**MINISTRY OF EDUCATION AND SCIENCE
OF UKRAINENATIONAL AVIATION
UNIVERSITY FACULTY OF
AERONAVIGATIONS, ELECTRONICS
ANDTELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO
ENGINEERINGSYSTEMS**

ADMIT TO DEFENCE
Head of the Department

________ Victor HNATIUK

“_____”____________2023

QUALIFICATION WORK

(EXPLANATORY NOTE)

MASTER’S DEGREE GRADUATE

Topic: «Methods of improving cybersecurity of IP PBX »

Performer: ______________________ Kateryna ZHUKOVA
(signature)

Supervisor: ______________________ Viktor HNATIUK
(signature)

Consultants from individual sections of the explanatory note:

Consultant in the « Occupational Safety »section: _____ Batyr KHALMURADOV
(signature)

Consultant of the « Environmental Protection »section:
______________________ Andrian IAVNIUK
(signature)

Normocontroller: ______________________ Denys BAKHTIIAROV
(signature)

Kyiv 2023

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications
Department of telecommunication and radio engineering systems
Speciality: 172 "Telecommunications and radio engineering"

ADMIT TO DEFENCE
Head of the Department

________Victor HNATIUK

"_____"_____________2023

TASK

for execution of qualification work

Kateryna Zhukova

(full name)

1. Topic of diploma work: «Methods of improving cybersecurity of IP PBX» approved by the order of the rector from «28» September 2023 №1965/ст.

2. The term of the work: from 02 October 2023 to 31 December 2023.

3.Initial work data: Security protocols of an IP Telephony; Operational and vulnerability scheme to determine the security level of the system.

4. Explanatory note content: INTRODUCTION; CHAPTER 1 ANALYSIS OF CURRENT THREATS AND VULNERABILITIES IN IP PBX SYSTEMS; CHAPTER 2 DEVELOPMENT AND ENHANCEMENT OF CYBERSECURITY METHODS FOR IP PBX SYSTEMS; CHAPTER 3 TESTING, EFFECTIVENESS EVALUATION, AND CONCLUSIONS; APPENDICES

5. List of required illustrative material: figures, tables.

6. Work schedule

№ n/p	Task	Implementation term	Performance note
1	Develop a detailed content of sections of qualification work	02.10.2023 - 04.10.2023	Done
2	INRODUCTION	05.10.2023-08.10.2023	Done
3	ANALYSIS OF CURRENT THREATS AND VULNERABILITIES IN IP PBX SYSTEMS	09.10.2023-22.10.2023	Done
4	DEVELOPMENT AND ENHANCEMENT OF CYBERSECURITY METHODS FOR IP PBX SYSTEMS	23.05.2023 - 05.11.2023	Done
5	TESTING, EFFECTIVENESS EVALUATION, AND CONCLUSIONS	06.11.2023 - 30.11.2023	Done
6	APPENDICES	01.12.2023 - 06.12.2023	Done

7. Consultants from separate sections

Section	Consultant (position, Full Name)	Date, signature	
		Issued the task	Task accepted
Occupational Safety	Ph.D. in Med., Professor Batyr KHALMURADOV		
Environmental Protection	Ph.D. in Biol., Associate Professor Andrian IAVNIUK		

8. Date of issue of the assignment: September 29, 2023.

Supervisor ______________________________ Victor HNATIUK

(signature) (full name)

Accepted task for execution ______________________________ Kateryna ZHUKOVA

(signature) (full name)

ABSTRACT

Diploma work «Methods of improving cybersecurity of IP PBX» contains 88 pages, 15 images, 5 tables, 31 sources.

The object of study: IP PBX system.

The purpose of the diploma work: Creation of a protection system for IP PBX systems.

Research methods: Analysis of the literature sources. Developing the secyrity system suitable for using in IP PBX environment.

Materials of diploma work are recommended to be used in reliable protection systems from the feasible threats and create a strong defense against attacks by attackers. This guarantees the stable operation of the network and the protection of users' personal data from leaks, as well as the breakage of the system.

Keywords: VoIP, IP, SIP, H23, PBX, CYBER SECURITY.

CONTENTS

LIST OF ABBREVIATIONS

IP – Internet Protocol

PBX - Private Branch Exchange

VOIP – Voice Over IP

TCP -Transmission Control Protocol

SIP- Session Initiation Protocol

UDP – User Datagram Protocol

HTTP -Hyper Text Transfer Protocol

INTRODUCTION

As we sail into the digital age, Voice-over-IP (VoIP) has emerged as a novel mode of communication that is steadily replacing conventional phone lines. A sizable number of corporations are shifting to VoIP and distancing themselves from old-school modes of interaction. Apart from being cost-effective, VoIP offers remarkable flexibility allowing employees to carry out their duties from diverse locations on various devices–a testament to its potential for shaping future business dialogues [1].

Yet with technology's smooth promises come some rough edges; cybersecurity risks remain an ongoing concern for internet-reliant systems like VoIP which can become gateways for cyber pirates eager to plunder your network assets or deploy nasty software assaults if not adequately protected.

The realm of virtual attacks grows murkier each day teeming with sly varieties aimed at distinct nefarious objectives - demanding zhuzhed-up counter strategies specially crafted against unique attack types in this ever-evolving matrix. Hence comes the need for stringent security policies whose implementation would be instrumental in mitigating such ominous threats efficiently. Intricate work goes into fortifying one’s router-based calls considering prevalent dangers including hackers spying on conversations, unauthorized access leading towards confidential data thefts and even assuming false persona through call spoofing resulting sometimes misconduct activities. In fact about 46% mischievous global liaisons owe it all up funnily enough to our very own cherished tech: The 'innocuous' VOIP.

But let us stay clear; although these perils exist none undermines VOIPs inherent capacity offering robust protection granted proper installation practices followed effective management principles incorporated alongside alliance formed sound service providers eventually turn adversities favor.

This underlines urgency implementing full proof safety measures ensure dynamic perimeter defense keeping close tab evolving tactics adopt proactive risk prevention mechanism source referenced.

For Small-to-Medium Enterprises, studies note significant benefits of VoIP protocols in terms of improving call handling (67%), message organisation (63%) and remote work options (57%). It remains essential nonetheless to be proactive regarding security issues concerning VoIP and maintaining adherence to trustworthy best practice guidelines as highlighted below [1].

A superb illustration can be appropriated from protection plans for PBX telephone systems where a multi-tiered security solution's strategic introduction is seen as the optimum defence tactic. This shrewd method entails incorporating multiple protective steps aimed at strengthening vulnerable zones within telecommunication system infrastructure. By embracing this layered-security paradigm, businesses reinforce their safeguarding measures via redundancies that enhance complete coverage. Importantly, adopting such an outlook allows resilience with continuous guard irrespective if one layer gets breached [2].

Boosting cybersecurity mechanisms around IP PBX systems becomes paramount given its pivotal role in company communications; it provides secrecy for sensitive data contributes towards seamless business operations whilst warding off financial shortfall or legal ramifications connected with non-compliance scenarios [3].

Crucially there are additional reasons like adherance regulation requirements defending creative rights alongwith resistance against social engineering attacks also add bulk to significance enhancing cybersecure precautions. For instance, VoIp fraud countermeasures reducing denial-of-service susceptibilities, and curbing eavesdropping-on-communications' risks. Consequently, in light of modern-working-patterns securing IP-PBX services take even bigger precedence. In broader aspect tightening cybersecurity provisions elicits shield opposing potential disruptive outcomes financially severe consequences marred public-reputation spring boarded by safety breaches.

Traditional phone-conversation-transmission-utilising exclusive cables alongside hardware-establishments facilitating auditory content traffic. Albeit functionally vaild numerous occasions, this model incorporates inherently restrictive nature on diversified scalability capabilities. Moreover, the desideratum luring extra structural-capital expenditures erect-edifices presents obstacles smoothly releasing novel applications. Simply put legacy phonesystems exhibit series of constraints often tieing down businesses to avoid major system overhauls.

VoIP disrupts the traditional communication paradigm, propelling it into a new era as voice traffic is routed via network channels and mediated through software applications like computer-based softphones.

This monumental shift from reliance on conventional hardware offers an unparalleled level of flexibility - one that contributes to VoIP's surging popularity.

Post COVID-19 pandemic necessity has shed light onto this adaptability; enterprise-grade VoIP systems deliver remarkable ease when adapting to remote work arrangements — maneuvers which significantly vex classical phone systems tethered by rigid infrastructural constraints.

But do not think that these feats are simply a post-pandemic phenomenon. They provide specialized expertise to companies with evolving needs, positioning them as consistently progressive in the ever-evolving landscape of communications technology tools [3].

The purpose of the diploma work is strengthening IP PBX cybersecurity. As it is crucial to protect communications, secure sensitive data, and maintain seamless business operations. It prevents unauthorized access, ensures regulatory compliance, and adapts to evolving threats, bolstering overall business infrastructure.

The object of study is strengthening the overall cybersecurity framework of IP PBX systems to fortify defences against a wide range of cyber threats.

The subject of study is IP PBX System; Possible threats in the VoIP systems.

The scientific novelty of the obtained results

These measures are specific to each network's utilization parameters. Both current strategies and future tactics have been identified for strengthening security protocols in these systems, with scientific advancements playing a key role.

Various methods of preserving data integrity throughout an IP-PBX system’s operation were compared revealing their diverse advantages leading to better results across changing situations without jeopardizing globally accepted practices or standards governing telecommunications worldwide.

Approbation of research results

Scientific and practical conference "Problems of operation and protection of information and communication systems", Kyiv,2023

CHAPTER 1
ANALYSIS OF CURRENT THREATS AND VULNERABILITIES IN IP PBX SYSTEMS

1.1 Analysis of Current Threats

1.1.1 Types of threats affecting IP PBX systems

VoIP enables the utilization of any IP network for the arrangement and execution of real-time telephone conversations, video transmission, and fax communications. Currently, IP telephony is emerging as the standard in telephone communications, offering convenience, reliability, and comparatively lower costs when contrasted with analog communication. This technology not only enhances efficiency but also facilitates the integration of various business applications, unlocking previously unavailable capabilities. Moreover, it proves instrumental in improving the operations of government institutions, contributing to a more streamlined and effective communication infrastructure.

Despite the cost-effectiveness and enhanced security features offered by VoIP-based telephony, it still exhibits certain vulnerabilities. In contrast to traditional telephone networks relying on physical isolation for protection, VoIP networks face potential eavesdropping risks if not adequately secured. However, implementing robust protection measures, such as standard encryption commonly used in data networks, specialized applications, or customized settings, can significantly minimize the risk of eavesdropping. Notably, achieving a comparable level of security in a conventional telephone network is nearly impossible and considerably more expensive.

In a typical telephone network configured on a point-to-point basis, each telephone set is intricately linked to a specific switch. Any malfunction in this device can result in a complete disruption of phone operations. In contrast, VoIP networks are designed with a flexible distributed "three-point-to-point" scheme. The VoIP software switch can be easily relocated without disrupting the overall system functionality, allowing for adaptability and resilience. The ability to reroute voice data streams at any time ensures that a well-designed VoIP network doesn't have singular points of failure that could entirely block service. This inherent flexibility safeguards against the disruption of individual telephone sets, making VoIP an attractive and versatile solution.

VoIP technology is notably susceptible to network bandwidth challenges compared to many other network infrastructure technologies. Integrating this technology into a conventional data network necessitates the introduction of a new security consideration known as Quality of Service (QoS).

The QoS parameter denotes a network's capability to assign traffic priorities, ensuring that VoIP voice packets maintain essential characteristics, such as clarity and continuity of conversation, regardless of bandwidth utilization in other technologies. This underscores the critical importance of prioritizing and managing network traffic to uphold the quality and reliability of VoIP communications.

For instance, many non-commercial users have observed that during the download of large files from the Internet, ongoing VoIP calls may experience a decline in quality until the download is completed.

Network availability emerges as a crucial security requirement within a data transmission network, directly influencing the functionality of VoIP technology. If the data transmission network experiences downtime due to factors like DoS attacks or a malfunctioning VoIP router, it can result in network outages, impacting overall infrastructure operations.

Enforcing Quality of Service (QoS) and ensuring network availability pose intricate challenges for IT staff, particularly when managing these conditions across the entire enterprise. Unintended internal threats, such as bandwidth overruns, resource exhaustion, or the failure/misconfiguration of network devices, add to the complexity. VoIP packets, essential for communication, traverse an inherently unreliable IP network. Network congestion or packet chain damage may lead to the deletion of some data.

Moreover, retransmitting lost packets at the transport layer is impractical for real-time traffic due to the introduction of additional delays.

In spite of its widespread use, the IP telephony system remains susceptible to a range of potential threats and attacks. These encompass worms and viruses, DoS attacks, unauthorized remote access, and other common security risks. Noteworthy threats include:

- Unauthorized registration of someone else's terminal, allowing illicit calls on another individual's account.
- User substitution, enabling malicious entities to redirect calls and manipulate communication pathways.
- Alteration of voice or signaling traffic, introducing the risk of unauthorized modifications.
- Deterioration in the quality of voice traffic, potentially compromising communication clarity.
- Redirection and interception of voice or signaling traffic, posing privacy and security concerns.
- Forgery of voice messages, creating the potential for misleading or malicious communication.
- Denial of service attacks, disrupting the normal functioning of the IP telephony system.
- Remote unauthorized access to the IP telephony infrastructure, opening avenues for unauthorized control and manipulation.

Yet, the challenges associated with the use of IP telephony extend beyond the mentioned issues. The VoIP Security Alliance has compiled a comprehensive document outlining a diverse array of threats related to IP telephony. These threats encompass not only technical concerns but also extend to issues such as user deception and unwarranted spam.

Addressing information security concerns is pivotal during the preparation phase of an IP telephony project. It is at this juncture that stakeholders need to collaborate and determine the most suitable network infrastructure protection mechanisms to deploy in the network. The proactive consideration of security measures during the project's initiation lays a crucial foundation for safeguarding against a multitude of potential threats in the realm of IP telephony.

Until now, a significant obstacle to the widespread adoption of VoIP has been the concern regarding the clarity and interference-free nature of conversations compared to traditional public telephony. Inadequate quality in IP telephony networks can lead to dropped calls, poor or choppy sound, and communication becoming unintelligible to the extent that participants may have no option but to terminate the conversation. Additionally, network attacks and congestion problems can impact the signaling aspect of VoIP, causing delays in the ready tone or the initial call setup after dialing.

Network delay refers to the time it takes for a packet to traverse from one participant to another. In conventional telephony, slight delays in speech are typically encountered during international calls due to the distance covered by the call. VoIP latency, however, can be influenced by various factors, including the physical distance of cable networks, numerous intermediate transitions through the Internet, network congestion, and inadequate or absent internal bandwidth prioritization.

The codec documentation specifies that a one-way delay exceeding 150 milliseconds becomes noticeable to conversing parties. This type of network delay is most likely attributed to the Internet provider used by the interlocutor. Many Internet services offer a service level agreement to ensure minimal latency within their own network.

In the data transmission network, packet loss predominantly occurs under heavy load and congestion. Unlike many traditional TCP/IP applications where lost packets are typically retransmitted, in VoIP applications, resending a lost packet is impractical as the conversation has already progressed beyond that point.

To bolster security against eavesdropping, IP-telephones with built-in encryption capabilities offer advanced protection. Additionally, encrypting traffic between phones and gateways provides supplementary security, although it represents a less robust logical solution to the eavesdropping challenge. However, it's essential to consider that such encryption functionality may extend signal duration, necessitating careful consideration when establishing a secure communication line.

In the transmission of voice signals and data within local virtual networks, a shared physical bandwidth is employed. The presence of a virus or worm in a node can lead to a traffic influx, potentially inundating the network. Nevertheless, employing appropriately configured Quality of Service (QoS) mechanisms ensures that IP telephony traffic retains priority over common physical channels, rendering a denial-of-service (DoS) attack ineffective.

Denial-of-service attacks pose a significant challenge in the realm of IP telephony and the broader data transmission environment. When considering attacks on the data transmission environment, the RTP protocol plays a pivotal role in IP telephony. To fortify network protection, various information security mechanisms embedded within network equipment, along with additional solutions, can be implemented.

