UDC 004.056 DOI: 10.20535/2411-2976.22025.55-62

METHODS FOR ENHANCING SECURITY IN IP TELEPHONY

Serhii O. Fedorov, Rina L. Novogrudskaya

Educational and Research Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. The widespread adoption of IP telephony in corporate and operator networks has led to an increased risk of cyber threats such as fraud, eavesdropping, service interruptions and unauthorised access. Unlike traditional telephony, IP-based systems inherit all the vulnerabilities of IP networks, requiring a systematic, multi-layered approach to security.

Objective. The purpose of the paper is to present and analyse methods for enhancing the security of IP telephony systems. The focus is placed on protecting signalling and media traffic, preventing fraud, ensuring the integrity and confidentiality of communications, and maintaining service availability in the presence of attacks.

Methods. The research involves analysing potential threats for IP telephony systems and various protecting methods such as Encryption for VoIP traffic, Configuration Authentication, Separation of VoIP and Data Traffic, Firewalls and Session Border Controllers (SBCs) which are widely used, Intrusion detection and prevention systems(IDPS), AI and Machine Learning for Real-Time Threat Detection, Blockchain for Security and Authentication which are the future of IP telephony security.

Results. The analysis shows that there is no single universal solution capable of comprehensively protecting IP telephony; instead, effective security is achieved through the combination of multiple complementary mechanisms. For each major threat class, well-established countermeasures and best practices are identified. Current trends in security development for IP telephony systems were analysed.

Conclusions. The conducted review indicates that enhancing security in IP telephony is primarily a question of systematically applying and combining already known methods. The surveyed techniques provide a solid basis for protecting confidentiality, integrity and availability of IP-based voice services. Furthermore, modern technologies like blockchain, artificial intelligence, and machine learning allow experimenting and implementing new methods of IP telephony security enhancement.

Keywords: *IP telephony; VoIP; SIP; RTP; security.*

1. Introduction

Modern IP telephony systems are rapidly evolving under the influence of migration to cloud technologies, distributed offices and the practice of using personal devices, as well as growing demands for data security and privacy. In this context, IP telephony has become the backbone of corporate communications; however, its reliance on open protocols such as SIP, RTP/RTCP and related services — extends the attack surface. Key challenges include preventing eavesdropping and call interception, reducing caller ID spoofing and SPIT/robotic calls, protecting credentials and billing from fraud, and ensuring resilience against DDoS attacks, registration hijacking, and man-in-the-middle attacks.

These problems are exacerbated by architectural changes in the deployment and consumption of voice services. Modern IP telephony platforms are often hosted in public or hybrid clouds, connected to multiple carriers, and accessed through a variety of endpoints, ranging from hardware IP phones to software phones on laptops and mobile devices. Voice and signalling traffic increasingly passes through public networks, VPN tunnels, and overlay architectures designed primarily for data applications rather than real-time media. At the same time, telephony subsystems are tightly integrated with directory services, CRM platforms, and contact centre applications, creating additional trust relationships and interfaces that can be abused if not properly secured. As a result, vulnerabilities in the surrounding IT infrastructure can directly impact the confidentiality, integrity, and availability of voice communications.

In this context, improving IP telephony security is not so much about offering a single universal architecture as it is about understanding the spectrum of relevant threats and the range of available countermeasures. Different organisations face different risk profiles depending on their size, regulatory environment, telephony usage patterns, and integration complexity. Therefore, a systematic review of threat vectors and existing protection methods covering network segmentation, encryption, authentication, fraud prevention, monitoring, and incident response can help practitioners select and combine appropriate methods for their specific scenarios. This work aims to contribute to this understanding by analysing typical security issues in IP telephony and summarising methods that can be applied to mitigate them.

2. IP telephony system architecture

IP telephony, as used, today has some fundamental differences compared to voice transmission in the public switched telephone network (PSTN): In PSTN, signalling takes place in a separate, closed network. With IP telephony, signalling takes place in an open, highly unprotected network (e.g. the Internet).

