№ 4(58) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.72:621.395:35.07
https://doi.org/10.52058/2786-6025-2026-4(58)-2857-2871

Борзов Юрій Олексійович кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівський державний університет безпеки життєдіяльності, м. Львів, https://orcid.org/0000-0002-0604-0498

Пилипенко Володимир Миколайович старший викладач кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності, м. Львів, https://orcid.org/0009-0008-5957-4822

Довбняк Віра Йосипівна викладач кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності, м. Львів, https://orcid.org/0009-0008-7971-9873

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ МЕРЕЖ IP-ТЕЛЕФОНІЇ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

Анотація. Стаття має аналітичний характер і досліджує актуальну тему вдосконалення та перспективи розвитку інформаційно-комунікаційних мереж в органах державної влади із застосуванням IP-телефонії. Сьогодні державний апарат працює в умовах жорсткого дефіциту часу на прийняття рішень, тоді як старі телефонні лінії фізично не в стані витримувати таких навантажень. Їхня архітектура не дозволяє швидко масштабувати інформаційно-комунікаційну мережу чи повноцінно забезпечувати обмін мультимедійними даними. Перехід державних установ на сучасні хмарні сервіси та апаратні VoIP-рішення ускладнюється специфічними жорсткими вимогами до захисту інформації, відмовостійкості (живучості) мереж в умовах можливих руйнувань критичної інфраструктури, а також необхідністю безшовної інтеграції новітніх систем із наявними відомчими лініями зв'язку.

Сучасна IP-телефонія є потужною комплексною системою у сфері забезпечення сталого зв'язку, яка інтегрує методи цифрової обробки сигналів, передачу мови, даних і відеоінформації, дозволяючи об'єднувати територіально розподілені підрозділи в єдиний захищений інформаційний простір. Використання шлюзів IP-телефонії та сучасних програмно-апаратних комплексів (SoftPBX) дозволяє ефективно поєднати новітні цифрові технології з

ISSN 2786-6025 Online

існуючими класичними телефонними мережами. В роботі проведено ґрунтовний аналіз принципів функціонування відомчих систем зв'язку та систематизовано ключові показники, які впливають на інтегральну оцінку їхньої ефективності. Доведено, що на відміну від корпоративного (комерційного) сектору, для інформаційних мереж органів державної влади першочергове значення мають не економічні показники, а критерії відмовостійкості, безпеки передачі даних (захист від несанкціонованого втручання, шифрування сигнального та медіатрафіку) та якості обслуговування (QoS – пріоритезація критичного трафіку, мінімізація затримок і втрат пакетів).

Основні результати полягають у систематизації та адаптації критеріїв оцінки ефективності відомчих VoIP-мереж з урахуванням специфіки функціонування органів державної влади в умовах воєнного стану та надзвичайних ситуацій, а також в обґрунтуванні концептуальної моделі конвергенції базових послуг IP-телефонії із системами уніфікованих комунікацій (Unified Communications). Окреслено перспективи подальшого розвитку систем, що передбачають створення децентралізованих автономних вузлів зв’язку на базі мобільних пунктів управління та підвищення загальної структурної надійності відомчого комунікаційного простору.

Ключові слова: інформаційні технології, автоматизовані системи управління, IP телефонія, мережеві технології.

Borzov Yurii Oleksiiovych PhD in Engineering (Candidate of Technical Sciences), Associate Professor, Associate Professor of the Department of Information Technologies and Electronic Communication Systems, Lviv State University of Life Safety, Lviv, https://orcid.org/0000-0002-0604-0498

Pylypenko Volodymyr Mykolaiovych senior lecturer at the Department of Information Technology and Electronic Communications Systems, Lviv State University of Life Safety, Lviv, https://orcid.org/0009-0008-5957-4822

Dovbniak Vira Yosypivna Lecturer of the Department of Information Technologies and Electronic Communication Systems, Lviv State University of Life Safety, Lviv, https://orcid.org/0009-0008-7971-9873

CURRENT STATE AND DEVELOPMENT PROSPECTS OF IP TELEPHONY INFORMATION NETWORKS IN PUBLIC AUTHORITIES

Abstarct. The article is analytical in nature and investigates the highly relevant topic of the improvement and development prospects of information and communication networks in public authorities using IP telephony. Today, the state

ISSN 2786-6025 Online

apparatus operates under a severe time deficit for decision-making, while legacy telephone lines are physically incapable of handling such loads. Their architecture does not allow for rapid scaling of the information and communication network or fully ensuring the exchange of multimedia data. The transition of state institutions to modern cloud services and hardware VoIP solutions is complicated by specific stringent requirements for information protection, network fault tolerance (survivability) under conditions of potential destruction of critical infrastructure, as well as the need for seamless integration of cutting-edge systems with existing departmental communication lines.

