ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

РОМАНЕЦЬ ІГОР ЄВГЕНОВИЧ

УДК 004.056:004.94:654.18

ДИСЕРТАЦІЯ
ІНТЕЛЕКТУАЛІЗОВАНА КОМП'ЮТЕРНА СИСТЕМА ВИЯВЛЕННЯ ЗЛОВМИСНИХ ПОВІДОМЛЕНЬ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

05.13.05 – комп'ютерні системи та компоненти

Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ І. Є. Романець

Ідентичність за змістом з оригіналом підтверджую
Секретар Дубак

Науковий керівник:
Саченко Анатолій Олексійович
доктор технічних наук, професор.

Тернопіль – 2025

АНОТАЦІЯ

Романець І.Є. Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп’ютерні системи та компоненти». – Західноукраїнський національний університет, Тернопіль, 2025.

Дисертаційна робота присвячена актуальній науково-технічній задачі підвищення рівня захищеності корпоративних мереж шляхом розробки та дослідження інтелектуалізованої комп'ютерної системи, призначеної для виявлення зловмисних повідомлень в IP-телефонії.

В роботі проаналізовано сучасні загрози та вразливості систем IP-телефонії в корпоративному середовищі, такі як спам через інтернет-телефонію, шахрайство з оплатою дзвінків та атаки на відмову в обслуговуванні (DoS). Виявлено недостатню ефективність існуючих методів та засобів захисту перед новими та адаптивними атаками, що зумовлює необхідність застосування інтелектуальних підходів.

Запропоновано архітектуру інтелектуалізованої комп'ютерної системи, яка використовує методи машинного навчання для аналізу трафіку (SIP-повідомлень) та метаданих медіа-потоків (RTP/RTCP) IP-телефонії. Розроблено моделі та алгоритми для виділення інформативних ознак зловмисних повідомлень, класифікації трафіку та виявлення аномалій в реальному часі. Особливу увагу приділено здатності системи до самонавчання та адаптації до нових, раніше невідомих типів загроз.

Досліджено ефективність різних алгоритмів машинного навчання для вирішення задачі класифікації та виявлення аномалій в IP-телефонії. Проведено експериментальну перевірку розробленої системи на реальних та змодельованих наборах даних, що підтвердило її здатність виявляти зловмисні повідомлення з високою точністю та низьким рівнем помилкових спрацювань.

Наукова новизна роботи полягає у розробці комплексного підходу до виявлення зловмисних повідомлень в IP-телефонії на основі інтелектуального аналізу багатовимірних даних, що враховує специфіку корпоративних мереж, а

також у вдосконаленні методів адаптивного виявлення загроз на основі онтологічного підходу та нечіткої логіки.

Практичне значення отриманих результатів полягає у розробленому програмному прототипі системи, рекомендаціях щодо її впровадження та налаштування в корпоративних мережах для підвищення рівня безпеки IP-телефонії, запобігання фінансовим втратам та захисту конфіденційної інформації.

Ключові слова: IP-телефонія, VoIP, зловмисні повідомлення, вішинг, інтелектуалізована система, машинне навчання, виявлення аномалій, кібербезпека, захист інформації.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. A. Melnyk, R. Shevchuk, I. Romanets, I. Yakymenko, S. Voznyak, and V. Luchyk, "A Method of Detecting Anomalies in IP Phone Traffic based on Ontology of Voip Messages," *2024 14th International Conference on Advanced Computer Information Technologies (ACIT)*, Ceske Budejovice, Czech Republic, 2024, pp. 485-489, DOI: 10.1109/ACIT62333.2024.10712505.
2. Balyk, A., Karpinski, M., Naglik, A., Shangytbayeva, G., & Romanets, I. (2017). Using Graphic Network Simulator 3 For DDoS Attacks Simulation. International Journal of Computing, 16(4), 219-225 DOI: 10.47839/ijc.16.4.910
3. Todd J.B. Blayone, Olena Mykhailenko, Svetlana Usca, Anda Abuze, Ihor Romanets, Mykhailo Oleksiiv; Exploring technology attitudes and personal–cultural orientations as student readiness factors for digitalised work. *Higher Education, Skills and Work-based Learning* 17 June 2021; 11 (3): 649–671. DOI:10.1108/HESWBL-03-2020-0041
4. Романець І. Захист від термінації трафіку в IP-мережі на основі нечіткої логіки: Науковий журнал “Вимірювальна та обчислювальна техніка в технологічних процесах”(1), Хмельницький національний університет, Хмельницький, 2024 с. 186-193, DOI: 10.31891/2219-9365-2024-77-23.