Traditional telephones are simple devices with limited functionality. IP telephony terminals, on the other hand, are complex devices with their own TCP/IP stack[1]. IP telephony offers mobility: users can change their location and use the same network ID. IP telephony users only need Internet access. In contrast, PSTN offers no mobility. Since PSTN offers no mobility, authentication is not necessary. Anyone with physical access to a wall jack can use that line. Since IP telephony can be used from anywhere on the Internet, additional authentication is necessary.

Extended IP Telephony structure can contain such elements as[2]:

Endpoints: Softphones, IP desk phones, mobile clients.

Call control/IP PBX: Handles dialling plans, features (transfer, park, hunt groups), voicemail, IVR.

SIP trunks: IP connections to carriers that replace PRI/T1 lines.

Session Border Controller (SBC): Security + interop at the edge—topology hiding, NAT traversal assistance, media anchoring, rate limiting, encryption offload, SIP normalisation.

Media services: Conferencing bridges (MCU/SFU), recording servers, transcoders, tone detection.

NAT traversal: STUN/TURN/ICE lets endpoints discover public addresses or relay media when behind firewalls/NAT[3].

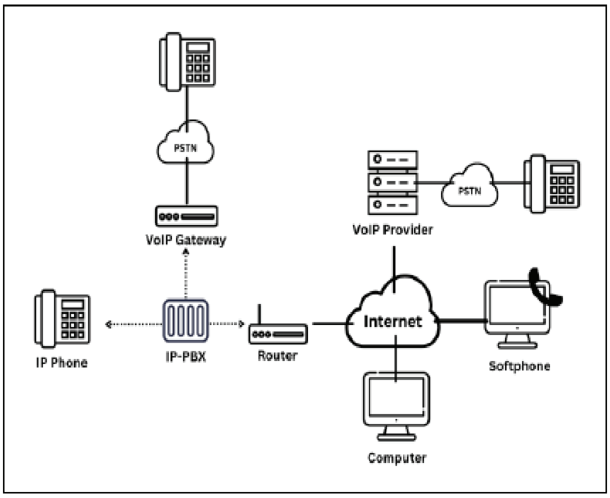

Fig. 1. Typical IP telephony network

Typically, there are two main stages involved in establishing a call when using IP telephony solutions. The primary step requires one party to initiate a call with the other party for mutual confirmation and agreement on certain parameters necessary to establish an effective IP telephony call, including the IP telephony codec to be used. To achieve this, IP telephony solutions use signalling protocols. SIP is the predominant signalling protocol due to its simplicity, adaptability, extensibility, and special features that enhance IP telephony solutions[1]. In the next step, after the call is established, media information begins to be transmitted between the two parties to the call. IP telephony systems use media transmission protocols such as the RTP protocol.

The Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) standard designed to initiate, maintain, and terminate interactive communication sessions between users. These sessions can include voice, video, instant messaging, interactive games, and virtual reality. The Session Initiation Protocol (SIP) was defined by the IETF as a standard for signalling and control in multimedia communications over IP[4].

SIP uses a small number of text messages exchanged between SIP entities, i.e. SIP User Agents in user terminals. During message exchange, messages may pass through network objects such as proxy servers or redirection servers, which are used for support, for example, for address resolution, call routing to other objects, etc. SIP only defines session initiation; all other parts of the session are covered by other protocols. SIP messages are usually divided[5] into two types: requests and responses.