Modern IP telephony is a powerful comprehensive system in the field of ensuring reliable communication, which integrates methods of digital signal processing and the transmission of voice, data, and video information, allowing geographically distributed units to be united into a single secure information space. The use of IP telephony gateways and modern software-hardware complexes (SoftPBX) enables the effective integration of cutting-edge digital technologies with existing classic telephone networks.

The paper provides a thorough analysis of the operational principles of departmental communication systems and systematizes the key indicators that affect the integral assessment of their effectiveness. It is proven that, unlike the corporate (commercial) sector, for the information networks of public authorities, primary importance lies not in economic indicators, but in criteria of fault tolerance, data transmission security (protection against unauthorized access, encryption of signaling and media traffic), and Quality of Service (QoS – prioritization of critical traffic, minimization of delays and packet loss).

The main results consist in the systematization and adaptation of criteria for evaluating the effectiveness of departmental VoIP networks, taking into account the specifics of the functioning of public authorities under martial law and emergency situations, as well as in the substantiation of a conceptual model for the convergence of basic IP telephony services with Unified Communications systems. Prospects for further system development are outlined, involving the creation of decentralized autonomous communication nodes based on mobile control posts and the enhancement of the overall structural reliability of the departmental communication space.

Keywords: information technologies, automated control systems, IP telephony, network technologies.

Постановка проблеми. В умовах стрімкої цифровізації та зростаючих вимог до трансформації і робочих процесів, працівники державного сектору все частіше потребують більшої гнучкості та інструментів, що забезпечують надійний віддалений зв'язок. Для багатьох установ це означає необхідність

ISSN 2786-6025 Online

масштабнішого використання уніфікованих комунікацій або консолідації існуючих розрізнених інструментів зв'язку в єдину платформу.

Існуюча експлуатація традиційних аналогових АТС в органах державної влади супроводжується низкою критичних недоліків, серед яких низька якість звуку, великі затримки маршрутизації та відсутність гнучкості масштабування. Такі застарілі системи вимагають утримання надлишкових ліній зв'язку та не здатні забезпечити комплексне управління процесами, що безпосередньо знижує оперативність координації між відомствами. Досвід модернізації інформаційно-комунікаційних мереж доводить, що впровадження новітніх рішень уніфікованих комунікацій є критично необхідним кроком для державного сектору. Це забезпечує конвергенцію послуг зв'язку, усуває проблеми дублювання інфраструктури та створює захищений єдиний інформаційний простір для взаємодії відомств.

Для вирішення цих проблем здійснюється перехід до сучасних технічно обґрунтованих рішень мультисервісних комунікаційних мереж. Однією з базових технологій таких мереж є IP-телефонія, яка інтегрує методи та засоби цифрової обробки сигналів. Ця технологія дозволяє використовувати Інтернет або відомчі локальні IP-мережі для ведення міжміських розмов та передачі текстових повідомлень у режимі реального часу. Завдяки використанню спеціального обладнання — шлюзів IP-телефонії — абоненти, які розділені тисячами кілометрів, можуть спілкуватися між собою, при цьому оплачується лише час підключення до самої IP-мережі, що робить технологію вкрай вигідною для розгалуженої мережі державних органів. Сучасним стандартом для комплексного управління процесами є перехід від базової телефонії до систем Уніфікованих комунікацій (Unified Communications, UC) — комунікаційних платформ на основі IP, які поєднують передачу голосу, відео, даних та забезпечують мобільність співробітників. Системний підхід до розбудови таких мереж передбачає створення єдиної інтелектуальної, безпечної та відмовостійкої інфраструктури.

Впровадження програмно-апаратних систем обробки викликів (наприклад, серверів рівня Cisco Unified Communications Manager) дозволяє маршрутизувати виклики з високим рівнем безпеки. Такий підхід не лише знижує експлуатаційні витрати та підвищує продуктивність персоналу, але й забезпечує високий рівень захисту інформації, що є критично важливим для органів державної влади.

Аналіз останніх досліджень і публікації за тематикою дозволив встановити, що технології пакетної комутації та мультисервісних мереж активно досліджуються та впроваджуються при вирішенні проблем модернізації застарілої комунікаційної інфраструктури. У роботах [1-3] обґрунтовано принципи розбудови інформаційно-телекомунікаційних систем для державних

ISSN 2786-6025 Online

структур із використанням віртуальних приватних мереж (VPN) та маршрутизаторів для створення відмовостійкої топології. Такі підходи суттєво підвищують надійність та безперебійність управлінських процесів і міжвідомчого інформаційного обміну.

При цьому запропоновані поточні дослідження недостатньо враховують заходи, які орієнтовані на ізольовані відомчі сегменти мереж і не дають змоги повною мірою врахувати специфіку гнучкого масштабування комунікацій в органах державної влади загального профілю.