5. І. Романець, «Онтологічний підхід в системі забезпечення безпеки використання IP-телефонії», *Опт-ел. інф-енерг. техн.*, вип. 47, вип. 1, с. 240–252, Чер. 2024. DOI: 10.31649/1681-7893-2024-47-1-240-252.
6. І. Романець, “Архітектура інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі”, *Вісник Хмельницького національного університету. Серія: Технічні науки*, vol. 337, no. 3(2), pp. 425–436, May 2024, DOI:10.31891/2307-5732-2024-337-3-65.
7. Markowsky, G., Sachenko, A., Voznyak, S., Spilchuk, V., Romanyak, R., Turchenko, V. and Romanets, I. 2014. The Ternopil Educational Communication Center: A Nato Project To Integrate Regional Information Technology Resources. *International Journal of Computing*. 7, 1 (Aug. 2014), 185-190. DOI:10.47839/ijc.7.1.503.

Список наукових праць, які додатково відображають наукові результати та засвідчують апробацію матеріалів дисертації:

8. I. Romanets, A. Sachenko and L. Dubchak, "Method of Protection Against Traffic Termination in VoIP," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-5, DOI: 10.1109/ECAI.2018.8678992.
9. Komar, M., Kochan, V., Dubchak, L., Sachenko, A., Golovko, V., Bezobrazov, S., Romanets, I. “High performance adaptive system for cyber attacks detection”, 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, Bucharest, Romania, 2, art. no. 8095208, pp. 853-858. DOI: 10.1109/IDAACS.2017.8095208
10. M. Dyvak, A. Pukas, A. Melnyk, I. Voytyuk, S. Valchyshyn, and I. Romanets, "Software Architecture for Modeling the Interval Static and Dynamic Objects," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 2021, pp. 572-575, DOI: 10.1109/ ACIT52158.2021.9548577.

11. M. Dyvak, A. Melnyk, L. Dostalek, V. Ostroverkhov, L. Honchar, and I. Romanets, "Repository of Interval Models of Dynamics of Concentrations of Harmful Emissions of Motor Transport," 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 89-94, DOI: 10.1109/ACIT54803.2022.9913123.
12. O. Kochan, O. Osolinskyi, A. Sachenko, V. Kochan, and I. Romanets, "Simulator of Microcontroller's Power Consumption," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 787-792, DOI: 10.1109/IDAACS58523.2023.10348884.
13. V. Tymchyshyn, B. Tymchyshyn, A. Melnyk, V. Manzhula, V. Faifura, and I. Romanets, "The System Architecture of the Software for Modeling Harmful Emissions in Soil," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 58-62, DOI: 10.1109/ACIT58437.2023.10275416.
14. A. Sartiukova, O. Markiv, V. Vysotska, I. Shakleina, N. Sokulska, and I. Romanets, "Remote Voice Control of Computer Based on Convolutional Neural Network," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1058–1064, DOI: 10.1109/ IDAACS58523.2023.10348808.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VoIP – Voice over Internet Protocol

SIP – Session Initiation Protocol

RTP –Real-time Transport Protocol

RTCP – Real-Time Transport Control Protocol

АТА – Адаптер телефонний аналоговий

SBC – Session Border Controller

ТМЗК – Телефонна мережа загального користування

SGCP – Simple Gateway Control Protocol

IPDC – Internet Protocol Device Control

TLS – Transport Layer Security

SRTP – Secure Real-time Transport Protocol

IP – Internet Protocol

IVR – Голосове меню (Interactive Voice Response)

ВСТУП

Актуальність теми дослідження. Сучасні корпоративні мережі все частіше використовують IP-телефонію (VoIP) як ефективний засіб комунікації через її гнучкість, масштабованість та економічні переваги. Однак зростання популярності VoIP супроводжується збільшенням кількості кіберзагроз, зокрема зловмисних повідомлень (спам, фішинг, атаки на відмову в обслуговуванні тощо), що становлять серйозну небезпеку для конфіденційності, цілісності та доступності комунікаційних сервісів [1].