Table 1. Typical SIP requests

SIP Request	
INVITE	Session initiation
BYE	Session termination
OPTIONS	Discover SIP capabilities and codecs supported by a UA or server
REGISTER	Register a SIP user's current location
ACK	Acknowledges the final response to an INVITE
CANCEL	Cancel a pending INVITE request
NOTIFY	Conveys state change notifications not tied to a specific session
REFER	Transfers calls and references external resources

Table 2. Typical SIP responses

SIP Response	
100 Trying	Indicates that the recipient has received the INVITE request and is processing it.
180 Ringing	The called party is being alerted (ringing).
200 OK	Session established.
401 Unauthorized	Unauthorized — indicates authentication is required (commonly in response to REGISTER).
403 Forbidden	The server understood the request but refuses to fulfil it.
407 Proxy Authentication Required	The request requires user authentication, issued by proxy servers.
408 Request Timeout	No response received within the time allowed.
503 Service Unavailable	The server is unavailable; the request cannot be processed now.

The flexibility and rich feature set of SIP-based IP telephony, compared to traditional telephone networks, come with additional security risks. SIP-based IP telephony systems are vulnerable to both general Internet attacks and attacks specific to SIP. Since the development of SIP was primarily focused on expanding functionality and compatibility, there is much room for improvement in terms of SIP security[5].

After the signalling phase is complete and the call is established, the media transfer function is performed. This function is responsible for sending the actual voice or multimedia data between the devices involved in the call. Media transmission depends on protocols such as RTP, which handles the packetisation, sequencing, and timestamping of media data. It cooperates with real-time protocols to transmit data over networks.

3. Overview of security concerns in IP telephony

3.1 Eavesdropping and call interception

Eavesdropping remains one of the most serious security issues in IP telephony systems[6]. Attackers exploit unencrypted SIP (Session Initiation Protocol) and RTP (Real-Time Transport Protocol) traffic to intercept confidential voice data. Traditional telephony had the advantage of dedicated transmission lines, which reduced the risk of interception. However, VoIP packets are transmitted over shared networks, making them vulnerable to packet sniffing attacks. Once they have access to VoIP packets, attackers can reconstruct conversations, exposing confidential corporate communications, financial transactions, and users' personal data.

3.2 DoS and DDoS attacks

DoS and DDoS attacks have become significant threats to IP Telephony networks. During a DoS attack, attackers flood the server with an excessive number of requests, consuming network resources and making services unavailable[14]. DDoS attacks exacerbate this effect by distributing the attack across multiple compromised devices, making mitigation more difficult[7]. Attackers often target SIP servers by sending malformed packets that exploit protocol vulnerabilities. This disrupts call processing, causing delays, dropped calls, and degraded voice quality. The financial and operational consequences of such attacks can be severe, especially for businesses that rely on VoIP for customer interactions and internal communications.

3.3 Man-in-the-middle (MitM) attacks

A man-in-the-middle (MitM) attack occurs when an attacker intercepts and alters VoIP traffic between two communicating parties. Attackers exploit vulnerabilities in SIP signalling and RTP transmission to manipulate call data, record conversations, or redirect calls to unauthorised endpoints. Weak SIP authentication and unencrypted RTP streams make IP Telephony systems highly vulnerable to MitM attacks[8]. In a corporate environment, these attacks can lead to corporate espionage, identity theft, and financial fraud.

3.3.1 Typical SIP attacks:

Modification of SIP messages

SIP messages do not have a built-in integrity mechanism. By performing one of the man-in-the-middle attacks, an attacker can intercept and modify a SIP message by changing some or all of its attributes[5].

This may include the person being called in the session initiation message, giving the victim the impression that they are calling one person while the system connects them to another. By modifying SIP messages, an attacker can impersonate a subscriber or redirect a call to an unwanted person.

SIP Cancel/Bye Attack

An attacker can create a SIP message with a Cancel or Bye command in its payload and send it to the end node (telephone) to terminate the current call. If the attacker sends a constant stream of these packets to the phone, it will be unable to make or receive calls. This can be spread to multiple phones, causing the entire system to malfunction[9].