У [4-6] автори пропонують комплексні рішення щодо переходу від застарілих АТС до сучасних платформ уніфікованих комунікацій (UC), що дає змогу консолідувати програмні застосунки, оптимізувати адміністративні процеси та знизити експлуатаційні витрати. Запропоновані у цих роботах моделі часто спираються на критерії комерційної ефективності хмарних рішень і не завжди можуть бути повноцінно використані у державному секторі через жорсткі нормативні обмеження щодо захисту інформації (на що вказують вимоги стандартів [7-9]).

Роботи [10-13] присвячені розгляду різноманітних аспектів інформаційної безпеки систем IP-телефонії, зокрема виявленню та захисту від специфічних кібератак (наприклад, DDoS-атак на SIP-сервери) та впровадженню протоколів криптографічного захисту для збереження конфіденційності. Разом з тим, зважаючи на складність гетерогенних (змішаних) мереж, публікації досить часто оминають проблематику балансування між вимогами посиленого шифрування та забезпеченням високої якості обслуговування (QoS) [14-16] під час безшовної інтеграції новітніх VoIP-систем із наявними традиційними мережами - телекомунікаційними мережами загального користування (ТМЗК) за допомогою шлюзів.

Це підтверджує необхідність подальшої роботи у цій сфері з метою формування комплексної методології розгортання захищених та інтегрованих комунікаційних мереж для органів державної влади.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

– проаналізувати перспективи застосування технологій пакетної комутації та платформ уніфікованих комунікацій для модернізації застарілої телекомунікаційної інфраструктури державного сектору;

– розробити концептуальну архітектуру інтегрованої комунікаційної мережі з використанням VoIP-шлюзів та SIP-серверів для забезпечення безшовної взаємодії між різними відомствами;

– обґрунтувати основні принципи інформаційної безпеки та управління якістю обслуговування (QoS) запропонованої системи, що забезпечують її захищеність від специфічних кіберзагроз (зокрема DDoS-атак та несанкціонованого перехоплення) і гарантують конфіденційність управлінського зв'язку.

№ 4(58) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online

Таблиця 1

Порівняння існуючих архітектур функціонування IP-телефонії

Автор, рік	**Основний напрям дослідження**	**Архітектурний підхід**	**Забезпечення безпеки**	**Підхід до QoS**	**Обмеження**	**Релевантність для органів державної влади**
Stiawan et al., 2021	Безпека VoIP	Централізована на SIP-архітектура	TLS, SRTP	Базова пріоритизація трафіку	Обмежена масштабованість	Середня
Rafiq et al., 2022	SDN у VoIP мережах	SDN-керована мережа	Контроль політик доступу	Динамічне керування потоками	Складність впровадження	Висока
Akter et al., 2023	QoS у мультисервісних мережах	IP-конвергентна інфраструктура	Частково розглянуто	DiffServ, DSCP EF	Недостатня увага безпеці	Середня
Benzaid et al., 2024	Захист сигналізації SIP	Розподілена архітектура	IDS/IPS, шифрування	Не є центральним аспектом	Відсутність інтеграції UC	Висока
Chen et al., 2024	Unified Communications	UC-платформи	Комплексна автентифікація	Адаптивне QoS	Орієнтація на корпоративний сектор	Часткова
Узагальнений підхід	Інтегрована модернізація держмереж	Гібридна UC-архітектура	TLS/SRTP + VPN + сегментація	DiffServ + пріоритизація службового трафіку	Потребує стандартизації впровадження	**Висока**

Проведене порівняння в таблиці 1 демонструє, що існуючі дослідження здебільшого розглядають окремі аспекти функціонування IP-телефонії. Водночас комплексна інтеграція вимог безпеки, якості обслуговування та відмовостійкості державних інформаційно-комунікаційних систем залишається недостатньо дослідженою.

Мета статті - комплексне дослідження сучасного стану, принципів організації та показників ефективності функціонування систем IP-телефонії у державному секторі, а також обґрунтування перспективних моделей їхнього подальшого розвитку.

Виклад основного матеріалу. Незважаючи на значну кількість досліджень у сфері мультисервісних комунікаційних мереж та IP-телефонії, низка питань залишається недостатньо опрацьованою. Зокрема, існуючі підходи переважно орієнтовані на корпоративний сектор і не повною мірою враховують специфічні вимоги щодо відмовостійкості, інформаційної безпеки та функціонування в умовах кризових ситуацій інформаційно-комунікаційних

ISSN 2786-6025 Online

систем органів державної влади. Крім того, недостатньо дослідженим залишається баланс між криптографічним захистом VoIP-трафіку та забезпеченням гарантованої якості обслуговування в гетерогенних мережах.

Для досягнення поставленої мети та вирішення визначених завдань у статті застосовано комплекс загальнонаукових та спеціальних методів. Метод **системного аналізу** використано для оцінки сучасного стану та виявлення критичних недоліків наявної електронної комунікаційної інфраструктури органів державної влади. За допомогою **порівняльного аналізу** здійснено зіставлення функціональних можливостей традиційних ізольованих систем зв'язку (АТС) із сучасними рішеннями IP-телефонії та мультисервісними платформами уніфікованих комунікацій (UC) (див. табл. 2).