As of now, the SIP protocol, which supplants the H.323 protocols, lacks robust security features. This deficiency raises concerns among potential users about the future viability of IP telephony, with many experts attributing these doubts to the current state of the SIP protocol.

Common threats encountered are those prevalent in most information systems, while network threats specifically pertain to risks associated with data transmission through communication channels. To address the challenge of ensuring secure interaction with VoIP over open communication channels, additional information security measures become imperative from the standpoint of safeguarding information.

Network attacks are malevolent actions orchestrated by attackers with the aim of gaining control, causing destabilization, and acquiring confidential data from the targeted system or network [7].

- Common types of potential attacks on VoIP include:
- Data interception
- Denial of service

- Number manipulation
- Service theft
- Unexpected challenges
- Unauthorized configuration changes
- Account fraud [7]

Data interception poses a significant challenge in the realm of IP telephony. Unlike traditional telephony, where physical access to the telephone line is required for interception, IP telephony opens avenues for attackers without such constraints. Most protocols built on the TCP/IP stack utilize open data transmission, and IP voice traffic between gateways is not inherently encrypted. This lack of default encryption makes it easier for an attacker intercepting the data to resume the original negotiation and potentially transmit the intercepted data or voice with alterations. Data interception can occur both from within the corporate network and externally.

A proficient attacker with access to the physical data transmission environment can connect their IP phone to the switch, enabling eavesdropping on others' conversations. Such an attacker can also manipulate network traffic routes, becoming the central node through which the traffic of interest flows within the corporate network. While unauthorized devices intercepting voice data may be detectable with a certain probability within the internal network, it is nearly impossible to detect such intrusions in the external network. Therefore, any unencrypted traffic outside the corporate network should be considered insecure.

The heavy load of the transmission network with digitized voice data can lead to significant distortion or loss of messages in VoIP. One form of attack involves sending a large volume of "noise" packets to the IP telephony server, characteristic of a "denial of service" attack. Without constant monitoring for signs of such attacks and the application of passive protection measures, servers may struggle to handle the high load, resulting in service disruptions for connected subscribers.

In the context of VoIP, the IP address plays the role of a traditional telephone number. This introduces the potential for criminals to exploit address replacement to impersonate a desired subscriber. Insufficient use or simplification of telephony authentication and authorization mechanisms increases the risk of unauthorized access by attackers replacing user data with their own. There is also the possibility of hacking user accounts through snooping or eavesdropping on unsecured communication channels, leading to unauthorized use of the victim's account for making expensive calls and compromising the benefits of using IP telephony. Data replacement can also be employed to receive calls with the aim of utilizing the information for malicious purposes.

Call centers implemented on personal computers and other software-based VoIP components are inherently less secure than dedicated IP phones. Consequently, attacks specific to IP telephony can extend to these components, considering the vulnerability of computers and their associated elements, such as operating systems, application programs, and databases, to various security threats.

1.1.2 Examples of real incidents and attacks

Attackers may target nodes storing information about user conversations, including caller details, timestamps, call durations, and reasons for call termination. This aims to acquire confidential information about conversations and potentially manipulate or delete data in billing systems. Such manipulation can lead to incorrect invoicing, causing damage to the entire infrastructure of IP telephony and disrupting its functionality. Given that IP telephony is not bound to a subscriber's location, it allows communication from virtually anywhere on the planet, provided there is an Internet connection.

Denial-of-service (DoS) attacks exhibit a range from single packet assaults capable of crashing applications and servers to a flood of packets from the same attacker. Single-package attacks exploit known flaws in operating systems or applications to exhaust server or network resources. While such attacks are identifiable and isolatable, distributed denial-of-service (DDoS) attacks, where an attacker employs multiple machines, are more challenging to counter. In DDoS attacks, a stream of packets from various sources is used to overwhelm the target.

Flooding represents a conspicuous denial-of-service attack wherein the attacker attempts to utilize all available network or system resources (bandwidth, TCP/UDP connections, etc.), rendering standard software unsuitable for secure use. The proliferation of botnets has significantly increased the frequency of DDoS attacks, leveraging computers infected with malware. The motivations behind DoS and DDoS attacks range from extortion to sheer amusement.

A botnet refers to a substantial number of compromised computers under the control of an attacker. Initially infected with bot worms, each computer connects back to the attacker. With each new infection, the attacker can exploit vulnerabilities in the network or send virus attachments to random email recipients, using the infected army of computers to find and infect other vulnerable hosts. Presently, botnets stand as the primary source of DDoS attacks on the Internet. Identifying and isolating DDoS attacks can be challenging due to the diverse and unpredictable source addresses of botnet hosts, originating from various locations worldwide.

Flooding the User Datagram Protocol (UDP) presents a formidable bandwidth attack due to its susceptibility to address spoofing, allowing attackers to manipulate addresses effortlessly. The prevalence of UDP support in almost all Session Initiation Protocol (SIP)-capable devices makes it an effective choice for attackers. When directed to listen on a SIP port (5060) or even random ports, a raw UDP packet stream can corrupt many VoIP devices and operating systems.

The landscape of freely downloadable tools facilitates the execution of UDP flooding attacks, offering attackers a readily available means to exploit vulnerabilities. With VoIP utilizing a diverse range of protocols, attackers have various avenues to orchestrate a Denial-of-Service (DoS) attack. A more sophisticated approach, flooding, strategically undermines the network's quality of service mechanisms to degrade VoIP applications.

Assuming an organization's Quality of Service (QoS) technologies prioritize Real-Time Transport Protocol (RTP) traffic over other types, a conventional flooding attack is often ineffective. However, if an attacker inundates a phone, proxy server, or VoIP

Private Branch Exchange (PBX) with RTP traffic, the QoS mechanism struggles to discern between genuine and fake calls, complicating the determination of network priority.

Threats in VoIP systems encompass violations of the authentication mechanism, allowing attackers to alter identity and data. Social engineering tactics may exploit user

trust to gain necessary data without bypassing authentication. Once inside the network, attackers can make unauthorized calls, alter or delete account data, and engage in malicious activities that may persist undetected in large organizations. Without encryption in VoIP, attackers can illicitly connect to the network, engaging in traffic analysis to eavesdrop on specific conversations or collect sensitive data like phone numbers and credit card details. Active actions in manipulating network traffic expose vulnerabilities arising from protocol implementation errors.

A TCP SYN attack involves an attacker flooding the victim with SYN packets, utilizing spoofed source IP addresses. The victim responds with SYN-ACK, unaware of the nonexistent spoofed sources, and waits for an ACK packet that never arrives. This fills the victim's connection table, depleting resources and hindering its ability to distinguish between spoofed SYNs and legitimate ones.

An Established Connection Floods attack extends the TCP SYN attack, fully establishing a connection before rapidly dropping it. This sophisticated attack may even make actual requests to subvert the target, overwhelming a VOIP PBX with simultaneous REGISTER / INVITE / BYE requests or inundating a SIP client with spoofed incoming calls.

Attackers often exploit the Internet Control Message Protocol (ICMP), which lacks source message authentication. A smurf attack, a variant of ICMP abuse, involves sending large volumes of ICMP traffic with replaced source IP addresses to broadcast addresses, causing network bandwidth throttling with invalid ICMP replies.

As the complexity and frequency of attacks on VoIP servers rise, automatic port scans, security probes, and diverse attack sources contribute to the challenge of detection and mitigation. Spoofed source addresses further complicate identifying the true sender, adding to the difficulty of thwarting these attacks with firewalls.

In a Man-in-the-Middle (MitM) attack, a malicious actor clandestinely intercepts and potentially modifies the communication between two parties, all while deceiving both parties into believing they are directly communicating with each other. The objectives of such an attack may involve pilfering sensitive information or injecting malicious data [9].

As an illustration, an attacker could establish a rogue wireless access point (WAP) designed to mimic a legitimate WAP, utilizing the same or a similar network name (SSID). Unsuspecting users, thinking they are connecting to a trustworthy network, unknowingly link up with this rogue WAP. Consequently, all their wireless data traffic is directed through the deceptive access point, allowing the attacker to eavesdrop, scrutinize, and potentially alter the transmitted data [9].

Two prevalent forms of Man-in-the-Middle (MitM) attacks include:

Session hijacking: In this scenario, an assailant intercepts and seizes control of a user's active session, aiming to attain unauthorized entry to a server or web application. A common technique involves the use of a packet sniffer to capture communication between the user and the server. By capturing or predicting the session token, attackers can circumvent authentication, posing as the victim to gain access to sensitive information or execute functions on the targeted system.

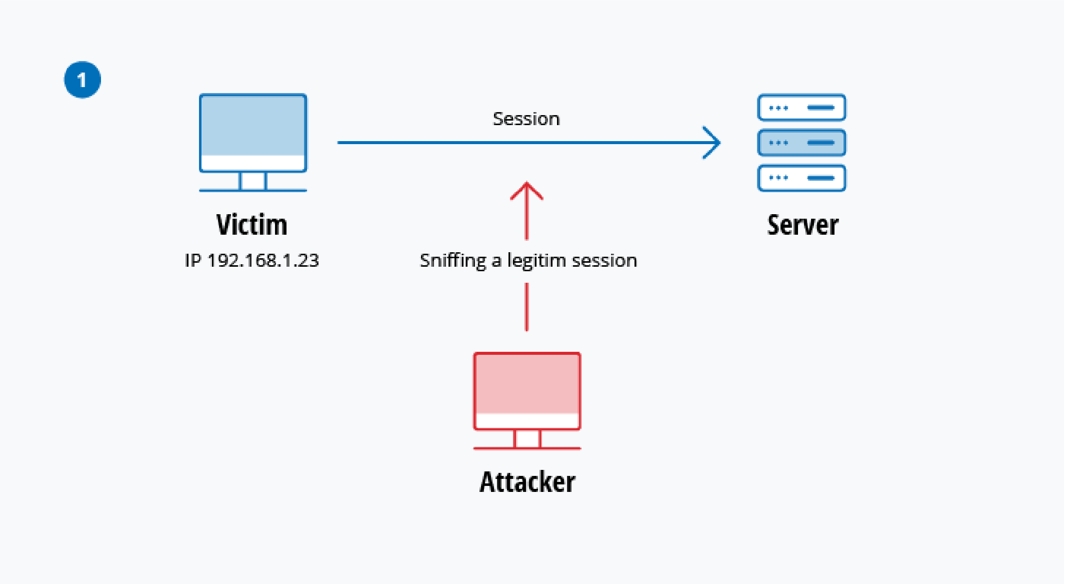


Fig. 1.1. Session hijacking diagram [9]

The diagram depicted below illustrates how the assailant could subsequently initiate a Denial of Service (DoS) attack to disrupt the victim's system and then establish a connection with the server following the session hijacking [9].

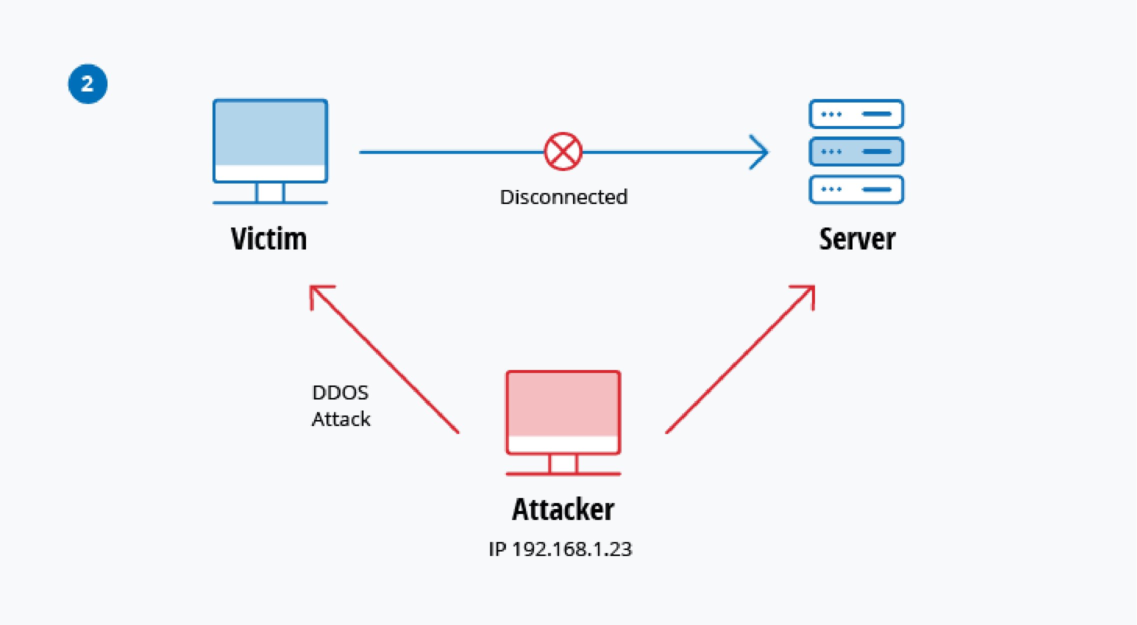


Fig. 1.2. IP spoofing attack [9]

IP spoofing involves an attacker concealing their actual source IP address to masquerade as a trusted entity. Through the manipulation of packet headers, attackers can trick systems into perceiving a malicious packet as originating from a legitimate source. This deceptive tactic allows them to gain unauthorized access or execute Denial of Service (DoS) attacks on networks and services [9].

Protective strategies against Man-in-the-Middle (MitM) Attacks:

While no singular technology or configuration can completely eliminate all MitM attacks, organizations and individuals can adopt various security measures to safeguard against these threats [9].

Recommended practices include:

- Opt for encrypted sites (HTTPS) over HTTP.
- Refrain from conducting sensitive tasks on public Wi-Fi. If necessary, employ a VPN.
- Verify that websites possess valid SSL/TLS certificates.
- Keep servers updated with the latest encryption techniques and protocols.
- Implement Multi-Factor Authentication (MFA) to thwart hackers who succeed in intercepting login credentials [9].

1.2 Vulnerabilities in IP PBX Systems

Private Branch Exchange (PBX) systems, pivotal in facilitating internal and external communication within organizations, face a spectrum of vulnerabilities that demand vigilant attention to maintain the integrity and security of communication networks. This abstract provides a concise overview of key vulnerabilities associated with PBX systems and proposes mitigation strategies to fortify these critical components of modern telecommunication infrastructure. Unauthorized access vulnerabilities, often stemming from weak passwords and susceptible to brute force attacks, underscore the importance of robust password policies and intrusion detection measures. Denial of Service (DoS) threats, in the form of flooding attacks, necessitate the implementation of firewalls, intrusion prevention systems, and rate limiting to mitigate potential service disruptions. Eavesdropping risks, particularly from man-in-the-middle attacks, emphasize the adoption of encryption protocols such as Secure Real-time Transport Protocol (SRTP) to safeguard sensitive communication. Call fraud vulnerabilities, exemplified by toll fraud, necessitate the implementation of strong authentication mechanisms and continuous monitoring of call patterns to detect and prevent unauthorized usage. Software exploits, inherent in any software-driven system, highlight the significance of regular software updates and patch management to address identified vulnerabilities. Social engineering threats, including phishing attacks, necessitate comprehensive user education programs to mitigate the risk of information disclosure and unauthorized access. Insecure network configurations, typified by inadequate firewall settings, demand strategic adjustments to enhance security, including stringent firewall configurations and network segmentation. The absence of effective monitoring and logging practices can be mitigated by implementing robust logging mechanisms and conducting regular reviews to promptly detect and respond to security incidents. This abstract serves as a valuable resource for organizations seeking to fortify their PBX systems against a dynamic threat landscape and to ensure the continued reliability and security of their communication infrastructure.