3.3.2 Typical RTP attacks:

RTP Payload

The RTP protocol transmits the actual encoded voice message between two subscribers. It is a simple extension of the UDP protocol that adds sequence information. Using a man-in-the-middle attack to gain access to the RTP media stream between two nodes, an attacker can verify or modify the payload of the message[10]. Verification in this case turns into eavesdropping on the conversation. If an attacker can modify the payload of the messages, they can either inject noise or their own message into the packet. This will either degrade or make the conversation between the call parties impossible in the case of noise, or potentially change the meaning of the conversation.

RTP Tampering

By manipulating the sequence number and timestamp fields in the RTP packet header, packets can be either reordered or rendered unusable[11]. This attack can either make the conversation incomprehensible or, in some implementations of the protocol stack, actually cause the node receiving the packets to crash, thus taking the node offline until the software is rebooted.

3.4 Spoofing and manipulating caller ID

Caller ID spoofing is a deceptive technique in which attackers manipulate SIP headers to impersonate legitimate users[12]. This tactic is commonly used in phishing schemes, where fraudulent callers pose as trusted contacts to trick victims into divulging confidential information. Spoofing attacks undermine trust in VoIP communications and increase the risk of social engineering attacks.

3.5. Toll Fraud

Toll Fraud is an attempt by a malicious party to obtain money by making a large number of calls to a telephone number that incurs high charges. An example of this is when a telephone system makes numerous calls to a ‘900’ number, resulting in high costs for the owner of the telephone system. These costs are then shared between the owner of the ‘900’ number and the attacker[9].

Another common attack is impersonating another telephone to obtain free long-distance calls[8]. The attacker spoofs the system into thinking that his telephone is another legitimate telephone. The attacker then uses his ‘cloned’ identity to make numerous calls. The cost of the calls is then passed on to the victim.

3.6 Redirection of call

One of the goals in developing the IP Telephony system was flexibility and a rich set of features. The ability to forward calls from one phone number to the location of the owner is an advanced feature that provides subscribers with an easy way to find the person they are looking for by dialling a single phone number.

This advanced feature becomes a potential threat if an attacker compromises the call forwarding feature. An attacker can forward the victim's phone number to a location of their choice, potentially allowing them to impersonate the victim by forwarding their calls to the attacker's phone[7].

4. Methods for improving security

4.1 Encryption for VoIP traffic.

Encryption is a fundamental security measure that protects IP telephony communications from unauthorised interception[12]. Since VoIP traffic is transmitted in the form of data packets over the Internet, unencrypted voice streams are vulnerable to eavesdropping and packet sniffing attacks. Encrypting VoIP traffic ensures that voice data remains confidential, even if it is intercepted by an unauthorised party.

Secure Real-Time Transport Protocol (SRTP) is widely used to encrypt RTP packets, preventing attackers from capturing and reconstructing voice conversations[6]. SRTP uses Advanced Encryption Standard (AES) encryption and message authentication codes (MAC) to protect the integrity and confidentiality of VoIP packets.

In addition, the Transport Layer Security (TLS) protocol provides encryption for SIP signalling, protecting call setup and authentication processes. TLS ensures that SIP messages cannot be intercepted or altered by malicious parties. Despite the effectiveness of encryption, issues such as increased latency and processing overhead must be addressed. Organisations implementing VoIP encryption must optimise network performance to balance security with call quality.

4.2. Configuration Authentication

VoIP phones require basic configuration information to access the VoIP system. Configuring phones creates a classic bootstrapping problem, where obtaining configuration information from an untrusted source can lead to further problems. Pre-configuring phones with the public key of various configuration servers during production provides a possible mechanism for authenticating the configuration server.

An alternative would be for the phone installer to configure the phone with a public key or shared secret key for the configuration server. This can be automated by providing the installer with a hardware key or device that will be connected to the phone and provide a quick and accurate way to copy the public key to the phone[9].