IP-телефонія забезпечує гнучкість, масштабованість та економічність корпоративного зв'язку, дозволяє інтегрувати голосові сервіси з іншими інформаційними системами, включаючи CRM, ERP та інструменти управління знаннями.

Однак, разом із перевагами, IP-телефонія стає привабливою ціллю для зловмисників, що обумовлює виникнення нових загроз, зокрема – розсилання зловмисних SIP-повідомлень, фішингу, спуфінгу, DoS-атак, перехоплення конфіденційної інформації [3].

Значний внесок у сферу дослідження безпеки IP-телефонії (VoIP) та виявлення зловмисних повідомлень внесли зарубіжні та вітчизняні вчені, список яких наведено у дисертаційні роботі.

У контексті сучасних викликів, зумовлених гібридними загрозами та цифровими трансформаціями, питання підвищення ефективності виявлення зловмисних повідомлень в IP-телефонії набуває особливої актуальності. Це особливо важливо для корпоративного середовища, де забезпечення інформаційної безпеки прямо впливає на стійкість бізнесу, збереження критичних даних та довіру клієнтів.

На сьогодні існуючі методи, технічні засоби та програмні рішення не дозволяють своєчасно виявити та локалізувати зловмисну активність у VoIP-мережах. Більшість з них не враховують динаміку змін у поведінкових шаблонах трафіку, мають низьку адаптивність до нових типів загроз і не здатні до самонавчання. Це вимагає впровадження нових підходів, що базуються на

використанні технологій штучного інтелекту, машинного навчання, експертних систем та аналізу аномалій [4].

У зв’язку з цим актуальним є науково обґрунтоване розв’язання задачі підвищення ефективності захисту IP-телефонії із врахуванням своєчасності виявлення зловмисних VoIP-повідомлень шляхом створення інтелектуалізованої комп'ютерної системи, що відповідає сучасним тенденціям у сфері кібербезпеки та цифрової трансформації.

Розв’язання цієї задачі сприятиме підвищенню рівня захищеності корпоративних інформаційних систем, забезпеченню безперервності бізнес-процесів, зниженню ризиків фінансових та репутаційних втрат.

Мета і задачі дослідження. Метою роботи є підвищення ефективності захисту IP-телефонії у корпоративній мережі шляхом створення інтелектуалізованої комп'ютерної системи виявлення зловмисних повідомлень, що базується на онтологічній моделі її функціонування та методах інтелектуального аналізу даних.

Для досягнення цієї мети у дисертаційній роботі поставлено наступні завдання:

1) аналіз сучасних методів та засобів захисту IP-телефонії у корпоративній мережі, які включають компоненти інтелектуального аналізу даних;
2) розробити онтологічну модель функціонування IP-телефонії, яка включатиме формалізацію основних понять та зв’язків між ними;
3) розробити метод автоматизованого наповнення онтології тематичних повідомлень в корпоративній мережі;
4) розробити метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень;
5) розробити засіб захисту від термінації трафіку в IP-телефонії на основі використані нечіткої логіки, що сприятиме підвищенню рівня безпеки та якості зв'язку.
6) розробити архітектуру та структурно-функціональні схеми базових підсистем інтелектуалізованої системи;

7) здійснити експериментальні дослідження розроблених методів та засоби виявлення аномальних повідомлень у IP-телефонії корпоративної мережі.

Об'єкт дослідження – процеси захисту IP-телефонії з використанням інтелектуальних методів аналізу даних.

Предмет дослідження – методи та засоби захисту IP-телефонії в корпоративній мережі.

Методи дослідження. Для вирішення поставлених задач у дисертаційній роботі використовувалися такі методи:

- методи системного аналізу та огляду літератури – методи штучного інтелекту, зокрема онтологічного інжинірингу та представлення знань;
- методи машинного навчання, зокрема кластерного аналізу (групування) та виявлення аномалій;
- методи об'єктно-орієнтованого проектування та програмування;
- методи експериментальних досліджень та статистичної обробки даних.