Table 1.1

Vulnerability categorization

Vulnerability Category	Description	Mitigation Strategies
Unauthorized Access	Weak or default passwords: Many users do not change the default passwords on their IP PBX systems, making them vulnerable to unauthorized access. It is essential to use strong, unique passwords for all system accounts.	Use strong, unique passwords and Implement account lockout policies

Continue of the table 1.1

Denial of Service (DoS)	Attackers may flood the IP PBX system with excessive traffic, causing it to become unresponsive.	Implementing firewalls, intrusion prevention systems, and rate limiting can help mitigate the impact of DoS attacks.
Eavesdropping	Attackers may intercept and listen to VoIP communication between users.	Encrypting the communication using protocols like Secure Real-time Transport Protocol (SRTP) can prevent eavesdropping.
Call Fraud	Attackers may exploit vulnerabilities to make unauthorized international or long-distance calls, resulting in financial losses for the organization.	Implementing strong authentication mechanisms and monitoring call patterns can help detect and prevent toll fraud.
Software Exploits	Like any software, IP PBX systems may have vulnerabilities that can be exploited by attackers.	Regularly updating and patching the system software can help address known vulnerabilities.
Phishing and Social Engineering	Attackers may use social engineering techniques to manipulate users into revealing sensitive information or providing access credentials.	Employee training and awareness programs are essential for mitigating this risk.

The end of the table 1.1

Insecure Network Configuration	Poorly configured firewalls may expose the IP PBX system to external threats.	Configuring firewalls to only allow necessary traffic and implementing network segmentation can enhance security.
Lack of Monitoring and Logging	Without proper monitoring and logging, organizations may miss signs of a security incident.	Implementing robust logging mechanisms and regularly reviewing logs can help detect and respond to security incidents promptly.

Authentication, authorization, and encryption represent foundational pillars in the realm of cybersecurity, playing a pivotal role in safeguarding sensitive information and securing digital communication. This abstract explores the critical importance of these three components in ensuring the integrity, confidentiality, and availability of data within information systems.

Authentication serves as the initial line of defense, confirming the identity of users, devices, or entities seeking access to a system. Robust authentication mechanisms, including multi-factor authentication, mitigate the risks associated with unauthorized access, identity theft, and potential compromise of sensitive data.

Authorization complements authentication by defining and regulating the level of access granted to authenticated entities. Effective authorization controls prevent unauthorized individuals or systems from accessing resources, reducing the likelihood of data breaches and maintaining the principle of least privilege.

Encryption emerges as a powerful tool to protect data during transmission and storage. By converting plaintext information into ciphertext using complex algorithms, encryption ensures that even if unauthorized access occurs, the intercepted data remains indecipherable without the appropriate decryption key. This safeguards against eavesdropping, man-in-the-middle attacks, and data breaches.

The symbiotic relationship among authentication, authorization, and encryption forms a robust defense strategy against a myriad of cyber threats. Together, they create a secure environment where only authenticated and authorized entities can access sensitive information, and the information itself remains confidential through the application of encryption protocols.

This underscores the critical role of authentication, authorization, and encryption in fortifying the cybersecurity posture of organizations, promoting data privacy, and fostering trust in digital interactions. As cybersecurity challenges continue to evolve, a comprehensive understanding and implementation of these core principles become imperative to ensure the resilience and security of modern information systems.

CHAPTER CONCLUSIONS

IP telephony represents a highly sophisticated and rapidly evolving realm of technological advancement, driven by society's demands for swift, high-quality, and reliable media communication transmission. The pervasive adoption of this technology across various spheres of human activity underscores its robust development and the diversity of systems created to meet diverse needs. These systems, having undergone continuous refinement and optimization, offer distinct advantages over traditional public telecommunications networks.

In contrast to conventional telephony, IP telephony, or VoIP (Voice over Internet Protocol), introduces several benefits, including a reduction in communication time and costs when interacting with other subscribers. Its cost-effectiveness stems from the ability to conduct communication sessions without the need for dedicated telephone lines and infrastructure. Leveraging existing network structures further contributes to economical communication, allowing users to pay solely for data connections. Additionally, this technology optimizes bandwidth usage, leading to reduced tariffs and making it an attractive option for users.

Despite these advantages, the security of IP telephony becomes a pivotal consideration as the popularity and demand for this technology escalate. Recognizing that IP telephony is susceptible to both generic IP network threats and specific VoIP attack methods, the implementation of robust security measures is imperative. The ease of executing these methods emphasizes the critical importance of safeguarding IP telephony against potential vulnerabilities.

Addressing security concerns in IP telephony necessitates a comprehensive approach, as each stage demands specific protection mechanisms. The foundation of protective measures lies in satisfying security requirements related to the preservation of confidentiality, integrity, and availability of information. In an era where information ranks among the most valuable resources, ensuring the security of IP telephony, particularly the confidentiality of personal data and conversations, emerges as an increasingly significant and intricate task. The ongoing development of holistic security solutions is paramount to mitigate risks and fortify the overall resilience of IP telephony infrastructure.

CHAPTER 2

DEVELOPMENT AND ENHANCEMENT OF CYBERSECURITY METHODS for IP PBX Systems

2.1 Authentication and Authorization

2.1.1 Implementation of multi-factor authentication methods

In the context of Internet telephony, the imperative of safeguarding both informational and financial security takes center stage. Effectively addressing the outlined threats demands a comprehensive strategy for ensuring information security. Encryption stands out as a pivotal measure to secure the information transmitted via Voice over Internet Protocol (VoIP).

While most IP networks, including the Internet and closed IP networks like intranets, accommodate VoIP traffic, the inherent insecurity, unpredictability, and lack of control over the Internet make it unsuitable for numerous public safety applications. Organizations contemplating the deployment of VoIP as a communication operations solution must carefully assess their options. Although IP networks efficiently transmit voice and video data, there exists the potential for quality loss or transmission delays. Consumers can mitigate these issues by implementing quality-of-service protocols that prioritize voice data, particularly in the face of unpredictable network loads. Notably, variations in encoding and signal transmission methods across VoIP providers underscore the necessity for compatibility considerations.

The security of IP telephony systems extends beyond safeguarding users from unauthorized access to encompass the protection of user information stored or circulated within VoIP systems or transmitted over communication lines. Emphasis must be placed on ensuring the confidentiality of clients' personal information while guarding against unauthorized access. The protection of clients indirectly translates to safeguarding the interests of system owners and employees, as conflicts regarding information disclosure with clients could yield undesirable consequences for the company [11].

Utilizing the open Internet Protocol, characterized by standardized rules enabling data routing around network failures with minimal delay and content loss, VoIP technology encapsulates digitized voice and data traffic over the Internet. Two pertinent categories within public safety are VoIP telephony and VoIP in public safety communication systems. IP technology converts voice communication into digital form, facilitating transmission over IP data networks, allowing voice and other data to coexist on the same infrastructure.

When deploying a global network in the security system, reliance on access control systems and authorizations is paramount. Key tasks involve identification, authentication, authorization, control of order integrity, and ensuring confidentiality. Identification relies on recognizing users through their subscriber information, while authentication confirms a subscriber's authority to use the provided identifier.

Authorization grants specific user rights, with integrity control measures preventing changes or withholding of orders [12].

Ensuring confidentiality prevents third-party access to transmitted data. The approach to access control and authorization varies based on the access channel, with diverse protection mechanisms employed, ranging from operations through the global network to more limited means, such as phone access [13]. The most rudimentary and least efficient approach to client authentication involves a fixed code or password known exclusively to the client. Access via numerous channels often entails transmitting information through open networks, making password protection vulnerable to interception and subsequent misuse. Various IP phones offer authentication tools that enable users to access the phone and its functions only after presenting and verifying a password or personal PIN number. However, this solution may not always be user-friendly, especially with constant IP phone use, posing a dilemma between security and convenience. Opting for weak passwords not only compromises the VoIP account but also exposes overall privacy vulnerabilities. Thus, passwords serve as a surface-level defense, screening out a certain percentage of unskilled attempts to manipulate the telephony system.

Introducing a table of numbered variable codes, known as session keys, enhances security. Each variable code functions as a one-time password, rendering interception meaningless. Upon exhausting all codes, a new table is issued to the client, typically every six months, minimizing inconvenience. However, the drawback of variable codes lies in the necessity for clients to carry the table, as memorizing numerous codes becomes impractical. If the table falls into the wrong hands, it grants access to accounts and customer data, posing a vulnerability. Additionally, the table of variable codes is susceptible to attacks involving the emulation of the telephony system by attackers, enabling the interception and misuse of the current variable code on behalf of the client.

Augmenting protection involves combining a client-remembered password with a code table. Implementing a policy of complex passwords renders brute-force attacks impractical, requiring significant time and computing resources to obtain credentials by this method [10].

2.1.2 Improvement of access authorization processes

When initiating access to your online accounts, a process commonly referred to as "authentication," you are essentially verifying your identity to the service provider. Historically, this verification has relied on a combination of a username and a password. However, this conventional method presents inherent vulnerabilities. Usernames, often easily discoverable, may even be as straightforward as your email address. Meanwhile, due to the challenge of memorization, individuals frequently opt for uncomplicated passwords or reuse the same password across multiple platforms [14].

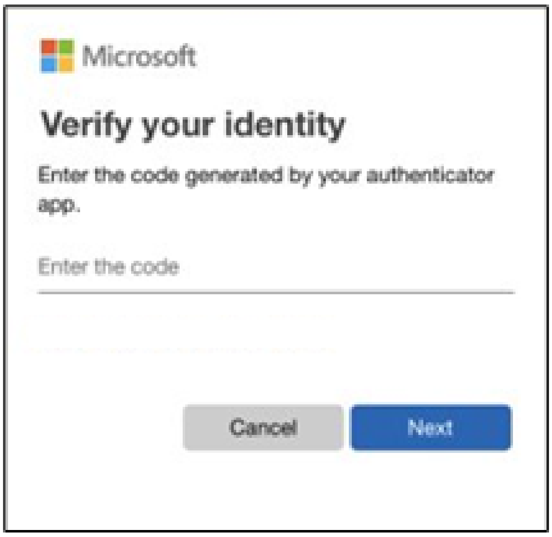
Recognizing these shortcomings, nearly all online services, including banks, social media platforms, shopping websites, and Microsoft 365, have incorporated measures to bolster the security of user accounts. This is commonly known as "Two-Step Verification" or "Multifactor Authentication," although the underlying principle remains consistent. In this enhanced approach, the initial login from a new device or application, such as a web browser, demands more than just a username and password. A supplementary element, often referred to as a second "factor," becomes a requisite to establish and confirm your identity [14].

Authentication involves utilizing a factor to validate your identity during the sign-in process. For instance, a password represents one type of factor, constituting something you know. The three predominant categories of factors encompass:

- Something you know - This includes items like a password or a memorized PIN.
- Something you have - This category encompasses possessions such as a smartphone or a secure USB key.
- Something you are - This pertains to inherent attributes like a fingerprint or facial recognition [14].

Consider the scenario where you are in the process of logging into your work or school account, and you input your username and password. In instances where solely this information is required, anyone possessing knowledge of your login credentials can potentially access your account from any location globally [14].

However, the implementation of multifactor authentication introduces an added layer of complexity. During your initial sign-in on a device or application, you provide your username and password in the usual manner. Following this, you are prompted to input a second factor to further authenticate and verify your identity [14].



Microsoft

Verify your identity

Enter the code generated by your authenticator app.

Fig. 2.1. Example of the process of MFA [14]

Perhaps you have chosen the Microsoft Authenticator app as your secondary authentication method. Upon accessing the app on your smartphone, it generates a unique, dynamically created 6-digit number. This numerical code is then entered into the respective site, facilitating your access [14].

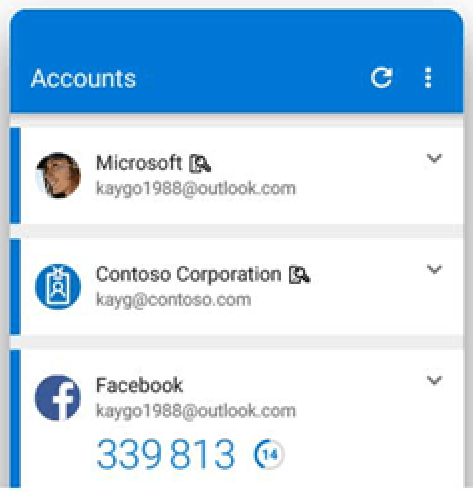


Fig. 2.2. Example of obtaining the security code [14]

In the event that another individual attempts to sign in as you, they would input your username and password. However, when prompted for the second factor, they encounter an impasse. Unless they possess your smartphone, obtaining the 6-digit number required for entry is impossible. Furthermore, the 6-digit number generated by Microsoft Authenticator changes every 30 seconds. Consequently, even if they were aware of the number you used to sign in yesterday, they would still be precluded from gaining access [14].

Role-Based Access Control (RBAC) involves the allocation of permissions to users based on their designated roles within an organization. This method provides a straightforward and easily manageable approach to access control, reducing the likelihood of errors compared to individually assigning permissions to users [15].

In the implementation of RBAC for Role Management, the process entails assessing user requirements and categorizing them into roles based on shared responsibilities.

Subsequently, each user is assigned one or more roles, and each role is associated with one or more permissions. This structured approach simplifies user assignments, eliminating the need for individual management, as users possess privileges aligned with the permissions assigned to their respective role(s) [15].

For instance, in the context of controlling access to an HR application using RBAC, HR managers could be granted a role permitting them to update employee details, while other employees would have access limited to viewing only their own information [15].

When devising an access control strategy, it is considered best practice to allocate users the minimal number of permissions essential for carrying out their tasks effectively [15].

Implementing regular audits and reviews of user access rights plays a crucial role in recognizing and correcting any disparities or outdated permissions. This proactive approach ensures that access privileges consistently align with the evolving requirements of the organization. By conducting these periodic assessments, discrepancies can be promptly addressed, promoting a more robust and secure access control environment. This practice not only enhances the overall integrity of the access management system but also serves as a preventive measure against potential security risks associated with obsolete or misconfigured permissions.

The education of users on the significance of secure access practices and the potential risks linked to unauthorized access stands as a critical imperative. Awareness programs serve as a valuable tool in empowering users to adhere to best practices, fostering a culture of heightened security consciousness. By imparting knowledge about the potential threats and consequences of unauthorized access, users become better equipped to recognize and respond to suspicious activities promptly. These awareness initiatives not only contribute to the overall resilience of the security framework but also establish a collaborative environment where users actively contribute to maintaining a secure digital landscape.

The practice of IP address whitelisting is a cybersecurity strategy that provides IT administrators with the ability to regulate access to business systems and resources [16].

IP whitelisting, also known as allowlisting, entails the creation of a catalog of trusted IP addresses, typically requiring dedicated static IP addresses.

These addresses are then linked to a specific user or a group of users as unique identifiers, and access permissions are exclusively granted to the designated IP addresses on the target server [16].

Consequently, any system within the local area network (LAN), datacenter, or third-party Software as a Service (SaaS) application can be configured to permit access solely to users possessing the organization's approved IP address. This encompasses connections originating from a private corporate network or through a Virtual Private Network (VPN) gateway. Unauthorized entities attempting to access the system from an unlisted IP address are effectively restricted [16].

IP whitelisting is commonly managed through various components:

- Firewall:

Configured to authorize network access exclusively for specific users, devices, or Local Area Networks (LANs).

- Edge Routers:

Typically established to block undesirable traffic on the router's TCP and UDP ports, safeguarding the internal LAN against potential threats from the public internet.

- Business VPN Gateway:

Various types of VPNs are utilized for secure connections. Learn more about these to understand how VPN gateways contribute to IP whitelisting.

- Web Server:

Primarily employed to regulate incoming requests, preventing extensive malicious queries such as brute force attacks.

- Application Layer:

Allows the evaluation and control of incoming queries within the application code, enabling the blocking or allowance of requests based on design.

- SaaS Application:

SaaS applications commonly provide options to establish IP whitelists, enhancing security measures.

As a result, any system within the LAN, datacenter, or third-party SaaS application can be configured to grant access exclusively to users with the organization's approved IP address. This includes connections originating from a private corporate network or through a Virtual Private Network (VPN) gateway, effectively restricting unauthorized entities attempting to access the system from unlisted IP addresses [16].