To obtain the phone configuration, the phone will make a DHCP request. In the response from the DHCP server, the phone receives both its IP address and the IP address of its configuration server. The phone will then establish a connection to the configuration server using TLS. During TLS authentication, the authenticity of the server will be established using the public key contained in the phone device and the private key contained on the configuration server[7]. If these two keys do not match, the phone will not download configuration information from the server. If the key pair matches, the configuration information will be downloaded to the phone using FTP over a secure TLS transport.

4.3 Separation of VoIP and Data Traffic

Similar to authentication, separating voice and data traffic to different networks is a key factor in overall security. Traffic separation can prevent a number of attacks, as PCs and workstations cannot be used by attackers as an easy entry point into the VoIP network. Due to the cost of operating two separate physical networks, this separation is achieved using VLAN technology.

Network switches implement VLANs, allowing only routing between devices in the same VLAN, as configured by the network administrator. VoIP phones that implement a second LAN port for PC data connectivity must implement VLAN technology (802.1q) so that PCs connected to the phone are placed on the data LAN rather than the voice LAN.

4.4 Firewalls and Session Border Controllers (SBCs)

Firewalls and session border controllers (SBCs) play an important role in securing IP telephony networks by filtering malicious traffic and enforcing security policies. Unlike traditional firewalls, VoIP-compatible firewalls are made to inspect SIP and RTP traffic, block unauthorised requests, and prevent DoS and DDoS attacks[14]. These firewalls use deep packet inspection (DPI) to analyse VoIP packets, detect anomalies and potential threats for the system security. SBCs enhance VoIP security by acting as intermediaries between VoIP endpoints, inspecting and encrypting traffic before it reaches its destination. SBCs help mitigate man-in-the-middle (MITM) attacks, protect SIP signalling, and provide traffic management features to prevent congestion and issues with latency.

4.5 Intrusion detection and prevention systems(IDPS) for IP telephony.

IP telephony networks require specialised intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and mitigate cyber threats. Traditional IDS solutions are ineffective against VoIP-specific attacks such as SIP flooding, RTP injection, and protocol obfuscation attacks[10]. Advanced IDS/IPS solutions that support VoIP can:

- Monitor SIP and RTP traffic for unusual behaviour.
- Detect unauthorised call attempts and fraudulent transactions.
- Block DoS attack attempts in real time by applying traffic filtering rules.

IDPS solutions also integrate honeypots, which act as decoy VoIP servers to lure attackers and gather information about new threats. Through proactive monitoring of traffic, IDPS enhances security by preventing unauthorised access and mitigating attacks before they escalate[15].

4.6 AI and Machine Learning for Real-Time Threat Detection

Artificial intelligence (AI) and machine learning (ML) are changing the world of IP telephony security by enabling real-time threat detection and response[10]. Traditional security systems rely on signature-based detection, which struggles to detect zero-day attacks and evolving VoIP fraud techniques.

AI-based security systems analyse traffic patterns, call metadata, and user behaviour to detect anomalies[13]. Behavioural analytics based on machine learning models can detect fraudulent call patterns, unauthorised account takeovers, and suspicious VoIP login attempts. AI-based threat intelligence also improves DoS mitigation by enabling VoIP firewalls to dynamically adjust traffic filtering rules based on attack behaviour.

4.7 Blockchain for Security and Authentication

Blockchain technology offers promising advances in IP telephony security by providing decentralised authentication mechanisms. Traditional authentication relies on centralised credential databases, which are vulnerable to breaches. Blockchain-based identity verification allows users to authenticate user sessions without relying on a single point of failure[13]. Smart contracts can also be used to enforce security policies, ensuring that only authenticated users can initiate VoIP calls. By decentralising authentication, blockchain enhances the integrity and security of VoIP communications, reducing the risk of credential theft and impersonation attacks.