Таблиця 2

Порівняльний аналіз традиційних та сучасних мультисервісних комунікаційних мереж в державному секторі

Характеристика / Критерій	**Традиційні відомчі мережі (ТМЗК та ізольовані АТС)**	**Інтегровані мультисервісні мережі (платформи UC та IP-телефонія)**
Базова архітектура та комутація	Комутація каналів, жорстка прив'язка до фізичних ліній (мідний кабель).	Комутація пакетів (IP), логічна маршрутизація незалежно від середовища передачі.
Апаратна залежність	Висока (vendor lock-in). Обладнання та плати розширення від одного виробника.	Низька. Використання відкритих протоколів (SIP) та універсальних серверів (Softswitch).
Консолідація сервісів	Відсутня. Голос, відео та повідомлення працюють у різних, не пов'язаних системах.	Висока. Єдине середовище (голос, відеоконференції, захищений чат, статус присутності).
Масштабованість	Обмежена ємністю апаратної АТС (кількістю портів FXS/FXO).	Практично необмежена (визначається лише обчислювальною потужністю серверів та пропускною здатністю мережі).
Інформаційна безпека	Фізична ізоляція ліній. Складно реалізувати наскрізне шифрування між відомствами.	Захист на рівні мережі (VPN, IPSec) та наскрізне криптографічне шифрування трафіку (TLS/SRTP).
Управління якістю (QoS)	Гарантована якість завдяки виділеному фізичному каналу на час розмови.	Потребує складного налаштування мережевого обладнання (пріоритезація трафіку)

ISSN 2786-6025 Online

Методи синтезу та узагальнення застосовано під час опрацювання міжнародних наукових джерел, галузевих стандартів та актуальної нормативно-правової бази (зокрема Закону України «Про електронні комунікації») [7] з метою врахування правових обмежень та формування концептуальних вимог до захищеності, надійності й масштабованості електронних комунікаційних мереж.

Крім того, під час розроблення концептуальної архітектури інтегрованої мережі та механізмів міжвідомчої взаємодії використано елементи **об'єктного моделювання** електронних комунікаційних систем.

Аналіз поточного стану електронної комунікаційної інфраструктури органів державної влади свідчить про наявність значної кількості успадкованих (legacy) систем. З огляду на масштаби державного апарату та критичність безперервного управлінського процесу, миттєва відмова від традиційних телефонних мереж загального користування (ТМЗК) та наявних ізольованих відомчих АТС є неможливою.

Відповідно, найбільш технічно обґрунтованим шляхом модернізації є побудова гетерогенної (змішаної) електронної комунікаційної мережі, яка забезпечує поступову міграцію до технологій пакетної комутації [5, 6].

У межах запропонованої концепції ключовим апаратним елементом інтеграції на перехідному етапі виступають спеціалізовані VoIP-шлюзи. Головна функція шлюзу полягає в апаратній трансляції протоколів сигналізації та конвертації медіатрафіку між середовищем із комутацією каналів (цифрові потоки, аналогові лінії FXO/FXS застарілих АТС) та сучасним середовищем із комутацією пакетів [4, 6].

Впровадження VoIP-шлюзів на межі відомчих сегментів вирішує одразу два стратегічні завдання: по-перше, дозволяє зберегти існуючий номерний план (внутрішню нумерацію співробітників міністерств та відомств), а по-друге, забезпечує безшовний голосовий зв'язок між вже модернізованими (IP) та ще не модернізованими (аналоговими) підрозділами. Як наочно продемонстровано на рис. 1, побудова такої архітектури дозволяє централізовано керувати реєстрацією та маршрутизацією як локальних (LAN 1, LAN 2), так і віддалених SIP-клієнтів через єдиний SIP-сервер, тоді як VoIP-шлюз бере на себе функцію прозорої взаємодії з традиційними мережами PSTN/ISDN.

Наступним рівнем архітектури є розбудова ядра управління викликами, яке базується на використанні програмних комутаторів (Softswitch) та SIP-серверів.

Як підтверджують дослідження [4, 17], використання відкритих стандартів (зокрема протоколу SIP) для сигналізації та управління сесіями дозволяє подолати проблему «прив'язки до одного виробника» (vendor lock-in), яка була характерною для старих апаратних АТС.