Ensuring secure remote access to the PBX system is imperative, and the implementation of encryption protocols plays a pivotal role in this regard. By encrypting the data transmitted over external networks, a robust layer of security is established, mitigating the risks associated with eavesdropping and unauthorized interception. This cryptographic safeguard not only protects sensitive information during transmission but also fortifies the overall integrity of the PBX system, instilling confidence in the confidentiality and privacy of communication over external channels.

An individual attempting multiple unsuccessful passwords during a login attempt may signify a malicious user employing a trial-and-error approach to discover an account password. Windows domain controllers maintain a log of such logon attempts, and these controllers can be configured to counter potential attacks by temporarily disabling the account. The Account Lockout Policy settings govern the threshold for triggering this response and the subsequent actions [15].

These Account Lockout Policy settings are adjustable in the Group Policy Management Console, specifically under Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy. The subsequent topics delve into the implementation of each policy setting, considerations for best practices, the location of the policy, default values for the server type or Group Policy Object (GPO), distinctions across operating system versions, security aspects (including potential vulnerabilities of each policy setting), recommended countermeasures, and the potential impact associated with implementing these countermeasures [15].

The deployment of real-time monitoring tools plays a crucial role in fortifying the security infrastructure. These tools facilitate the instantaneous identification of suspicious activities within the system. Instances of anomalies or unauthorized access attempts act as triggers for immediate alerts, providing a vigilant security apparatus. This swift notification system empowers organizations to respond promptly to potential security threats, initiating mitigation measures to curb any potential risks. By embracing real-time monitoring, organizations can proactively address security incidents, enhancing overall resilience and safeguarding against potential breaches or unauthorized intrusions.

Maintaining the PBX software in an up-to-date state is a critical practice aimed at addressing and rectifying security vulnerabilities. By regularly applying updates and patches, organizations can effectively fortify the overall security posture of their PBX systems. These proactive measures not only ensure the elimination of potential weaknesses but also contribute to the resilience and robustness of the PBX infrastructure against emerging security threats. The abstract underscores the significance of continuous software maintenance as a fundamental element in sustaining a secure and protected communication environment.

2.2 Data Encryption

2.2.1 Development and implementation of encryption schemes to protect communications and data

Encryption stands as a widespread and effective security measure, making it a prudent choice for safeguarding an organization's sensitive information. However, with a plethora of encryption methods at one's disposal, the challenge lies in making an informed selection.

In a landscape where cybercrimes are escalating, the array of available methods provides assurance that diverse options exist to fortify network security against various infiltration attempts. The true dilemma arises in determining the most suitable techniques for an internet security expert based on the unique circumstances of their organization.

Explore the video below for a comprehensive explanation of encryption, delving into the intricacies of how encryption and decryption function through a straightforward, step-by-step guide. The video also covers different types of encryption and more, offering valuable insights for making informed security decisions.

Data encryption serves as a protective measure, transforming data into an encoded format that can only be deciphered or accessed with the corresponding encryption key. Unauthorized access to encrypted data results in an appearance of scrambled or unreadable content.

The encryption process involves converting readable data into a scrambled form, a practice essential for securing confidential information during transit. Whether applied to documents, files, messages, or any form of communication across a network, encryption plays a pivotal role in preventing unauthorized interception [17].

Preserving the integrity of data is a paramount objective, and encryption emerges as a vital tool in achieving this goal. Virtually every facet of online activity, including websites and applications, involves some layer of encryption. According to cybersecurity experts at Kaspersky, encryption is foundational to data security, serving as the fundamental building block widely adopted by organizations of varying scales and individual users. In their definition, encryption is the conversion of data into an encoded format, readable or processable only after decryption.

Given the heightened risks of cybercrime, it is imperative for every internet user, whether individual or organizational, to be acquainted with and implement fundamental encryption techniques. In today's digital landscape, where data security is of paramount importance, the adoption of encryption practices is not just a recommendation but a fundamental necessity [17].

The information designated for encryption is commonly referred to as plaintext or cleartext. To transform plaintext, various encryption algorithms come into play, involving intricate mathematical calculations applied to raw data. These algorithms, each distinguished by its application and security level, contribute to the diverse landscape of encryption methods.

In addition to employing algorithms, the encryption process necessitates the use of an encryption key. By utilizing this key alongside a suitable encryption algorithm, the plaintext undergoes a transformation into encrypted data, often referred to as ciphertext. Rather than transmitting the original plaintext through potentially insecure communication channels, the ciphertext is dispatched [17].

Upon reaching the intended recipient, the ciphertext can be reverted to its original readable format, i.e., plaintext, through the use of a decryption key. The secrecy of this decryption key is paramount and should be safeguarded at all times. Furthermore, it may or may not mirror the key utilized for the initial encryption of the message. An example will be provided to illustrate this concept.

A plethora of encryption algorithms exists in the contemporary landscape, and among them, five stand out prominently [17].

- Advanced Encryption Standard (AES):

AES, the trusted standard algorithm employed by the U.S. government and various organizations, is known for its efficiency, especially in its 128-bit form. With the capability to use 192- and 256-bit keys for robust encryption needs, AES is deemed virtually impervious to attacks, barring brute force attempts. Internet security experts widely anticipate AES becoming the preeminent standard for data encryption in the private sector.

- Triple DES:

As the successor to the original Data Encryption Standard (DES), Triple DES is a symmetric encryption algorithm developed in response to DES vulnerabilities exploited by hackers. Although it was once the industry's most widely used symmetric algorithm, Triple DES is gradually being phased out. Applying the DES algorithm three times to each data block, it finds common use in encrypting UNIX passwords and ATM PINs.

- RSA:

RSA, a public-key encryption asymmetric algorithm, serves as the standard for securing information transmitted over the internet. Renowned for its robustness, RSA encryption generates complex data configurations that confound potential hackers, requiring significant time and effort to breach systems.

- Blowfish:

Designed as a replacement for DES, Blowfish is a symmetric algorithm that divides messages into 64-bit blocks, encrypting them individually. Notable for its speed, flexibility, and being unbreakable, Blowfish operates in the public domain, rendering it free and enhancing its appeal. Widely employed in e-commerce platforms for securing payments and in password management tools.

- Twofish:

Serving as Blowfish's successor, Twofish is a license-free symmetric encryption method capable of deciphering 128-bit data blocks. It consistently employs 16 rounds of encryption regardless of the key size, making it suitable for both software and hardware environments. Regarded as one of the fastest in its category, Twofish is a preferred choice in many contemporary file and folder encryption software solutions.

- Rivest-Shamir-Adleman (RSA):

RSA, an asymmetric encryption algorithm, operates based on the factorization of the product of two large prime numbers. Decoding the message successfully requires knowledge of these two numbers, making RSA commonly used for digital signatures. However, the algorithm experiences a slowdown when encrypting large volumes of data.

Table 2.1

Encryption algorithms

Criteria	Description
Strength and Reliability	Modern encryption standards, such as Advanced Encryption Standard (AES), are renowned for their proven strength and reliability. These algorithms undergo rigorous testing and scrutiny by the cryptographic community, making them widely accepted as secure choices.

Continue of the table 2.1

Key Length	The key length in encryption algorithms significantly influences security. Longer key lengths generally provide increased resistance against brute-force attacks. The optimal key length is determined during the development phase based on the specific security requirements of the application.
Cryptographic Resistance	Algorithms must resist various cryptographic attacks, including differential and linear cryptanalysis. During development, designers work to create structures that minimize vulnerabilities and withstand attempts to deduce sensitive information through analysis of ciphertext patterns.
Speed and Efficiency	Efficiency is crucial, especially in applications requiring real-time processing. Balancing strength with computational efficiency is considered during both development and implementation phases.
Quantum-Resistant Algorithms	With the advent of quantum computing, there's a focus on developing encryption algorithms resistant to quantum attacks. These algorithms aim to secure data against potential threats posed by quantum computers, which could compromise traditional cryptographic methods.
Adaptability to Evolving Threats	Designing algorithms with flexibility to adapt to emerging security challenges ensures their longevity in dynamic threat landscapes. The development phase involves anticipating potential future cryptographic threats.
Standardization and Interoperability	Standardization ensures wide acceptance and consistent implementation of encryption algorithms across different systems and applications. Interoperability is crucial for seamless communication and data exchange between diverse platforms.

The end of the table 2.1

Open Source and Peer Review	Open-source algorithms undergo extensive peer review, fostering transparency and collective scrutiny by the cryptographic community. Collaborative examination enhances confidence in the security and reliability of the algorithms.
Regulatory Compliance	Certain industries and regulatory frameworks may mandate specific encryption standards. Adhering to these standards is essential for ensuring compliance with legal and industry requirements.
Post-Quantum Cryptography	As quantum computing advances, researchers explore post-quantum cryptography to develop algorithms resilient to quantum attacks. This forward-looking approach anticipates the potential impact of quantum technology on encryption methods.

2.3 Detection and Prevention of Attacks

The address filtering system functions by blocking false or suspicious actions when attempting to access valid addresses, thereby preventing attacks that may go undetected. This protective measure can be applied across all closed IP networks. To enhance network security, one approach involves registering an IP address for subsequent authorization, reducing the frequency of false authentication attempts.

This system is particularly effective in safeguarding against various threats, such as DDOS (denial of service) attacks and brute force attacks, which aim to compromise the system by preventing the manipulation of IP addresses.

The initial component of the filtering system focuses on IP address filtering. In a private network like IP telephony, a predefined list of specific users with access rights is maintained. The first step involves verifying if an incoming address falls within the allowed filter range. Access is granted if the address is valid; otherwise, it is blocked [18].

The second aspect involves the program scanning log files to identify IP addresses exhibiting signs of malicious activity, such as numerous password failures or exploit searches. Addresses flagged for such behavior are temporarily blocked using the Iptables management interface. This security policy method can also establish conditions for usernames and passwords, addressing the issue of weak authentication and preventing intentional address changes or network interference.

The third part of the system enables the identification of CallerID replacement by analyzing the content of SIP packets. This analysis helps determine the real end user, offering protection against indirect hacking attempts targeting users who have successfully passed all verification stages.

Apart from their deployment locations, IDS solutions also vary in their methods of identifying potential intrusions:

Signature Detection: Signature-based IDS solutions employ fingerprints of known threats for identification. After recognizing malware or other malicious content, a signature is created and included in the list used by the IDS solution to scrutinize incoming content. This approach ensures a high threat detection rate with no false positives, as all alerts are triggered by the detection of known malicious content. However, a signature-based IDS is limited to detecting known threats and remains oblivious to zero-day vulnerabilities [19].

Anomaly Detection: Anomaly-based IDS solutions construct a model of the "normal" behavior of the protected system. Subsequent behavior is compared to this model, and any anomalies are flagged as potential threats, generating alerts. While this method can identify novel or zero-day threats, the challenge of building an accurate model of "normal" behavior requires these systems to balance false positives (incorrect alerts) with false negatives (missed detections) [19].

Hybrid Detection: A hybrid IDS incorporates both signature-based and anomaly-based detection. This allows it to identify more potential attacks with a lower error rate than using either system independently [19].

Call Pattern Analysis involves analyzing call patterns to detect irregularities, such as sudden increases in call volume or unusual call destinations, indicative of potential fraudulent activities. Continuous monitoring of call traffic, coupled with the establishment of thresholds for normal activity, enables the prompt detection and response to abnormal call patterns. This proactive approach enhances the system's ability to identify and mitigate potential security threats in real-time.

Picture the realm of securing IP PBX systems as a grand orchestral performance, where Secure Authentication Mechanisms take center stage, weaving a tapestry of defense against potential threats and unwarranted intrusions. These advanced security measures, led by the majestic concept of multi-factor authentication, act as vigilant guardians, ensuring that access to the sacred space of IP PBX remains an exclusive privilege for authorized users.

At the core of this protective stronghold is the use of robust passwords, much like a vigilant sentinel stationed at the gateway. By demanding intricate combinations of uppercase and lowercase letters, numbers, and special characters, this initial defense line becomes an impregnable barrier, thwarting the attempts of cyber adversaries.

Adding to the security narrative, the inclusion of CAPTCHAs during the authentication process dances gracefully, distinguishing between the natural movements of human users and the mechanical routines of automated scripts or bots. This not only foils the plans of automated brute force attacks but also introduces a touch of finesse to the authentication journey, ensuring that only human users gracefully gain access.

Raising the intensity of the security symphony, the introduction of Two-Factor Authentication (2FA) adds a dramatic twist. Users, embodying the protagonists in this cyber saga, must present a second act of authentication – a code sent to their mobile device or generated by an authenticator app. Even if the fortress walls of passwords are breached, the second act serves as an impenetrable moat, preventing unauthorized access attempts.

Harmonizing these secure authentication measures, organizations compose a masterpiece of defense, a unique and intricate melody resonating through the digital corridors. This avant-garde security approach not only aligns with industry best practices but also stands as a testament to the commitment of organizations to safeguard their digital realms. In an era where the protection of digital assets is a grand narrative, Secure

Authentication Mechanisms emerge as the maestros, conducting the symphony of security in the realm of IP PBX systems.

CHAPTER CONCLUSIONS

In essence, the security of VoIP services is a multifaceted challenge that necessitates a holistic strategy to effectively thwart potential threats at every level. In our increasingly tech-dependent world, information technologies, such as VoIP, play a pivotal role in solving various tasks, especially facilitating remote communication among users. Originally conceived for global communication among everyday users, the scope of VoIP has expanded dramatically, now handling hundreds of billions of minutes in user communications. Beyond personal use, VoIP software clients are now integral not only at the household level but also within corporate landscapes, positioning VoIP as a crucial business tool comparable to cellular communication and email.

Given the sensitive nature of the data transmitted through IP telephony, maintaining the highest standards of confidentiality, integrity, and availability is paramount. The security system detailed in this section has been meticulously designed to comprehensively address vulnerabilities. Each component of the system is tailored to counter specific threats, deliberately discarding less secure mechanisms in favor of alternatives that offer enhanced protection. Notably, standard VPNs have been replaced with the more secure IPsec protocol, and TLS/SRTP is preferred over SRTP/ZRTP, with customized settings for each element of the security system.

A novel method for safeguarding information in IP telephony networks, centered around the Asterisk PBX, has been introduced. This method has the potential to elevate the security posture of IP telephony networks, mitigating the risk of third-party interference and data theft. Applicable to Unix-like platforms for communication and compatible with Windows users employing the Putty software application, the proposed method is detailed through a diagram illustrating the system's functionality across the network.

Acknowledging the inherent vulnerability of IP telephony and video conferencing to potential attacks due to their openness, the text emphasizes the need for robust protection. While attacks on these networks are not yet widespread, the proactive development of security measures anticipates potential threats. The devised security measures aim to prevent attacks on the IP-telephony system, minimizing potential losses in the event of a successful intervention attempt. Overall, the comprehensive security approach outlined here serves as a proactive defense against emerging threats to the integrity and confidentiality of IP telephony networks.

CHAPTER 3
TESTING, EFFECTIVENESS EVALUATION, AND CONCLUSIONS

3.1 Testing of New Methods

In our contemporary era, a myriad of fascinating technologies are at humanity's disposal, with IP telephony standing out as a particularly noteworthy innovation. This technology not only simplifies the lives of ordinary citizens but also empowers businesses to address key aspects such as boosting sales, enhancing employee efficiency, elevating customer service quality, automating workflows, and providing essential information for management. Essentially, IP telephony represents a harmonious fusion of classical telephony and the Internet, encapsulating the crucial functions of both. However, the seamless integration of IP telephony into daily operations necessitates a vigilant focus on cybersecurity. Neglecting this aspect can lead to substantial financial losses and damage to the reputation of businesses. Therefore, there is a pressing need for ongoing research and development of novel, effective methods to enhance the cybersecurity of IP telephony, constituting a significant scientific imperative.