5. Conclusion

IP telephony has revolutionised modern communications by enabling cost-effective and scalable voice transmission over IP networks. However, its reliance on open Internet protocols makes it vulnerable to a wide range of cyber threats, including eavesdropping, denial-of-service (DoS) attacks, spoofing, Toll Fraud and MiTM attacks. These threats underscore the need for robust IP telephony security mechanisms to ensure the confidentiality, integrity, and availability of voice communications. This study examines key IP telephony security threats, ranging from unauthorised call interception and SIP vulnerabilities to large-scale DoS attacks. It highlights the importance of encryption, authentication, intrusion detection and prevention systems (IDPS), and firewalls as fundamental defence mechanisms for protecting VoIP networks.

Given the constant evolution of cyber threats, IP telephony security strategies must remain dynamic to counter new attack vectors.

Future research should focus on integrating AI-driven behavioural analytics with real-time traffic and the whole IP telephony system monitoring produced by modern intrusion detection and prevention systems, developing scalable blockchain authentication frameworks, and advancing brand-new encryption methods. These innovations will be critical in strengthening IP telephony security as cybercriminals continue to develop sophisticated attack techniques.

References

1. Muhammad Yeasir Arafat, Feroz Ahmed & M Abdus Sobhan(2013), SIP Security in IP Telephony, Conference: *Proc. of ElasticWorld 2013*, pp. 1-11. Retrieved from: https://www.researchgate.net/publication/291833783_SIP_Security_in_IP_Telephony

2. Mosleh M. Abualhaj, Sumaya N. Al-Khatib, Qusai Y. Shambour, Ahmad Adel Abu-Shareha(2021), An Efficient Method to Enhance IP Telephony Performance in IPV6 Networks, CYBERNETICS AND INFORMATION TECHNOLOGIES Volume 21, No 4, pp.145-157. Retrieved from: https://www.researchgate.net/publication/356946930_An_Efficient_Method_to_Enhance_IP_Telephony_Performance_in_IPV6_Networks

3. Martin Klimo, Tatiana Kováčiková, Pavol Segeč(2004), SELECTED ISSUES OF IP TELEPHONY, Communications - Scientific letters of the University of Zilina 6(4), pp. 63-70. Retrieved from: https://www.researchgate.net/publication/291432188_Selected_issues_of_IP_telephony

4. IETF Network Working Group. 2016. SIP: Session Initiation Protocol. Retrieved September 21, 2016 from https://www.ietf.org/rfc/rfc3261.txt

5. Fedorov S., Novohrudska R.(2025), OVERVIEW OF SIP BASED ATTACKS IN VOIP NETWORKS, International Scientific Conference "Modern Challenges in Telecommunications 2025" section 4, pp. 231-234. Retrieved from: https://conferenc.its.kpi.ua/2025

6. Zainb Asimiyu(2024), VoIP Security in Practice: Implementing Robust Defense Mechanisms for Safe Communication, pp. 1-19. Retrieved from: https://www.researchgate.net/publication/388614637_VoIP_Security_in_Practice_Implementing_Robust_Defense_Mechanisms_for_Safe_Communication

7. David Butcher, Xiangyang Li, and Jinhua Guo(2007), Security Challenge and Defense in VoIP Infrastructures, IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews) 37(6), pp. 1152 – 1162. Retrieved from: https://www.researchgate.net/publication/3421877_Security_Challenge_and_Defense_in_VoIP_Infrastructures

8. Perigo, L., Gandotra, R., Gedia, D., Hussain, M., & Others. (2020), VoIP security: A performance and cost-benefit analysis, Information Technology in Industry. Retrieved from: https://it-in-industry.org/index.php/itii

9. Ramly, A. M., Ng, Z. W., Khamayseh, Y., Kwa, C. S. C., & Neo, T. K. (2024), Review and enhancement of VoIP security: Identifying vulnerabilities and proposing integrated solutions, Journal of Telecommunications and the Digital Economy, 12(4), pp. 109-136. Retrieved from: https://jtde.telsoc.org/index.php/jtde

10. Dabbebi, O., & Festor, O. (2018). Advanced threat detection in Asterisk PBX systems, VoIP Systems Journal, 21(3), pp. 121-134.