ISSN 2786-6025 Online

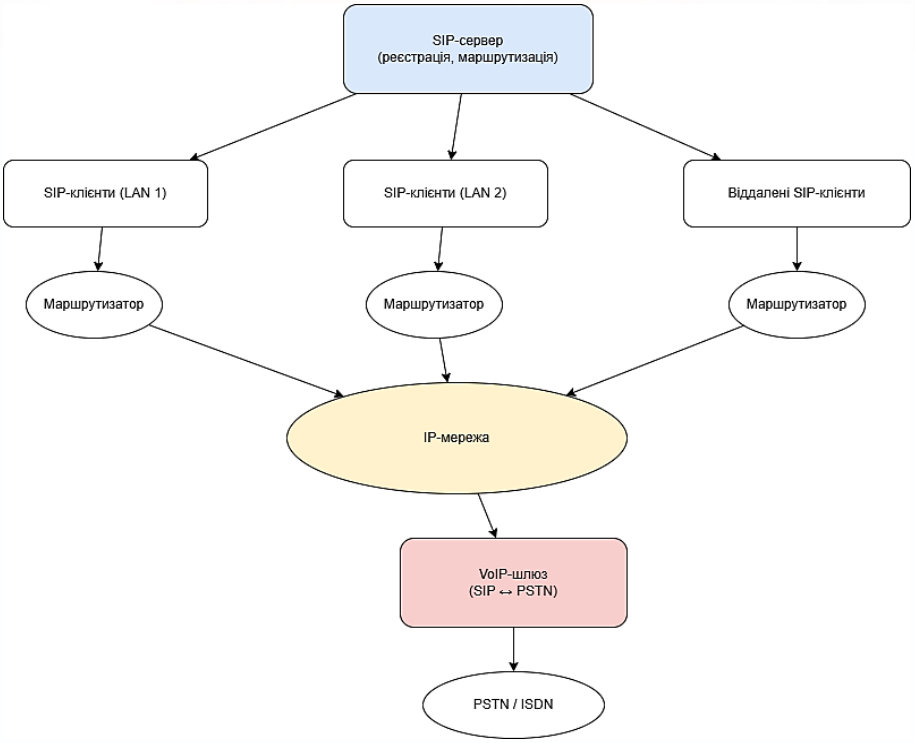

Рисунок 1 - Структурна схема інтеграції мультисервісної SIP-мережі

Це забезпечує гнучке масштабування мережі шляхом додавання нових абонентських терміналів (IP-телефонів або програмних SIP-клієнтів) без необхідності фізичного прокладання нових кабельних ліній. Окремим архітектурним викликом для органів державної влади є забезпечення захищеного міжвідомчого інформаційного обміну. Оскільки передача відкритого голосового трафіку через публічні мережі є неприпустимою з огляду на вимоги державних стандартів захисту інформації [8, 9, 18], концептуальна модель передбачає обов'язкове інкапсулювання VoIP-трафіку у віртуальні приватні мережі (VPN). Використання протоколів тунелювання рівня L2/L3 (наприклад, IPSec або L2TP) на базі граничних маршрутизаторів дозволяє створити логічно ізольований та криптографічно захищений простір для взаємодії територіально розподілених підрозділів [1, 2, 19].

Перехід до платформ уніфікованих комунікацій (UC) та консолідація сервісів. Впровадження базової IP-телефонії та програмних комутаторів є лише першим етапом модернізації електронної комунікаційної інфраструктури. Сучасні вимоги до оперативності та скоординованості державного управління зумовлюють необхідність еволюційного переходу від розрізнених засобів зв'язку до комплексних платформ уніфікованих комунікацій (Unified Communications, UC). Як доводять дослідження [5, 6], ключовою перевагою UC-рішень для державного сектору є консолідація різноманітних комунікаційних сервісів (голосовий зв'язок, відеоконференцзв'язок, захищений обмін миттєвими

ISSN 2786-6025 Online

повідомленнями, індикація статусу присутності) в єдиному керованому середовищі. Такий підхід дозволяє державним службовцям відмовитися від використання неконтрольованих публічних месенджерів для службового листування, що критично важливо для збереження конфіденційності. Крім того, централізація управління цими сервісами суттєво знижує фінансові та часові витрати на адміністрування відомчих мереж. Практична реалізація таких платформ (на прикладі розгортання систем класу Cisco Unified Communications Manager або їх відкритих аналогів) вимагає впровадження стандартизованих протоколів [4, 17]. Базовим протоколом встановлення, модифікації та завершення мультимедійних сесій виступає SIP (Session Initiation Protocol). Його архітектура дозволяє не лише забезпечити сумісність кінцевого обладнання від різних виробників, але й організувати складну маршрутизацію викликів. Наприклад, у разі недоступності абонента на робочому IP-телефоні, система здатна автоматично переадресувати виклик на його захищений програмний SIP-клієнт (Softphone) на мобільному пристрої або перевести дзвінок на голосову пошту. Водночас міграція до конвергентного середовища висуває нові вимоги до безперебійності роботи системи. Згідно з результатами досліджень ефективності функціонування систем IP-телефонії [14, 15, 20], консолідація медіатрафіку вимагає постійного контролю якості користувацького досвіду. Для органів державної влади це означає необхідність інтеграції в UC-платформи спеціалізованих аналітичних модулів, які здатні в режимі реального часу відслідковувати навантаження на сервери (CPU/RAM), фіксувати затримки передачі пакетів та оперативно реагувати на деградацію сервісу ще до моменту переривання управлінського зв'язку.