The operational principle of IP telephony is rooted in the automatic transformation of a subscriber's voice into data packets. These packets traverse the network to reach the intended recipient and are promptly reconverted into audible speech. This form of telephony falls within the broader category known as VoIP (Voice Over IP), facilitating not only the transmission of standard voice messages but also enabling the exchange of various video files and similar media. This innovative technology significantly reduces network load and concurrently lowers the cost of landline phone calls. To harness the capabilities of IP telephony, specialized devices are required, such as SIP phones and softphones. While only a handful of enterprises are involved in manufacturing equipment for IP telephony, notable success has been achieved by companies like Grandstream and Cisco SB. These brands continually enhance product quality, offering a diverse catalog of

IP telephones featuring various design elements such as wired tubes, wireless options, LCD displays, and Wi-Fi connectivity. Each distinct feature contributes to the overall convenience and functionality of these devices for IP telephony purposes.

In the contemporary landscape, numerous solutions abound for establishing IP telephony systems, with notable contenders like Asterisk, 3CX, Oktell, among others. However, standing out as the unequivocal leader in this domain is the open-source Asterisk, a free computer telephony solution developed by Digium. Asterisk's open-source nature distinguishes it as a robust and versatile choice, contributing to its widespread adoption and acclaim in the market.

The architecture of the Asterisk system, depicted in Figure 3.1, encompasses various integral elements, including the network, equipment, local operating system, and additional components [20].

This intricate system design underscores Asterisk's comprehensive approach to IP telephony, providing a framework that accommodates diverse needs and functionalities.

One of Asterisk's key strengths lies in its adaptability, allowing users to tailor the telephony solution to their specific requirements. The open-source code not only promotes transparency but also encourages a collaborative community-driven approach to development. This ensures that Asterisk remains at the forefront of innovation in the rapidly evolving landscape of IP telephony.

The significance of Asterisk's role in the market is further emphasized by its seamless integration of Voice over Internet Protocol (VoIP) capabilities, enhancing communication solutions for businesses and individuals alike. Its versatility extends beyond mere telephony, enabling advanced features and integrations that contribute to increased efficiency and functionality.

As businesses and organizations continue to navigate the dynamic terrain of communication technologies, Asterisk's position as the premier free computer telephony solution with open-source code solidifies its standing as a cornerstone in the realm of IP telephony. The ongoing commitment to innovation and collaborative development ensures that Asterisk remains a driving force, shaping the present and future of communication solutions.

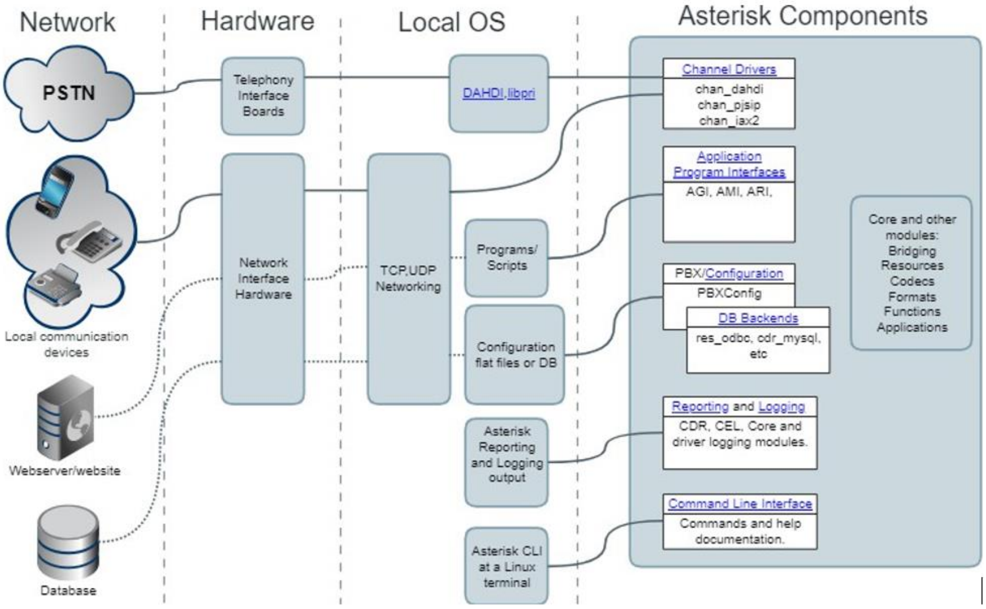

Network
Hardware
Local OS
Asterisk Components
PSTN
Telephony Interface Boards
DAHDI,libpri
Channel Drivers
chan_dahdi
chan_pjsip
chan_iax2
Application Program Interfaces
AGI, AMI, ARI,
Network Interface Hardware
TCP,UDP Networking
Programs/ Scripts
Core and other modules: Bridging Resources Codecs Formats Functions Applications
PBX/Configuration
PBXConfig
DB Backends
res_odbc, cdr_mysql, etc
Configuration flat files or DB
Local communication devices
Webserver/website
Asterisk Reporting and Logging output
Reporting and Logging
CDR, CEL, Core and driver logging modules.
Command Line Interface
Commands and help documentation.
Asterisk CLI at a Linux terminal
Database

Fig. 3.1. Asterisk system architecture

Asterisk, in conjunction with essential equipment, encompasses all the attributes of a traditional Private Branch Exchange (PBX). It boasts support for numerous VoIP protocols, including SIP, H.323, IAX2, MGCP, SIMPLE, SCCP, XMPP, and Unistim, while offering robust control functions for call management such as voicemail, conference communication, Interactive Voice Response (IVR), call center features, and Call Detail Record management. Additionally, Asterisk facilitates the transmission of text and video, demonstrating its versatility in supporting a wide array of equipment and computer protocols. This versatility enables the creation of diverse scenarios for network interaction, fostering open gathering and processing of information.

Asterisk is adaptable to both analog (FXO/FXS modules) and digital (ISDN, BRI, and PRI - T1/E1 streams) lines. By utilizing specific computer boards, Asterisk can be seamlessly integrated with high-bandwidth T1/E1 lines, enabling simultaneous operation with numerous telephone connections. The comprehensive list of equipment for general usage in connection with the phone network is dictated by hardware support in kernel modules. Figure 3.2 illustrates a typical diagram outlining the organization of Asterisk IP telephony.

When deploying Asterisk as an IP PBX, a critical consideration is the meticulous attention to software and cyber security. Neglecting this aspect can result in substantial financial and reputational losses, as cyber incidents, including hacking attempts, could compromise the system [21].

In instances of successful breaches, unauthorized access to Asterisk can lead to the exploitation of entire organizations, enabling attackers to make international calls at the victim's expense. Often, small organizations become targets due to insufficient attention to Asterisk security, and ongoing internet scanning perpetuates the search for vulnerable victims.

The primary objective of this work is to construct a data model aimed at enhancing the cyber security of IP PBX. To achieve this goal, we will delineate various vulnerabilities within IP PBX, outline the steps involved in executing cyber attacks on IP PBX, and propose a series of actions to bolster cyber security. This comprehensive approach aims to identify potential vulnerabilities, scrutinize the procedures for executing

cyber attacks, and implement preventative measures to enhance the overall level of cyber security for IP PBX systems.

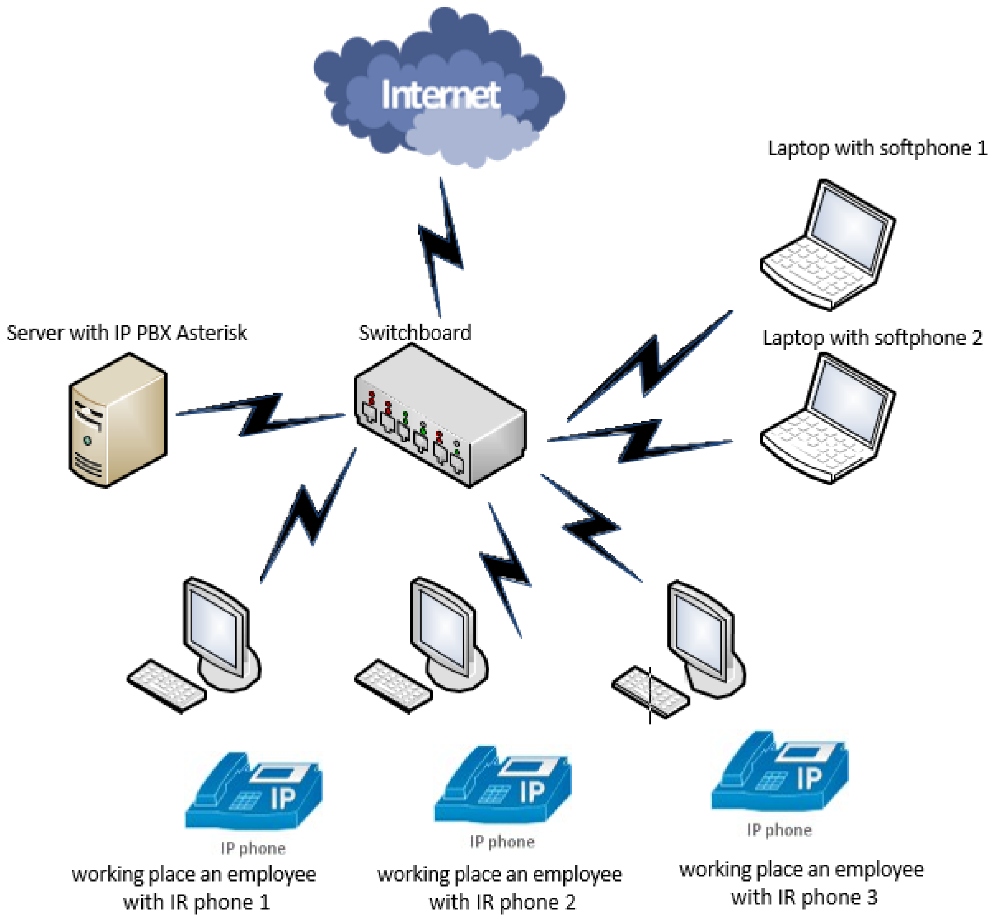

Internet
Laptop with softphone 1
Laptop with softphone 2
Server with IP PBX Asterisk
Switchboard
IP
IP phone
working place an employee with IR phone 1
IP
IP phone
working place an employee with IR phone 2
IP
IP phone
working place an employee with IR phone 3

Fig. 3.2. Scheme organizations IP telephony Asterisk

Let's establish a collection of vulnerability types, denoted as V, that manifest during the operation of the IP PBX (IR-ATS).

$$V = \{\bigcup_{i=1}^{n} V_i\} = \{V_1, V_2, \ldots, V_n\}, \quad (i = \overline{1,n}),$$

where n – number possible species vulnerabilities

Fig. 3.3. The collection of vulnerability types

For example, as a result of the analysis of the existing types of vulnerabilities during the operation of the IP-PBX [3-11], we will create a table for the Asterisk

IP-PBX. 1.

So, using expression (1) and data with table 1, with $n = 11$ we will get:

$$V_A = \{\bigcup_{i=1}^{n} V_i\} = \{V_1, V_2, V_3, V_4, V_5, V_6, V7\_, V8\_, V_9, V_{10}, V_{11}\} =$$

$$= \{V_{NCF}, V_{DP}, V_{SP}, V_{BSF}, V_{FSD}, V_{FSA}, V_{SA}, V_{LE}, V_{AV}, V_{ICA}, V_{LF}\} = \quad (2)$$

$$= \{NCF, DP, SP, BSF, FSD, FSA, SA, LE, AV, ICA, LF\},$$

where $V_1 = V_{NCF} = NCF$, $V_2 = V_{DP} = DP$, ..., $V_{11} = V_{LF} = LF$

Fig. 3.4. Vulnerabilities for IP PBX Asterisk

Table 3.1

Types of vulnerabilities in the IP PBX system Asterisk

No.	Code	Description
1	NCF	Asterisk, for specific reasons, utilizes a public IP address visible on the Internet. For instance, the Asterisk server also serves as an Internet distributor, directly connecting to the Internet with a "white" IP. Notably, no firewall is configured on the Asterisk server, making it vulnerable to external network threats.
2	DP	Default ports are assigned for both SSH and SIP, potentially exposing the system to security risks.
3	SP	Simple passwords are employed for SIP customers, presenting a security vulnerability.

Continue of the table 3.1

4	BSF	The protection mechanism against overrunning existing SIP customers is not activated, leaving the system susceptible to unauthorized access.
5	FSD	Security measures at the Dial Plan levels are not implemented, compromising the overall system protection.
6	FSA	The access restriction function to local networks is not in place, allowing potential unauthorized access from external sources.
7	S.A	Root user access is permitted via SSH, posing a security risk by granting high-level privileges.
8	LE	Unnecessary services with vulnerabilities are not disabled in the Linux operating system, exposing potential security holes.
9	AV	A PBX system, such as Elastix, is utilized with an interface that introduces additional vulnerabilities to the system.
10	ICA	The SIP provider allows international calls at the network level, even when unnecessary, potentially leading to security issues.

11	LF	The SIP provider lacks a function to restrict call volume, potentially leading to uncontrolled usage and billing at the end of the month.

Creating multiple steps for the execution of a cyber attack involves defining a set of sequential actions. To facilitate this stage, let’s designate these actions as a comprehensive set, denoted as S:

$$\{\bigcup_{j=1}^{m} \mathbf{S}_J\} = \{\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_m\},$$

where $\mathbf{S}_J \subseteq \mathbf{S}$, $(J = \overline{1,m})$, m – number steps the intruder

Fig. 3.5. Formation plural steps for implementation of a cyber-attack

Example, let’s consider sequence steps for implementation cyber attacks on IP PBX Asterisk (tab. 3. 2).

So, using the following expression and data with table 2, with n = 5 we will get:

$$\mathbf{S}_A = \{\bigcup_{i=1}^{5} \mathbf{S}_i\} = \{\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4, \mathbf{S}_5\} =$$

$$= \{\mathbf{S}_{\mathbf{SC}}, \mathbf{S}_{\mathbf{SL}}, \mathbf{S}_{\mathbf{BF}}, \mathbf{S}_{\mathbf{SR}}, \mathbf{S}_{\mathbf{MC}}\} = \{SC, SL, BF, SR, MC\},$$

Fig. 3.6. Sequence steps for implementation cyber attacks

where $\mathbf{S}_1 = \mathbf{S}_{\mathbf{SC}} = SC$, $\mathbf{S}_2 = \mathbf{S}_{\mathbf{SL}} = SL$, $\mathbf{S}_3 = \mathbf{S}_{\mathbf{BF}} = BF$, $\mathbf{S}_4 = \mathbf{S}$
$_{\mathbf{SR}} =$
SR , $\mathbf{S}_5 = \mathbf{S}_{\mathbf{MC}} = MC$

Fig. 3.7. The actions taken by the hacker in a cyber attack

To execute this phase, let’s initiate a series of actions denoted as A to enhance the cybersecurity of IR-PBX.

$$\mathbf{A} = \{\bigcup_{\mathbf{d=1}}^{v} \mathbf{A}_{d}\} = \{\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_v\},$$

Fig. 3.8. Enumerate the actions for enhancing PBX security.

Table 3.2

Description of the steps to execute cyber-attacks on IP PBX Asterisk.

No.	Code	Description
1	SC	Conducting network scans on the Internet to identify systems with open port 5060. SIP clients typically utilize port 5060 for TCP and UDP connections to servers, particularly in the initiation and termination of vocal and video calls.
2	SL	The system (Asterisk) actively searches for available SIP clients, sending requests until receiving confirmation of their existence. The intruder compiles a list of SIP clients in the format [1000] [1001] [1002].
3	BF	Initiating a “brute force” attack, employing programs to systematically guess passwords for SIP clients.

The end of the table 3.2

4	SR	Upon discovering the password, the attacker configures a softphone on their computer, registering it with the obtained external IP address (uncovered through scanning open port 5060), login (matching the SIP client number), and the deciphered password from the "brute force" process.
5	MC	With successful registration, the intruder gains the ability to make international calls and other unauthorized activities.

