication channels is also deemed irrelevant as access control and locked doors are implemented.

Interception of PEMIN and acoustic information is considered irrelevant because the primary data is stored securely on a separate database server within the controlled zone.

To address the remaining threats of unauthorized access, the following measures were implemented:

The network perimeter was protected by selecting and implementing the UserGate Proxy & Firewall 5.2 F, which serves as an effective alternative to costly

software and hardware solutions. It complies with the 4th class of protection RD according to ME.

Cryptographic protection against unauthorized access was ensured by employing the CIPF "ViPNet CSP" solution, suitable for safeguarding information in AC up to 1V and ISPD up to class 1.

The Security Studio Endpoint Protection (SSEP), which includes an intrusion detection tool and antivirus capabilities, was adopted to protect the network against intrusions, malware, and spam.

The proposed set of protective measures aligns with all the requirements for securing corporate information networks. It has undergone examination by company specialists and has been successfully implemented by the network administrator, as confirmed by the provided implementation report.

As a result, the tasks initially defined in this design process have been fully accomplished. The set goals have been successfully achieved and implemented, ensuring the security of the network infrastructure.

REFERENCES

1. Asghar M., Mohammadzadeh N., «Design and simulation of energy efficiency in node based on MQTT protocol in Internet of Things» // International Conference on Green Computing and Internet of Things. – 2015. – С. 1413-1417.

2. Bass A., Bauer M., Fiedler M., Kramp T., van Kranenburg R., Lange S., Meissner S. Enabling Things to Talk. Springer-Verlag GmbH, 2013. – P. 325.

3. Gubbi J., Marusicet S., Buyya R., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. – 2013. – №. 7. – С. 1645–1660. [сайт]. - URL: 10.1016/j.future.2013.01.010.

4. Heather Flanagan, “Digital Preservation Considerations for the RFC Series,” January 2015, Internet Draft, work in progress, draft-flanagan-rfc-preservation-03.

5. Internet of Things Global Standards Initiative: [WEB]. – URL: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

6. Internet of Things Global Standards Initiative: [WEB]. – URL: http://www.itu.int/en/ITU-T/gsi/iot/ Pages/default.aspx.

7. Kang D., Park M. Lin S.W., Martin R.A., Miller B.W., Durand J. et al. Industrial internet reference architecture technical report. IIC, 2015.

8. Lobaccaro G, Carlucci S, Lofstrom E. A review of systems and technologies for smart homes and smart grids. Energies, 2016. – 348 с.

9. Shih C., Chou J., Designing CPS/IoT applications for smart buildings and cities / C. Shih, J. Chou // IET Cyber-Physical Systems: Theory & Applications. – 2016. – № 1. – С. 3-12.

10. Wortmann F., Flüchter K. Internet of things. Business & Inform. Syst. Eng, 2015. – № 3. – С. 221–224 .

11. Xia F., Yang L.T., Wang L., Vinel A. Internet of things. Int. J. of Commun. Syst. – 2012. – Vol. 25. – № 9. – С. 1101–1109.

12. Yih-Fang Huang; Werner, S.; Jing Huang; Kashyap, N.; Gupta, V., "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the

Requirements of the Future Grid," Signal Processing Magazine, IEEE , vol.29, no.5, pp.33,43, Sept. 2012.

13. Tomoiagă, B.; Chindriş, M.; Sumper, A.; Sudria-Andreu, A.; Villafafila-Robles, R. Pareto

Optimal Reconfiguration of Power Distribution Systems Using a Genetic Algorithm Based on NSGA-II. Energies 2013, 6, 1439-1455.

14. F.R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication Systems for Grid

Integration of Renewable Energy Resources," IEEE Network, vol. 25, no. 5, pp. 22-29, Sept.

2011.

15. “Values and Principles”. Principles. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/values-and-principles.