Кібербезпека та управління якістю (QoS) в умовах гетерогенних мереж. Переведення голосового трафіку в середовище передачі даних (IP-мережі) породжує принципово новий клас загроз для систем державного управління. Як зазначається у дослідженнях [10, 21-23], відкритість протоколу SIP робить сервери управління комунікаціями вкрай вразливими до специфічних мережевих атак. Найбільшу небезпеку становлять розподілені атаки на відмову в обслуговуванні (DDoS-атаки на SIP-сервери), підміна ідентифікатора абонента (Caller ID Spoofing) та несанкціоноване перехоплення RTP-пакетів (Man-in-the-Middle) з метою прослуховування розмов [12, 13, 24, 25].

Відповідно до міжнародних стандартів захисту електронних комунікацій (зокрема вимог NIST та урядових директив [8, 18]), концептуальна архітектура урядової мережі вимагає обов'язкового впровадження механізмів криптографічного захисту. Захист сигнального трафіку (команд встановлення та завершення виклику) має здійснюватися за допомогою протоколу TLS (Transport Layer Security), тоді як безпосереднє шифрування медіаданих (самого голосу) — за допомогою протоколу SRTP (Secure Real-Time Transport

ISSN 2786-6025 Online

Protocol) [5, 11]. Однак, впровадження жорсткого шифрування (особливо при тунелюванні трафіку через IPSec-з'єднання між різними відомствами) створює вагому інженерну проблему — суттєве погіршення показників якості обслуговування (Quality of Service, QoS).

Дослідження [3, 14, 19] доводять, що криптографічні перетворення збільшують розмір пакетів (через додавання нових заголовків) та вносять додаткові апаратні затримки під час їх обробки маршрутизаторами. Для чутливого до затримок голосового трафіку це призводить до збільшення джитера (коливання затримки) та відсотка втрачених пакетів, що проявляється як «металевий голос» або обриви зв'язку. Для вирішення цього конфлікту між безпекою та якістю, запропонована методологія розгортання мереж вимагає впровадження механізмів пріоритезації трафіку на мережевому рівні [1]. Електронна комунікаційна інфраструктура державного органу повинна бути налаштована на використання моделі диференційованого обслуговування (DiffServ). Це передбачає маркування голосових пакетів найвищим класом обслуговування (наприклад, міткою DSCP EF - Expedited Forwarding) на виході з IP-телефону або шлюзу [16]. Завдяки цьому, навіть в умовах пікового завантаження каналів зв'язку між міністерствами або під час кібератаки на інформаційні ресурси відомства, маршрутизатори гарантовано і позачергово пропускатимуть зашифрований управлінський голосовий трафік, зберігаючи його цілісність та розбірливість.

Висновки. У статті проведено аналіз сучасного стану розвитку інформаційно-комунікаційних мереж органів державної влади на основі існуючих інформаційних технологій, зокрема IP-телефонії та платформ уніфікованих комунікацій (UC). Досліджувану тематику статті забезпечено шляхом виконання трьох ключових завдань, що охоплюють аналіз перспектив міграції інфраструктури, розробку концептуальної архітектури мережі та визначення принципів інформаційної безпеки й управління якістю обслуговування (QoS). Порівняльний аналіз наукових джерел і поточної інфраструктури показав, що традиційні ізольовані АТС вичерпали свій технологічний ресурс і не забезпечують належної масштабованості, тоді як платформи UC дозволяють консолідувати розрізнені комунікаційні сервіси (голосовий зв'язок, відеоконференції, захищений корпоративний чат). Встановлено, що інтеграція цих технологій є необхідною умовою для підвищення оперативності управління та повної відмови від використання вразливих публічних месенджерів у державному секторі. Запропонована концептуальна архітектура інтегрованої комунікаційної мережі інтегрує використання програмних комутаторів (Softswitch) для централізованого управління викликами та спеціалізованих VoIP-шлюзів для трансляції протоколів і взаємодії з успадкованими системами. Модель базується на гетерогенному підході, що забезпечує її гнучкість,

ISSN 2786-6025 Online

збереження наявного відомчого номерного плану та придатність для поступової модернізації без переривання управлінських процесів. Запропоновано комплексні принципи забезпечення доступності, безпеки та надійності системи для всіх відомчих користувачів, включаючи застосування віртуальних приватних мереж (VPN), наскрізного криптографічного шифрування (TLS/SRTP) та моделі диференційованого обслуговування (DiffServ). Реалізація цих принципів можлива завдяки апаратному маркуванню голосових пакетів, позачерговій пріоритезації трафіку та нейтралізації специфічних мережевих загроз (DDoS-атак, спуфінгу) у критичних умовах функціонування держави. А

налітичний підхід дав нам змогу не лише узагальнити можливості сучасних телекомунікаційних рішень, а й запропонувати цілісну концепцію модернізації урядового зв'язку, яка враховує як інженерно-технічні, так і безпекові аспекти. При цьому низка питань потребує подальшого дослідження. Серед них, зокрема, розробка математичних моделей для оцінки та прогнозування відмовостійкості кластерних SIP-серверів в умовах цілеспрямованих кібератак, створення оптимізованих алгоритмів маршрутизації зашифрованого трафіку для мінімізації джитера, а також проектування механізмів інтеграції відомчих платформ UC.