Table 3.3

Steps to enhance the cybersecurity of IP PBX Asterisk

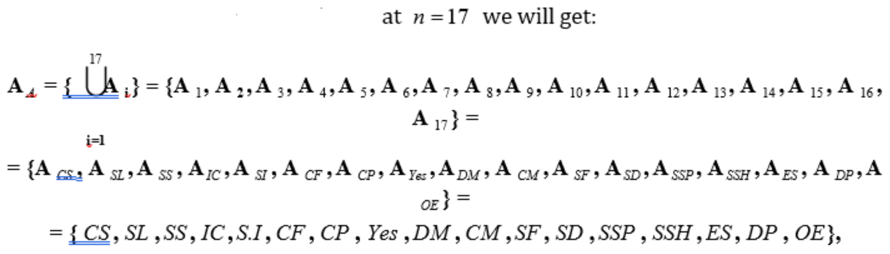
No.	Code	Description
1	CS	Modify SIP port settings (bindport = 3348 ;).
2	SL	Restrict SIP connections to the local network only (deny = 0.0.0.0 / 0.0.0.0; permission = 192.168.0.1 / 24; allowguest = no; call-limit = 2 ;).
3	SS	Implement safeguards to protect the server from number overruns (Alwaysauthreject = yes).
4	IC	Enforce complex passwords for SIP clients, utilizing password generators with official signs and numbers.
5	S.I	Block international calls at the Dial Plan level, triggering specific actions on matching patterns (ext => _3809X.,1,System(echo "That" ${EXTEN} "Ext" ${CALLERID(num)}

Continue of the table 3.3

6	CF	Configure the built-in iptables firewall settings (edit configuration file iptables).
7	CP	Change the SSH port, restrict root login via SSH, and introduce new security measures (useradd username, passwd username; AllowUsers username, PermitRootLogin no; Port 1265).
8	Yes	Disable Apache autoload and change its port (chkconfig httpd off server_ip_address: 7623).
9	DM	Disable unnecessary Asterisk modules and protocols (noload => chan_jingle.so noload => chan_skinny.so noload => chan_iax2.so noload => chan_console.so noload => chan_mgcp.so noload => chan_gtalk.so).
10	CM	Change the port for Asterisk Management Interface (AMI) (port = 8374).
11	SF	Configure the system fail2ban for enhanced protection against "Brute force" attacks.
12	SD	Implement defenses against DOS attacks by adjusting iptables rules. This includes setting conditions for handling multiport traffic and utilizing recent module features to identify and drop potential DOS attacks. Additionally, consider integrating iptables with the fail2ban system to log DOS attack messages for further analysis and notification via email.

The end of the table 3.3

13	SSP	Enhance protection against port scanning using iptables with xtables-addons.
14	SSH	Strengthen SSH security through certification. Explore options to allow SSH connections only from computers with attached certificates, involving key generation, authorized_keys file configuration, and key extraction to ensure secure connections. Audit and configure the SSH service in Linux.
15	ES	Improve security by disabling the Samba service (chkconfig smb off).
16	DP	At the provider level, consider implementing measures such as restricting international calls, setting call limits, and establishing maximum call cost limitations.
17	OE	Bolster security with the installation of a secure VPN connection, implementation of complex passwords for web interfaces on hardware phones, and modification of HTTP ports for added protection.



at $n = 17$ we will get:

$$\mathbf{A}_{A} = \{ \bigcup_{i=1}^{17} \mathbf{A}_{i} \} = \{\mathbf{A}_{1}, \mathbf{A}_{2}, \mathbf{A}_{3}, \mathbf{A}_{4}, \mathbf{A}_{5}, \mathbf{A}_{6}, \mathbf{A}_{7}, \mathbf{A}_{8}, \mathbf{A}_{9}, \mathbf{A}_{10}, \mathbf{A}_{11}, \mathbf{A}_{12}, \mathbf{A}_{13}, \mathbf{A}_{14}, \mathbf{A}_{15}, \mathbf{A}_{16}, \mathbf{A}_{17}\} =$$

$$= \{\mathbf{A}_{CS}, \mathbf{A}_{SL}, \mathbf{A}_{SS}, \mathbf{A}_{IC}, \mathbf{A}_{SI}, \mathbf{A}_{CF}, \mathbf{A}_{CP}, \mathbf{A}_{Yes}, \mathbf{A}_{DM}, \mathbf{A}_{CM}, \mathbf{A}_{SF}, \mathbf{A}_{SD}, \mathbf{A}_{SSP}, \mathbf{A}_{SSH}, \mathbf{A}_{ES}, \mathbf{A}_{DP}, \mathbf{A}_{OE}\} =$$

$$= \{ CS, SL, SS, IC, S.I, CF, CP, Yes, DM, CM, SF, SD, SSP, SSH, ES, DP, OE\},$$

Fig 3.9. Actions for improvement cyber security IP PBX Asterisk

CHAPTER CONCLUSIONS

In the ongoing effort to fortify the cybersecurity landscape of IP-PBX systems, the developed data model serves as a pivotal tool. By meticulously outlining IP-PBX vulnerabilities and elucidating the intricate steps involved in executing a cyber attack, the model provides a holistic understanding of the potential risks associated with IP-PBX infrastructure. Furthermore, it offers a proactive framework, consisting of actionable steps, to preemptively strengthen the defenses of IP-PBX against cyber threats.

The significance of this model extends beyond its immediate application, as it addresses the pressing need for robust cybersecurity measures within the intricate web of modern communication systems. Targeted primarily at system administrators and information security specialists operating within CERT/CSIRT-type cyber incident response teams, the model equips these professionals with the tools necessary to safeguard critical IT infrastructure within enterprises and organizations.

Looking ahead, the next phase of research endeavors involves establishing interconnections between vulnerabilities across various species and domains. This collaborative approach seeks to weave a comprehensive tapestry of cybersecurity measures tailored specifically for IP-PBX. By discerning and addressing potential weak points, this research aims to establish a resilient cybersecurity framework, thereby mitigating the risk of cyber incidents and fortifying the overall security posture of IP-PBX systems. The collaborative nature of this research ensures that it remains dynamic and adaptive to emerging cyber threats, providing ongoing support for IT security practitioners and decision-makers alike.

CHAPTER 4
OCCUPATIONAL SAFETY

The imperative of ensuring labor protection applies to every stage of the labor process within PBX (Private Branch Exchange) systems, regardless of the specific professional activity involved. The creation of a safe and healthy working environment in PBX settings depends significantly on the accurate assessment of potential dangers and harmful production factors. The complexities that may arise in an individual's body can stem from various sources, including factors within the production environment, excessive physical and mental workloads, neuro-emotional stress, and combinations of these elements.

Highlighting the significance of labor protection within PBX systems, consider the role of a programmer in the Information Technology department of an airline. This significance is particularly evident during the development phase of a software complex designed for overseeing network software functionality, detecting and addressing defects and crashes, as well as diagnosing and identifying issues in operational network equipment through the analysis of spectral signal graphs.

It is pertinent to note that the Information Technologies department, where the programmer operates, is situated within the central hub of the airline. This underscores the importance of implementing robust labor protection measures in critical areas like PBX, ensuring the well-being and safety of individuals involved in these technological processes.

4.1 Analysis dangerous and harmful factors, what effect on a programmer

The temperature and humidity in the PBX (Private Branch Exchange) department are monitored using devices such as the Augusta hygrometer, aligning with values specified for the warm period of the year. Within the premises housing 6 PBX stations, which serve as sources of heat emissions, microclimate systems with heated surfaces are utilized to maintain optimal conditions during the colder periods. The normalized indicator ICV represents the marginally permissible density of energy flow, etc., measured in W/m², with values set based on the square irradiated surface of a person (Sopr). The normalized levels are as follows for PBX operators: etc. = 35 W/m² when Sopr > 50%; etc. = 70 W/m² when Sopr is approximately 25-50%; etc. = 100 W/m² when Sopr < 25%.

In terms of lighting, the normalized parameter for natural lighting, according to, is the coefficient of natural lighting (KPO). KPO is determined based on the visual tasks at hand, considering PBX operations as falling under secondary accuracy works (IV discharge of visual works) [22]. For artificial lighting, the normalized parameters are Emin – the minimum level of illumination, and Kp – the coefficient of light stream pulsations, which should not exceed 20%. The minimum light level is determined based on the nature of visual tasks, with IV discharge of visual works requiring 300-500 lux.

Concerning production radiation, acceptable values for non-ionizing electromagnetic radiations from computer monitors are presented in tables 5.2. The normalized parameter for unused X-ray radiation is the power expositional doses. At a distance of 5 cm from the surface of the PBX monitor screen, the radiation level should not exceed 100 μR/hour. The maximum level of X-ray radiation at a PBX operator's workplace usually does not exceed 20 μR/hour.

Table 4.1

Acceptable parameters non-ionizing electromagnetic radiations

Parameter name	Let's admitand value
The voltage of the electric component of the electromagnetic field on a distance of 50 cm from the surface of the PC monitor	10 W/m

The end of the table 4.1

The intensity of the magnetic component of the electromagnetic field at a distance 50 cm from the surface of the PC monitor	0.3 A/m
The tension for PC operators should not exceed	20 kV/m

At a distance of 5-10 cm from the PBX screen and the monitor body, voltage levels can reach 6 V/m in the electrical component, which remains within permissible values.

Concerning electrical safety and static electricity in the PBX department premises, the risk of electric current damage is categorized as Class 1. This classification designates rooms without increased danger—dry, dust-free, with normal temperature air, insulated floors, and a minimal number of grounded devices.

At the PBX operator's workstation, only the systemic block of the computer, adhering to the standard of the IBM firm, has a metallic casing. According to, specifically item 5 "Events on protection from static electricity," grounding must be installed on systemic blocks to neutralize static electricity. Upon inspecting the system unit, it was found that grounding is missing, thus not adhering to the specified norms. [23]

The primary reasons for electric current damage to an individual at a PBX workstation include:

- Contact with metal non-conductive parts (computer casing) that may become energized, resulting in damage to isolation.

- Improper use of electrical devices.

- Lack of employee training on electrical safety rules in the PBX department.

4.2 Organizational and constructive and technological activities for decrease the influence of harmful production factors.

Normalization of air in PBX working zones is implemented to ensure optimal values of temperature, humidity, cleanliness, and air movement speed, regardless of external conditions. During the cold months, watery heating is utilized, while air conditioning is employed in the warm months [24].

In terms of production lighting, an analysis of the lighting in the PBX operator's workspace revealed that it does not meet the established norms. To enhance working conditions, it is recommended to increase the overall illumination of the rooms by installing five additional lamps, bringing the total number of lamps to 36 LED lamps. Additionally, a cleaning schedule should be implemented to ensure that windows and lamps are cleaned at least twice a year to maintain the projected lighting levels [22].

For electrical safety in the PBX department, the following technical measures are suggested:

- To reduce the accumulation of static electricity, use moisturizers and neutralizers, along with applying antistatic coating on floors.
- Ensure the connection of metal structures of equipment to a ground. Grounding the PBX equipment should be connected to a common ground at the outlet with a resistance grounding of 4 Ohms, following the guidelines of the Electrical Code for installations with voltages up to 1000 V. Organizational measures include conducting timely safety briefings [25].

In terms of ergonomics and the organization of working spaces, an analysis of PBX operator workstations revealed compliance with established requirements. To address challenges and alleviate labor-related difficulties and tensions, it is recommended to reduce computer work time and incorporate breaks, with a suggested break duration of 50 minutes during an 8-hour workday [26].

Based on measurements using a lux meter (Yu-116), the natural illumination level at the surface where the PBX operator's equipment is situated is 200 lux, while the illumination of the same surface when exposed to sky light is 20,000 lux. This results in a coefficient of natural lighting (KPO) of 1%, which does not meet the regulatory KPO.

For artificial lighting in the indoor PBX environment, LED lamps T8 G13 are employed. These lamps offer several advantages compared to fluorescent and incandescent lamps, including a spectral composition close to natural light, increased light output (2-5 times higher than incandescent lamps), and a longer service life (up to 10 thousand hours) [22].

To calculate artificial lighting for a room with an area of 40 m2, a width of 5 m, length of 8 m, and height of 3.5 m in the PBX department, the coefficient method is applied using the light flow.

To determine the necessary quantity of lamps required to achieve the normalized level of illumination, the luminous flux falling on the working area's surface is calculated using the formula:

$$F=E*S*K*Z/n \qquad (4.1)$$

(where **F** – light flow, what is calculated Lm; **E** – normalized minimal light, Lk; IS = 300 Lk; **S** – area of the illuminated PBX rooms (in our case S = 40 m ^{2}); **Z** – relation secondary illumination to minimal (usually is accepted equal 1,1...1,2, in our case Z=1.1); **K** – coefficient stock, what takes into account reduction light flow lamps in as a result pollution lamps in process operation (him value depends from type rooms and character works, what are held in him in our case K=1.5); **n** – coefficient using light stream, (expressed relationship light stream, what is falling on calculation surface, to total flow everyone lamps, and is calculated in fates units ;) depends from characteristics lamp, size of the PBX room, color walls and ceilings, what are characterized coefficients reflection from walls (ρ Art.) and the ceiling (ρ ceiling), value coefficients are equal ρ Art = 40% and ρ ceiling =60%.

Let's calculate index rooms by the formula:

$$i=S/h(A+B) \quad (4.2)$$

(where **S** is the area of the room, S=40 m^2 ; **h** – the estimated height of the suspension, h = 3.3 m; **A** – room width, A = 5 m; **B** is the length of the room, B = 8 m.)

Substituting value we will get: **and=40/3.3(5+8)=0.93** . knowing index room, we find **n=0.22** . Let's substitute all the values in the formula for determination luminous flux

$$F=(300*1.5*40*1.1)/0.22=90000 \text{ Lum.} \quad (4.3)$$

For lighting used LED lamps with matte coating type LRC-T8-S1500G13-220-22.0W, the luminous flux of which **F l = 2500** Lm

$$N=F/F \quad (4.4)$$

(where N – determined numeric lamps; F – light flow, F=90000 Lm ; Fl – light flux of one lamp, F l = 2500 Lm .)

4.3 Firefighter security

The PBX infrastructure within the central office of the airlines is classified under explosion fire and fire station danger, following the guidelines outlined in , placing it in category D [25].

"Non-combustible materials in controlled environments, encompassing spaces housing GRs in machinery, cooling and hydraulic drive systems of equipment, each unit weighing no more than 60 kg at pressures not exceeding 0.2 mPa, along with electrical wiring cables to equipment and specific pieces of furniture in designated areas."

The central office, which accommodates the PBX system, falls under the construction category K1 (low fire hazard). This classification is attributed to the presence of combustible materials such as books, documents, furniture, and office equipment, as well as heavier-burning substances like safes and various equipment. In the event of a fire, these materials can burn without causing an explosion.

Considering its structural characteristics, the building aligns with those constructed with supporting and enclosing elements crafted from natural or artificial stone materials, concrete, or reinforced concrete. The construction of floors allows for the use of wooden structures, provided they are shielded with plaster or fire-resistant materials, including plate materials.

Consequently, the central office building's fire resistance is designated as the third (III). The IT department rooms within the airline's premises fall under the functional fire hazard category, specifically classified as F 4.2.

4.3.1 Causes of fire

A fire in the PBX room can lead to severe consequences such as the loss of valuable information, harm to individuals, deterioration of property, and more. Therefore, it is essential to identify and eliminate all potential causes of fires. Developing a comprehensive plan for fire extinguishment within the facility and establishing evacuation procedures for the occupants is crucial.

Potential causes of fires may include malfunctions in wiring, outlets, and switches leading to short circuits or breakdowns in insulation. The use of damaged or faulty electrical appliances, electric heating devices with open heating elements, lightning strikes, external influences, and mishandling of fire are also factors contributing to fire incidents.

In accordance with safety guidelines , a fire protection regime should be implemented on the premises, including the organization of operations and maintenance of available fire protection equipment such as fire protection water supply, pump stations, fire alarm systems, automatic firefighting systems, smoke removal systems, fire extinguishers, etc. For fire extinguishing in the PBX room, a portable carbon dioxide fire extinguisher type VVK-5 has been installed, appropriate for the room's size and type [25].

Additionally, two wireless IR smoke sensors, Guard M-501, are mounted on the ceiling, designed to cover an area of 40 m².