11. Ramly, A. M., Ng, Z. W., & Khamayseh, Y. (2024). Review and enhancement of VoIP security: Identifying vulnerabilities and proposing integrated solutions, Digital Information and Security Journal, pp. 45-54. Retrieved from: https://search.informit.org/selectDatabases?redirectUri=

12. Jahanirad, M., Yahya, A. L. N., & Noor, R. M. (2011). Security measures for VoIP application: A state of the art review. Scientific Research and Essays, pp. 20-34. Retrieved from: https://academicjournals.org/

13. Melih Tas, Selcuk Baktir(2024), Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks, in *IEEE Access*, vol. 12, pp. 60123-60137. Retrieved from: https://ieeexplore.ieee.org/document/10508353

14. I. M. Tas, B. G. Unsalver, and S. Baktir(2020), A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism, IEEE Access, vol. 8, pp. 112574–112584. Retrieved from: https://ieeexplore.ieee.org/document/9114982

15. M. A. Ramírez-Reyna, F. A. Cruz-Pérez, S. Lirio Castellanos-López and G. Hernández-Valdez(2024), "Comparison of Analysis Methods for the Joint Connection-Level and Packet-Level Performance Evaluation of VoIP Traffic Networks," in IEEE Access, vol. 12, pp. 163349-163366. Retrieved from: https://ieeexplore.ieee.org/document/10742327

Федоров С.О., Новогрудська Р.Л.

Методи підвищення безпеки в IP телефонії

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, м. Київ, Україна

Проблематика. Широке впровадження IP-телефонії в корпоративних та операторських мережах призвело до зростання ризику кіберзагроз, таких як шахрайство, підслуховування, перебої в обслуговуванні та несанкціонований доступ. На відміну від традиційної телефонії, IP-системи успадковують всі вразливості IP-мереж, що вимагає системного, багаторівневого підходу до забезпечення безпеки.

Мета дослідження. Метою статті є представлення та аналіз методів підвищення безпеки систем IP-телефонії. Основна увага приділяється захисту сигналізації та медіа-трафіку, запобіганню шахрайству, забезпеченню цілісності та конфіденційності комунікацій, а також підтримці доступності сервісів в умовах атак.

Методика реалізації. Дослідження включає аналіз потенційних загроз для систем IP-телефонії та різних методів захисту, таких як шифрування VoIP-трафіку, аутентифікація конфігурації, розділення VoIP-трафіку та трафіку даних, брандмауери та контролери меж сеансів (SBC), які уже широко використовуються, а також системи виявлення та запобігання вторгнень (IDPS), штучний інтелект та машинне навчання для виявлення загроз у реальному часі, блокчейн для безпеки та аутентифікації, які є майбутнім безпеки IP-телефонії.

Результати дослідження. Аналіз показує, що не існує єдиного універсального рішення, здатного комплексно захистити IP-телефонію, натомість ефективний захист досягається шляхом поєднання декількох взаємодоповнюючих механізмів. Для кожного з основних класів загроз визначено контрзаходи та найкращі методи захисту. Проаналізовано сучасні напрямки розвитку безпеки для систем IP телефонії.

Висновки. Проведений огляд свідчить про те, що підвищення безпеки в IP-телефонії - це насамперед питання системного застосування та комбінування вже відомих методів. Розглянуті методи забезпечують надійну основу для захисту конфіденційності, цілісності та доступності голосових послуг на основі IP-телефонії. Крім того, сучасні технології, такі як блокчейн, штучний інтелект і машинне навчання, дозволяють експериментувати і впроваджувати нові методи підвищення безпеки IP-телефонії.

***Ключові слова**: IP-телефонія; VoIP; SIP; RTP; безпека.*

Received by the Editorial Office
October 18, 2025

Accepted for publication
December 2, 2025