Література

1. QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method / A. Darmawan. *IEEE Xplore*. 2023. URL: https://ieeexplore.ieee.org/document/9994572/.

2. VPN Traffic Analysis: A Survey on Detection and Application Identification / M. Rossi. *IEEE Xplore*. 2025. URL: https://ieeexplore.ieee.org/document/11091298.

3. Analysis QoS VoIP using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol / B. Santoso. *IEEE Xplore*. 2022. URL: https://ieeexplore.ieee.org/document/9970120/ [in English].

4. Methodology for Studying the Level of Network Security of an IP PBX Server / P. Petrov. *Telecom*. 2025. Vol. 7(1). P. 22. URL: https://www.mdpi.com/2673-4001/7/1/22

5. The Development of a Secure Internet Protocol (IP) Network Based on Asterisk Private Branch Exchange (PBX) / K. Ali. *Applied Sciences*. 2023. Vol. 13(19). P. 10712. URL: https://www.mdpi.com/2076-3417/13/19/10712

6. Що таке IP-телефонія і як вона працює: просте пояснення від IPTel / IPTel. 2025. URL: https://iptel.ua/blog/article/shcho-take-ip-telefoniia

7. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1089-20

8. Security Considerations for Voice Over IP Systems (NIST SP 800-58). National Institute of Standards and Technology. 2022. URL: https://csrc.nist.gov/publications/detail/sp/800-58/final

9. Нормативно-правова база. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/docs

10. Studying the Impact of a UDP DoS Attack on the Parameters of VoIP Voice and Video Streams / I. Georgiev et al. *Future Internet*. 2025. Vol. 17(4). P. 139. URL: https://www.mdpi.com/1999-5903/17/4/139

ISSN 2786-6025 Online

11. Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems / C. Smith et al. *Network*. 2022. Vol. 2(4). P. 32. URL: https://www.mdpi.com/2673-8732/2/4/32

12. An Approach to Mitigate DDoS Attacks on SIP Based VoIP / A. Al-Hajri. *Engineering Proceedings*. 2023. Vol. 14(1). P. 6. URL: https://www.mdpi.com/2673-4591/14/1/6

13. Enhancing VoIP Security: Recent Advances in Deep Learning for DoS Detection / M. A. et al. *IEEE Xplore*. 2024. URL: https://ieeexplore.ieee.org/document/10576456/

14. Ubunye: An MEC Orchestration Service Based on QoE, QoS, and Service Classification Using Machine Learning / N. Zulu. *Future Internet*. 2025. Vol. 17(2). P. 66. URL: https://www.mdpi.com/1999-5903/17/2/66

15. Enhanced Flow Rate-Based Queuing Discipline for Contention Avoidance in SD-WANs / S. Kumar. *IEEE Xplore*. 2025. URL: https://ieeexplore.ieee.org/document/10949159

16. Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications / F. Ahmad. *IEEE Xplore*. 2023. URL: https://ieeexplore.ieee.org/document/10314996

17. Session Initiation Protocol Proxy in a Role of a Quality of Service Control Application in Software-Defined Networks / J. Novak. *Information*. 2022. Vol. 6(6). P. 123. URL: https://www.mdpi.com/2411-9660/6/6/123

18. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : Постанова Кабінету Міністрів України від 18.06.2025 № 712. Кабінет Міністрів України. URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-zakhystu-informatsiinykh-elektronnykh-komunikatsiinykh-informatsiino-s712180625

19. Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol / D. Pratama. *IEEE Xplore*. 2023. URL: https://ieeexplore.ieee.org/document/10151888/

20. In-Depth Study and Analysis of OT and IT Traffic Separation in Refinery and Petrochemical Industries / H. Chen. *IEEE Xplore*. 2025. URL: https://ieeexplore.ieee.org/document/11373332

21. Assessing the Impact of DoS Attacks on the Performance of Asterisk-Based VoIP Platforms / I. Georgiev. *Telecom*. 2024. Vol. 6(4). P. 98. URL: https://www.mdpi.com/2673-4001/6/4/98

22. Studying the Impact of Different TCP DoS Attacks on the Parameters of VoIP Streams / P. Ivanov. *Telecom*. 2024. Vol. 5(3). P. 29. URL: https://www.mdpi.com/2673-4001/5/3/29

23. Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks / S. Al-Rubaye. *Sensors*. 2020. Vol. 20(20). P. 5875. URL: https://www.mdpi.com/1424-8220/20/20/5875

24. Detecting SPIT Attacks in VoIP Networks Using Convolutional Autoencoders: A Deep Learning Approach / M. Al-Shabi. *Applied Sciences*. 2023. Vol. 13(12). P. 6974. URL: https://www.mdpi.com/2076-3417/13/12/6974

25. Identification of Distributed Denial of Services Anomalies by Using Combination of Entropy and Sequential Probabilities Ratio Test Methods / Y. Al-Otaibi. *Sensors*. 2021. Vol. 21(19). P. 6453. URL: https://www.mdpi.com/1424-8220/21/19/6453

References:

1. Darmawan, A. (2023). QoS analysis on VoIP with VPN using SSL and L2TP IPSec method. *IEEE Xplore*. https://ieeexplore.ieee.org/document/9994572/ [in English].

2. Rossi, M. (2025). VPN traffic analysis: A survey on detection and application identification. *IEEE Xplore*. https://ieeexplore.ieee.org/document/11091298 [in English].

ISSN 2786-6025 Online

3. Santoso, B. (2022). Analysis QoS VoIP using GRE + IPSec tunnel and IPIP based on session initiation protocol. *IEEE Xplore*. https://ieeexplore.ieee.org/document/9970120/ [in English].

4. Petrov, P. (2025). Methodology for studying the level of network security of an IP PBX server. *Telecom, 7*(1), 22. https://www.mdpi.com/2673-4001/7/1/22 [in English].

5. Ali, K. (2023). The development of a secure internet protocol (IP) network based on Asterisk private branch exchange (PBX). *Applied Sciences, 13*(19), 10712. https://www.mdpi.com /2076-3417/13/19/10712 [in English].

6. IPTel. (2025). *Shcho take IP-telefoniia i yak vona pratsiuie: proste poiasnennia vid IPTel* [What IP telephony is and how it works: a simple explanation from IPTel]. https://iptel.ua/ blog/article/shcho-take-ip-telefoniia [in Ukrainian].

7. Verkhovna Rada of Ukraine. (2020). *Pro elektronni komunikatsii* [On electronic communications] (Law No. 1089-IX). https://zakon.rada.gov.ua/laws/show/1089-20 [in Ukrainian].

8. National Institute of Standards and Technology. (2022). *Security considerations for voice over IP systems* (NIST SP 800-58). https://csrc.nist.gov/publications/detail/sp/800-58/final [in English].

9. State Service of Special Communications and Information Protection of Ukraine. (n.d.). *Normatyvno-pravova baza* [Regulatory framework]. https://cip.gov.ua/ua/docs [in Ukrainian].

10. Georgiev, I., et al. (2025). Studying the impact of a UDP DoS attack on the parameters of VoIP voice and video streams. *Future Internet, 17*(4), 139. https://www.mdpi.com/1999-5903/17/4/139 [in English].

11. Smith, C., et al. (2022). Call me maybe: Using dynamic protocol switching to mitigate denial-of-service attacks on VoIP systems. *Network, 2*(4), 32. https://www.mdpi.com/2673-8732/2/4/32 [in English].

12. Al-Hajri, A. (2023). An approach to mitigate DDoS attacks on SIP based VoIP. *Engineering Proceedings, 14*(1), 6. https://www.mdpi.com/2673-4591/14/1/6 [in English].

13. M., A., et al. (2024). Enhancing VoIP security: Recent advances in deep learning for DoS detection. *IEEE Xplore*. https://ieeexplore.ieee.org/document/10576456/ [in English].

14. Zulu, N. (2025). Ubunye: An MEC orchestration service based on QoE, QoS, and service classification using machine learning. *Future Internet, 17*(2), 66. https://www.mdpi. com/1999-5903/17/2/66 [in English].

15. Kumar, S. (2025). Enhanced flow rate-based queuing discipline for contention avoidance in SD-WANs. *IEEE Xplore*. https://ieeexplore.ieee.org/document/10949159 [in English].

16. Ahmad, F. (2023). Attacks notification of differentiated services code point (DSCP) values modifications. *IEEE Xplore*. https://ieeexplore.ieee.org/document/10314996 [in English].

17. Novak, J. (2022). Session initiation protocol proxy in a role of a quality of service control application in software-defined networks. *Information, 6*(6), 123. https://www.mdpi.com/ 2411-9660/6/6/123 [in English].

18. Cabinet of Ministers of Ukraine. (2025). *Deiaki pytannia zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh, tekhnolohichnykh system* [Some issues of protection of information, electronic communication, information and communication, technological systems] (Resolution No. 712). https://www.kmu.gov.ua/npas/deiaki-pytannia-zakhystu-informatsiinykh-elektronnykh-komunikatsiinykh-informatsiino-s712180625 [in Ukrainian].