In the event of a fire, it is essential to activate the fire alarm. Simultaneously, it is necessary to turn off the power supply, contact the fire department at number 101, and initiate the evacuation of individuals from the premises following the evacuation plan outlined in Drawing 5.1. Additionally, the immediate response should involve utilizing fire extinguishers for the prompt extinguishment of the fire.

In case of small fire pits, readily available means should be used to terminate the air supply to the ignition source, helping to contain and control the fire.

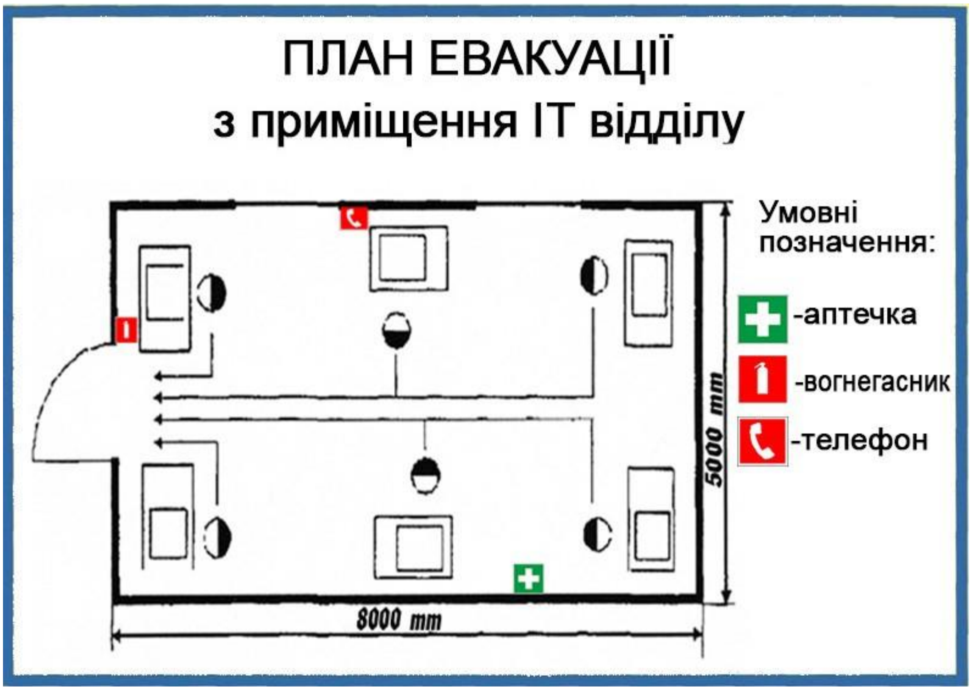


Fig. 4.1. Evacuation plan from the premises of the company's IT department

4.4 Instruction on labor protection when working with a personal computer

General requirements for PBX workplace equipment:

- Arrange the PBX workplace to prevent light from windows, lighting devices, and reflective surfaces from entering the operator's field of sight. Avoid polished surfaces on the working table to prevent reflections on PBX monitor screens, particularly during sunny days. Place the PBX monitor screen so that the light from windows falls from the side, preferably the left.
- Position the PBX monitor's screen at a distance of at least 500-700 mm from the operator's eyes. Optimal viewing angles range between 10-40 degrees. Place the screen perpendicular to the operator's line of sight for the best positioning.
- Ensure the PBX is situated at a distance no closer than 1 meter from heat

sources.

- Place the PBX keyboard on the table surface or a dedicated stand, positioned 100-300 mm from the edge facing the user. Maintain an inclination angle for the keyboard panel ranging from 5 to 15 degrees.
- Set the height of the working table surface within the range of 680-800 mm.
- Provide a chair that offers the PBX operator comfortable working conditions and a physiologically sound posture. The chair should allow adjustments for the seat surface height, backrest angle, and backrest height.
- Equip windows with sunscreen devices to prevent direct sunlight and glare on the PBX monitor screen. Position the video monitor so that light from windows falls on the working place from the side, preferably the left.
- Use fluorescent lamps as the primary source of artificial lighting in PBX rooms. For local lighting, consider incandescent bulbs. Ensure a minimum of 400 lux for horizontal plane light at a height of 0.8 m from the floor and limit vertical light in the screen plane to not exceed 200 lux. To reduce eye strain, maintain a uniform distribution of brightness on the PBX monitor's working surface and the surrounding space.
- Ensure daily wet cleaning and regular ventilation in PBX work premises, with a focus on dust removal from the screen at least once a day.
- Utilize protective screens to safeguard the operator from electromagnetic radiations and electrostatic fields emanating from the PBX equipment.
- When using PBX systems, users should opt for clothing made of natural materials or a blend of natural and artificial fibers.
- Safety protocols before initiating work on the PBX system:
- Prior to commencing work, employees should conduct an external review to verify the integrity of the PBX system components, including the systemic block, video monitor, printer, and keyboard.
- Inspect the integrity of power cables, examining connection points such as power sockets, power strip successors, branching boxes, and plug forks.

- Prepare the working space by removing any items that could hinder the work process.
- Power on the PBX system.
- If the PBX system encounters loading issues or fails to enter the working mode upon startup, employees should promptly inform the manager or the IT department specialist.
- Report any damages or defects to the direct manager and refrain from starting PBX-related tasks until receiving further instructions.

Safety requirements during work

- Ensure all components of the PBX devices are stably positioned on the table, including the keyboard. Additionally, there should be flexibility in moving the keyboard, allowing users to adjust its location and angle to their preferences. If the keyboard structure lacks space for palm support, it should be placed at a distance of at least 100 mm from the table's edge within the optimal zone of the monitor's field. When using the keyboard, adopt a straight sitting posture to prevent strain.
- Allocate a spacious area on the table for the "mouse" device to facilitate smooth movement and comfortable resting of the ulnar joint, minimizing any adverse impact on the user.
- Discourage external conversations, annoying noises, or other distractions during work.
- Periodically, when turning off the PBX system, use a slightly moistened soapy solution applied with cotton and paper napkin to clean the surfaces of the equipment. Wipe the screen and protective screen with cotton wool moistened with alcohol.
- Avoid using liquid or aerosol cleaning agents on PBX surfaces, as they are not permitted.

Prohibited:

- Avoid attempting to independently repair PBX equipment with high-voltage elements, such as the kinescope, without proper expertise (up to 25 kV).

- Refrain from placing any items, including food and drinks, on or near the PBX equipment, keyboard, as it may lead to disorder and potential damage.

- Ensure ventilation openings in the PBX equipment are not obstructed to prevent overheating and malfunctions.

To mitigate the negative impact on the health of employees working on PBX systems, consider the following recommendations for regulated breaks:

- Take a 10-minute break after every continuous work session.

- Schedule a 15-minute break every 2 hours.

Rotate and diversify activities during breaks to reduce monotony, alternating between tasks unrelated to PBX work.

When working with PBX systems:

- Position the equipment adjacent to the system unit, avoiding taut cords. Do not place the PBX equipment on the system bloc.

- Confirm that the PBX equipment is in connection mode with the system block before initiating any program work.

- Use paper specified in the PBX instructions, typically ranging from 60-135 g/m², such as Canon or Xerox 4024.

- Trim paper edges sharply with a blade knife to reduce the risk of paper jams.

- When not actively working on programs for more than 20 minutes, consider turning off the video monitor to conserve energy.

- To maintain general muscle tone, prevent musculoskeletal disorders, visual discomfort, and other subjective feelings, incorporate recommended exercises for the eyes, spine, and hands during regulated breaks. Tailor the number and content of micro-pauses, lasting 1-2 minutes, to individual needs, including tasks unrelated to PBX work, eating, and implementing recommended exercises. Include physical exercises throughout the day, adjusting based on individual fatigue levels, to correct posture, improve blood circulation, and compensate for limited motor activity.

CHAPTER CONCLUSIONS

In conclusion, the outlined general requirements and safety protocols for PBX workplace equipment constitute a comprehensive framework designed to prioritize the well-being and productivity of operators working within this environment. The meticulous guidelines cover various aspects ranging from the physical arrangement of the workplace to safety measures during work and regulated breaks.

The ergonomic considerations emphasized in the guidelines aim to create an optimal working environment for PBX operators. From the placement of the PBX monitor to the arrangement of the keyboard and mouse, every detail is strategically positioned to enhance comfort, prevent strain, and promote a physiologically sound posture. Notably, the emphasis on the use of natural materials in clothing, along with safety protocols before initiating work, underscores the commitment to safeguarding both the physical and technological aspects of the workplace.

Furthermore, the safety requirements during work highlight the importance of stable positioning of PBX devices, along with the need for flexibility in adjusting peripherals like the keyboard to suit individual preferences. Prohibitions against attempting high-voltage equipment repairs without expertise and placing items near PBX equipment underscore the commitment to safety and equipment integrity.

The guidelines extend beyond the physical aspects of the workplace to regulated breaks, recognizing the importance of mental and physical well-being. The recommended breaks and activities are geared towards mitigating the potential negative impact on the health of PBX operators, promoting a balanced and sustainable work routine.

In essence, these comprehensive guidelines serve not only as a set of directives but as a commitment to creating an environment that fosters the health, safety, and optimal performance of PBX operators. Adhering to these recommendations ensures a harmonious and efficient work atmosphere, reinforcing the importance of responsible and mindful practices in the operation and maintenance of PBX systems.

CHAPTER 5
ENVIRONMENTAL PROTECTION

5.1 Analysis impact man-made factors on the environment natural environment

As a consequence of extensive human involvement in the realm of PBX systems, substantial changes have taken place. These modifications have given rise to an environment where the traditional boundaries of PBX technology have been surpassed, leading to an evolution in communication systems. Scientific data suggests that

contemporary PBX environments are largely shaped by human intervention, covering a wide range of communication landscapes and even extending beyond conventional borders.

The PBX environment, as a component of the communication landscape, is a byproduct of human activity resulting from the influence of anthropogenic factors. Within this man-made communication system, individuals are consistently involved in at least two primary tasks:

- Ensuring seamless communication within the designated network.
- Establishing and utilizing protective measures to counteract the adverse effects of potential disruptions.

A distinction is made between the direct and indirect negative impacts of the PBX environment on both the communication infrastructure and its users [27].

5.2 Principle work basic stations and cellular devices and their negative impact on the environment

In light of the rapid expansion of technologies and devices, it's nearly impossible to completely avoid exposure to electromagnetic fields (EMF) in the contemporary world. Telephone handsets and base stations employed in PBX systems serve as sources of EMF in the context of telecommunication. The mechanisms governing the impact of these EMF sources on individuals differ.

A notable characteristic of a PBX system, in terms of EMF emission, is its potential proximity to the user's head during operation, typically within a range of a few centimeters in uncontrolled conditions. The effects of EMF are felt in receptor zones such as the vestibular and auditory analyzers, as well as the retina of the eyes, affecting both the central and peripheral components of the brain. It's essential to acknowledge that the negative consequences of PBX-related electromagnetic radiation may also extend to individuals in the immediate vicinity of the user during communication.

Electromagnetic fields generated by PBX systems are characterized by impulses. The intensity of this generation varies based on factors such as the time of day, the saturation of coverage in PBX stations, and the number of PBX stations within a particular zone.

PBX stations are strategically placed to cover entire zones, creating an artificial electromagnetic field within the realm of telecommunication.

As PBX stations are typically situated in locations where people are present continuously, there is a persistent, round-the-clock impact on individuals from a low-intensity electromagnetic field within the radio frequency range. According to data from ecologists and hygienists, it is well-documented that electromagnetic radiation across all ranges can affect human health and overall well-being, leading to serious consequences. The widespread influence of electromagnetic fields, especially in the context of PBX systems, is considered more concerning than radiation due to its continuous prevalence.

Electric fields of industrial frequency surround individuals constantly, emanating from various sources such as wiring, lighting equipment, household electrical appliances, and power lines associated with PBX infrastructure.

The energetic load from electromagnetic radiation in both the realm of PBX systems and everyday life is consistently increasing due to the rapid expansion of network sources generating electromagnetic fields and the concurrent increase in their capacities. While individuals may not physically feel the electromagnetic field, it can lead to a reduction in adaptive reserves, a decrease in immunity, and a decline in overall working capacity. Exposure to the electromagnetic field associated with PBX systems can contribute to the development of chronic fatigue syndrome and an increased risk of various diseases. This impact is particularly concerning for children, teenagers, pregnant women, and individuals with compromised health.

The influence of the electromagnetic field on PBX systems is noteworthy. It affects charged particles and currents, leading to the transformation of energy fields at the cellular level into other types of energy within the telecommunication infrastructure.

Cytogenetic research, specifically investigating chromosomal aberrations, revealed a significant increase in cells with abnormalities within the experimental group compared to the control group in the context of PBX systems. This rise in chromosomal aberrations was also noted during the irradiation of air-dry seeds and seedlings of lettuce associated with PBX technology. Additionally, cytogenetic analysis of blood cells from cows on the farm connected to PBX systems indicated an elevated number of genetic lesions and instances of abnormal hematopoiesis [28].

Examining the effects of electromagnetic fields on tissues within the PBX environment, it was observed that weak electromagnetic fields at intensities below the thermal effect threshold induce changes in living tissues. Research specifically focused on the biological impact of PBX equipment, such as cellular phones, computer blocks, and other electronic devices. These studies revealed that these PBX-related sources negatively influence tissue regeneration.

In the molecular context of PBX systems, electric fields cause the polarization of electrically polarizable molecules, aligning them in the direction of magnetic field propagation. Alternating electric fields, characteristic of PBX environments, induce heating in the living tissues of organisms through variable polarization of dielectric materials (such as tendons, cartilage, and bones) and the generation of conduction currents.

The impact of electromagnetic fields on the nervous system within the context of PBX systems has its origins in experimental research conducted in the USSR. These studies revealed a direct effect of electromagnetic fields on the brain, neuronal membranes, memory, and conditioned reflex activity. Model experiments demonstrated the potential of weak electromagnetic fields to influence synthesis processes in nerve cells. Significantly, alterations in cortical impulses of neurons were observed, leading to disruptions in the transmission of information to more complex structures in the brain. It was found that exposure to electromagnetic fields in the ultra-high-frequency range, characteristic of PBX systems, may result in disturbances in short-term memory.

In terms of the influence of electromagnetic radiation on the immune system within the PBX environment, a considerable body of data indicates that immunogenic processes are disrupted under the influence of electromagnetic fields. It has been established that changes in the nature of infectious processes arise due to the influence of electromagnetic fields associated with PBX systems.

Disruptions in protein exchange within the bloodstream are evident in PBX systems, with a decrease in albumin content and an increase in gamma globulins. Additionally, PBX-associated electromagnetic fields can act as allergens or triggering factors, leading to severe reactions in allergic individuals upon exposure.

Examining the influence of electromagnetic fields on the reproductive system within the context of PBX, there is a documented decrease in spermatogenesis function, alterations in the menstrual cycle, slowed embryonic development, and an increased incidence of innate mutilations in newborns. Moreover, lactation in nursing mothers is observed to be reduced under the influence of PBX-related electromagnetic radiation.

Turning to the impact of electromagnetic fields on plant life within PBX environments, extensive studies highlight their significant effects on biological entities. Both weak and strong electromagnetic fields associated with PBX systems exert pronounced influences on the morphological, physiological, biochemical, and biophysical characteristics of various plants, affecting their growth, development, and reproduction.

In a theoretical context, electric field levels near PBX infrastructure, such as air lines, are deemed sufficient to cause damage to plant leaves. Observations and experiments focused on the impact of electromagnetic fields from PBX power transmission lines on plants indicate a reduction in the dry mass balance above-ground in oats and sunflowers compared to control conditions. This negative impact extends to the nitrogenous activity in soil rhizosphere populations and the length of plant seedlings.

The influence of weak electromagnetic fields on living organisms, even at intensities below the thermal effect threshold, is notable within PBX settings. Research on the biological impact of electronic devices, including cellular phones and computer blocks, conducted in various scientific centers, assesses the harm caused by these PBX-associated devices in both operational and switched-off conditions, even without a power supply [29].

The findings from studies evaluating the impact of PBX systems, including cell phones, computers, and other modern radio-electronic devices, on various organisms, both in their operational and off states, were disconcerting. They revealed a significantly negative influence on the state of biological entities, characterized by:

- Diminished motor activity and decreased survival of microorganisms.
- Elevated mortality rates among microorganisms.
- Impaired tissue regeneration.
- Disruptions in embryonic and larval development.
- Decreased biochemical reactions and instances of metabolic disorders.

- Lowered energy potential across all vital systems of the body.

5.3 Methods and means protection surrounding environment from impact technogenic factors

Protection against electromagnetic radiation in PBX systems. In order to mitigate the impact of electromagnetic fields (EMF) on personnel and individuals within the vicinity of PBX systems, a comprehensive set of protective measures must be implemented. These measures encompass organizational, engineering and technical, as well as medical and preventive aspects.

The implementation of organizational and engineering and technical measures is primarily the responsibility of health authorities. Collaborating with sanitary laboratories at enterprises and institutions utilizing electromagnetic radiation sources, efforts should be directed towards conducting hygienic evaluations of new construction and reconstruction projects involving PBX radio equipment. This includes new technological processes and equipment utilizing EMF. Continuous sanitary supervision is essential for objects using radiation sources, and organizational and methodological work should focus on preparing specialists for engineering and technical supervision [30].

During the design stage, particular attention should be given to securing a mutual location of irradiating and irradiated objects that minimizes the intensity of irradiation.

Recognizing the impossibility of completely avoiding exposure, efforts should be directed at reducing the probability of individuals entering high-intensity EMF areas and minimizing the duration of exposure.

Significant emphasis is placed on engineering and technical methods and means of protection specific to PBX systems, including collective protection (group of buildings, district, settlement), local protection (individual buildings, rooms), and individual protection. Collective protection involves calculating the spread of radio waves in the specific relief area. Economically, it is advisable to utilize natural screens such as terrain folds, forest plantations, and non-residential buildings.

Installing antennas on elevated terrain in PBX systems can effectively reduce the intensity of fields irradiating the settlement. Similar results can be achieved through proper antenna orientation, especially with highly directional antennas. However, the challenges of complexity, cost, and stability increase with higher antennas. Additionally, the effectiveness of such protection diminishes with distance.

When safeguarding against screen radiation in PBX systems, consideration must be given to the attenuation of waves passing through the screen, for example, through a forest strip. Vegetation can also serve as a valuable tool for screening. Special screens in the form of reflective and radio-absorbing shields are rarely used in PBX systems due to their high cost and limited effectiveness.

Local protection within PBX systems is a highly effective strategy frequently employed to minimize the impact of electromagnetic fields (EMF) on personnel and individuals in proximity to radio-electronic devices. This protection primarily relies on the use of radio-protective materials designed for high energy absorption of radiation within the material and reflection from its surface. Shielding by reflection often involves the use of metal sheets and conductive nets with suitable conductivity.

Shielding premises from external radiations in a PBX environment can be achieved through various means, including the application of metallized wallpaper, protective age grids, and metallized curtains [30]. These measures substantially reduce irradiation within the protected space, with any reflected radiation dispersing across the area and minimizing its impact on other objects.

When it comes to personnel working closely with PBX radio equipment, it is crucial to provide reliable protection by effectively shielding the equipment.

Reflective screens are commonly used, and alongside these, there is widespread utilization of materials specifically designed to absorb radiation. These radio-absorbing materials come in various forms, including homogeneous compositions and composites incorporating different dielectric and magnetic substances. To enhance the efficiency of the absorbent surface, screens are often designed to be rough, ribbed, or in the form of spikes. Interestingly, radio-absorbing materials can also be applied for environmental protection from EMF, particularly when the source is located within shielded objects.

In the context of PBX systems, personal protective equipment, such as clothing made from metallized fabrics and radio-absorbing materials, is reserved for situations where other protective measures cannot be applied or are not sufficiently effective. These scenarios may include working in zones with increased radiation intensity, conducting repairs during emergencies, engaging in short-term control, or when adjusting exposure intensity. However, it's essential to note that such protective measures can be inconvenient, potentially limiting work operations and affecting hygienic conditions.

In the realm of PBX systems, clothing made from metallized fabrics involves cotton or kapron threads spirally wrapped with metal wire, providing effective radiation weakening by at least 20-30 dB. When stitching details of protective clothing, isolated conductor contacts are crucial. Electrosealing seams are conducted using conductive solutions or glues, ensuring galvanic contact or increasing the capacitive connection of non-contacting wires.

The eyes are protected by special glasses made of glass with a coating on the inner side, leading to a film of tin dioxide. The glasses have a rubber rim, and a metal grid is either pressed into the rubber or pasted over with metallized fabric. These glasses effectively weaken microwave radiation by 20-30 dB.

In the context of PBX systems, the use of gloves and shoe covers, once considered essential, is now deemed unnecessary. This shift is attributed to the acceptable energy flow density for hands and feet, which is significantly higher than that for the body.

Both collective and individual means of protection play a crucial role in ensuring the enduring safety of personnel working with PBX facilities [30].

Addressing noise protection, the most effective strategy in combating noise within PBX systems is to tackle its source. This involves implementing low-noise mechanical transfers and developing methods to reduce noise in bearing assemblies and fans.

To diminish noise through sound absorption in PBX environments, the emitting object is encased, and the inner walls of the casing are coated with sound-absorbing material. It is essential for the casing to possess adequate sound absorption capacity without impeding equipment maintenance during work or compromising the interior aesthetics of the workshop. An alternative method involves using a cabin where the noisiest object is housed, allowing the worker to operate within. The interior of the cabin is lined with sound-absorbing material to reduce the noise level inside, aiming not only to isolate the noise source but also to minimize its impact on the surrounding production premises within the PBX system.

Decreasing noise: sound insulation. This method involves strategically situating noise-emitting objects or the most prominent sources of noise separately, isolating them from the main, less noisy areas through the construction of soundproof walls or partitions. Achieving sound insulation is also possible by housing the noisiest components within a dedicated cabin. It's crucial to acknowledge that while the overall noise level might not decrease within isolated indoor spaces and cabins, the impact is minimized for a smaller group of individuals.

Sound insulation measures in PBX environments also encompass placing the operator in a specially designed cabin, allowing them to oversee and manage the technological processes. Additionally, the installation of screens and caps contributes to a soundproof effect, shielding the working space and individuals from the direct impact of sound. It's important to note that while these measures enhance localized sound protection, they may not necessarily reduce the overall noise levels in the room.

Decreasing noise: acoustic processing of rooms. Acoustic processing of rooms involves covering the ceiling and upper parts of walls with sound-absorbing material. This application results in a decrease in the intensity of reflected sound waves. In addition to treating the ceiling, sound-absorbing shields such as cones, cubes, and resonator screens can be hung or installed. These artificial absorbers are efficient in reducing reflected sound intensity. The effectiveness of acoustic processing in rooms depends on the sound-absorbing properties of the materials and structures used, their location, the volume and geometry of the rooms, and the placement of noise sources. This effect is more pronounced in low premises (where the ceiling height does not exceed 6 meters) with an elongated shape. Acoustic treatment can reduce noise by up to 8 dBA [30].

Efforts to decrease noise levels should be incorporated at the design stage of industrial objects and equipment. Special attention should be given to housing noisy equipment in separate rooms, allowing for the reduction of the number of workers exposed to increased noise levels. Measures to minimize noise should be implemented with a focus on cost-effectiveness, requiring minimal expenditure of funds, equipment, and materials. Successful noise reduction necessitates addressing all sources of high-level equipment noise.

The work of noise reduction in actively productive environments starts with creating noisy charts and spectra for equipment and production premises. Based on these analyses, decisions are made regarding the direction and strategies for noise reduction efforts.

CHAPTER CONCLUSIONS

The rapid advancement of electronics and radio equipment in PBX systems has contributed to the emission of electromagnetic radiations, leading to environmental pollution. The primary culprits for these emissions within PBX systems are radio devices, television connections, and radar equipment. In the vicinity of each regional center, numerous district centers, and major cities, one can find television centers, repeaters, radio stations, and diverse radio communication facilities associated with PBX networks

To reduce the impact of electromagnetic fields on personnel who are located in zone actions some radio electronic means necessary is number protective activities: organizational, engineering and technical and medical and preventive.

There are sanitary standards developed on the basis of medical and biological research and rules regarding radio engineering and electrical engineering objects. They regulate conditions their operation with purpose protection people from harmful impact electromagnetic radiation.

So, on stage designing mutual placing objects has be provided in such a way that the intensity of irradiation is minimal. Also it is necessary to take care in advance to reduce the time spent by personnel in the zone exposure Power sources radiation must be the smallest with possible In addition, it is necessary to demand from the governing bodies compliance with state lawsstandards of Ukraine and not to violate their norms.

CONCLUSIONS

Indeed, IR-telephony represents a paramount facet in the evolution of telephone communication, a relatively nascent realm that initially grappled with challenges distinct from security concerns. Primarily focused on ensuring communication reliability and quality, the field has witnessed a substantial surge in Internet telephony subscribers each year. This surge can be attributed to the advantageous conditions offered by IP networks, where the cost of transmitting voice and video data is notably lower. Today, both individual clients and large enterprises, including state institutions, leverage the Internet as the backbone of their telephone communication infrastructure.

As the utilization of personal information becomes increasingly confidential, the imperative of securing this mode of communication intensifies. In contrast to traditional telecommunications networks, IP telephony boasts several advantages. The use of Voice over Internet Protocol (VoIP) not only reduces communication time between subscribers but also presents a more economical means of conducting communication sessions. With VoIP, users pay solely for data connections, eliminating the need for traditional telephone lines and associated infrastructures. Leveraging existing network infrastructure further enhances cost-effectiveness and reduces necessary bandwidth, resulting in decreased tariffs.

Despite these advantages, the security of IP telephony emerges as a critical concern. The ubiquitous integration and rapid evolution of information technologies in today's interconnected world underscore the indispensability of telephones, computers, and the Internet in people's lives. As such, this study delves into the imperative task of augmenting the security level of IP telephony networks and safeguarding access to confidential information within these networks.

The research scrutinizes the legislative landscape governing the operation and security of IP telephony systems in Ukraine, comparing it with the regulatory frameworks in the USA and Europe. Findings underscore a significant gap, with Ukrainian legislation in the realm of information technologies and security trailing behind its Western counterparts. Additionally, the study recognizes the ambiguity surrounding VoIP systems for Ukrainians.

Subsequent stages of the research involve a meticulous examination of the Internet telephony system, its components, and operational frameworks. Recognizing that the development of security tools necessitates an in-depth understanding of network vulnerabilities, the study analyzes potential attacks on VoIP systems that could compromise information confidentiality, integrity, and availability. The need for enhanced protection systems and the development of countermeasures to address specific vulnerabilities is emphasized, including the creation of auxiliary applications to block suspicious IP addresses.

To ensure secure operations in IP systems, the study puts forth universally accepted recommendations, including the secret storage of passwords, one-time codes, and cryptographic keys, as well as the immediate blocking of accounts in the event of security breaches.

The research proposes a comprehensive approach to safeguarding IP telephony solutions, encompassing VoIP server settings, firewall implementation, and encryption of telephone conversations. The analysis advocates for the use of TLS and SRTP protocols for voice data encryption, coupled with the transmission of encrypted voice data between remote users through IPsec tunnels. A devised algorithm for blocking suspicious IP addresses further strengthens the security system.

The research concludes with a presentation of the application's results, highlighting the implemented protection against suspicious interference. Recognizing the vulnerability of both traditional and IP telephony systems to attacks, the study underscores the importance of diligently implementing and configuring IP systems to minimize risks while maintaining cost-effectiveness.

REFERENCES

1. Steps You Can Take to Improve Your VoIP Security - Copperband Tech
2. VoIP Security: Vulnerablities & Best Practices to Secure Your Phone System | Yeastar
3. Protecting Against Cyber Threats when using VoIP - (totem.tech)
4. What Is IP PBX? How It Works & Benefits of an IP PBX System (nextiva.com)
5. What is an IP PBX? (draytek.co.uk)
6. Roslyakov A.V. IP telephony / A.V. Roslyakov, M.Yu. Samsonova, I.V. Shibaeva - M.: Eco-Trendz, 2003. - 252 p.
7. Sorokovskaya A. A. Information security of the enterprise: new threats and prospects [Electronic resource] / A. A. Sorokovskaya // Visnyk Khmelnyts. National University. – 2010. – No. 2. – Access mode: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf – Head. from the screen (accessed December 25, 2019).
8. Khorev P.B. Methods and means of information protection in computer systems: Textbook. Aid for students. Higher education established / P.B. Khorev - M.: Publishing Center - Academy, 2005. - 8p.
9. The 12 Most Common Types of Cybersecurity Attacks Today (netwrix.com)
10. Sulkin A. PBX Systemsfor IP Telephony / A.Sulkin – McGrawHill Professional, 2002. – 487 p.
11. Asterisk security [Electronic resource] - Access mode: https://habrahabr.ru/post/188440. — Title from the screen (accessed August 6, 2019).
12. Ivanov V.B. Computer, multimedia, IP telephony. Programs and programming / V.B. Ivanov - M.: Major, 2005. - 240 c.
13. Sokolov O.V. Organization and opportunities of IP-telephony networks

[Electronic resource] / O.V. Sokolov, N.V. Slobodska – 2006. – Access mode: http://voipx.ru/cgi-bin/loscont.cgi?ID=08. - Title from the screen (viewed on December 16, 2019).

14. What is: Multifactor Authentication - Microsoft Support
15. Role-Based Access Control (auth0.com)
16. IP Whitelisting in 2023: Everything You Need to Know (goodaccess.com)
17. What Is Data Encryption: Algorithms, Methods and Techniques (simplilearn.com)
18. Bekala K.I. Investigation of vulnerabilities of IP-telephony networks / B.Ya. Kornienko, L.P. Galata // Trends of modern science. - 2018. - p. 39-42.
19. What is an Intrusion Detection System (IDS)? - Check Point Software
20. Asterisk Architecture. [Електронний ре- сурс]. Режим доступу: https://wiki.asterisk.org/ wiki/display/AST/Asterisk+Architecture%2C+The+Big 6 +Picture.
21. В. Гнатюк, "Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі", Безпека інформації, №3 (19), С. 175-180, 2013
22. DBN B.2.5-28-2006 "Engineering equipment houses and buildings Natural and artificial lighting"
23. NPAOP 0.00-1.29-97 "Rules protection from static electricians"
24. DSTU 12.1.005-88 "SSBP. General sanitary and hygienic requirements to air working zones"
25. DSTU B V.2.5-82:2016 "Electrical safety in buildings and buildings Requirements to protective measures from damage electric current"
26. DSTU 8604:2015 "Design and ergonomics. working place for implementation works in position sitting general ergonomic requirements" NAPB A.01.001-2004 "Rules fire station security in Ukraine
27. Prognostication ecological risks with using analysis hierarchs and theories unclear sets: international scientific and practical conference "I-th all-Ukrainian

congress of ecologists": Abstracts of reports. Ukraine, Vinnytsia, October 4-7 2016. – 2016. – P.25.

28. Klap Y. A., Yaremkevich O. S., Chervetsova V. G., Zayarniuk N. L., Novikov V. P., Study of the influence of electromagnetic, permanent magnetic and acoustic fields on human organism // Visnyk Nats. Lviv Polytechnic University. – 2016 – No. 812. – S. 365–372.

29. Modern state of research impact electromagnetic radiations on organism a person [Electronic resource]/[A. P. Black, IN. IN. Nikiforov, D. AND. Rod'kin, V. Yu. Nozhenko] // Engineering and educational technologies in electrical engineering and computer systems: a quarterly scientific and practical journal. – Kremenchuk: KrNU, 2013.

30. Ecology and protection of the natural environment: training. manual for universities / V. S. Dzhigirei. - 6th ed., ed. and additional - K.: Znannia, 2017. - 422 p

31. Struggle with noise on production: Directory / Under ed. AT. I. Yudina – M: Mechanical engineering, 2015. - 297 p