Наукова новизна одержаних результатів.

Основні наукові результати, висунуті на захист.

Вперше розроблено:

- онтологічну модель опису VoIP повідомлень в системі IP-телефонії, яка включає формалізацію основних понять у формі окремих концептів та опис зв’язків між цими поняттями, що у сукупності створило можливість розробки нових, більш ефективних методів виявлення аномалій в трафіку IP-телефонії;
- метод виявлення аномалій в трафіку IP-телефонії, який, ґрунтується на поєднані методів групування VoIP-повідомлень та контекстно-частотного аналізу, що у сукупності дозволило підвищити ефективність виявлення аномальних повідомлень.

Удосконалено:

- підсистему захисту від термінації трафіку в IP-телефонії, яка відрізняється від відомих тим, що здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних, що дозволяє враховувати

численні критерії, такі як IP-адреса клієнта, час здійснення дзвінка, часовий пояс і якість зв’язку, а також сприяє підвищенню рівня безпеки та якості зв'язку.

- архітектуру системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі, яка відрізняється від відомих наявністю блоків і процедур виявлення аномальних повідомлень в трафіку IP-телефонії на основі онтологічного підходу та розподілу доступу в режимі реального часу з використанням нечіткої логіки, що дозволило спростити функції адміністратора системи та зменшити час оброблення повідомлень.

Практичне значення отриманих результатів полягає в тому, що за результатами проведених автором теоретичних досліджень:

– розроблено систему, яка демонструє підвищення рівня виявлення зловмисних повідомлень при зниженні кількості хибних спрацьовувань в корпоративній мережі, що забезпечує значне зменшення фінансових втрат від VoIP-шахрайства та підвищення надійності зв’язку;

– створено прототип програмного рішення для Asterisk із відкритим інтерфейсом налаштування правил реагування, що спрощує його впровадження та адаптацію під потреби підприємств різного масштабу;

– запропоновані методи нечіткого виведення та онтологічного аналізу можуть бути використані як окремі модулі в існуючих системах безпеки мережі, що підвищує масштабованість та гнучкість рішення;

– результати дослідження можуть лягти в основу технічних рекомендацій із захисту IP-телефонії для IT-відділів корпоративних замовників, а також можуть бути враховані при формуванні політик інформаційної безпеки в галузевих стандартах.

- Теоретичні та практичні результати роботи використані у ПП «Колумбус», компанії «Infineon Technologies AG» та у Тернопільській обласній військовій адміністрації в управління цифрової трансформації для захисту від несанкціонованого доступу до інформації, а також у навчальному процесі при викладанні дисциплін “Комп’ютерні системи”, «Комп’ютерні мережі», «Програмно-апаратні засоби захисту інформації».

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи доповідались та обговорювались на 7 міжнародних науково-практичних конференціях, зокрема:

1. IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications – IDAACS (м. Бухарест, Румунія, 2017 р.);
2. 10th International Conference on Electronics, Computers and Artificial Intelligence – ECAI (м. Яси, Румунія, 2018 р.);
3. 11th International Conference on Advanced Computer Information Technologies – ACIT (м. Дегендорф, Німеччина, 2021 р.);
4. 12th International Conference on Advanced Computer Information Technologies – ACIT (м. Руженберок, Словаччина, 2022 р.);
5. IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications – IDAACS (м. Дортмунд, Німеччина, 2023 р.);
6. 13th International Conference on Advanced Computer Information Technologies – ACIT (м. Вроцлав, Польща, 2023 р.);
7. 14th International Conference on Advanced Computer Information Technologies – ACIT (м. Чеське Будейовіце, Чехія, 2024 р.).

Автор висловлює щиру подяку професору Карстену Вольфу (Carsten Wolff) з Університету прикладних наук і мистецтв м. Дортмунд (Dortmund University of Applied Sciences and Arts, Німеччина) за регулярну підтримку, змістовні консультації та корисні дискусії з питань кібербезпеки в IP-телефонії. Його глибоке розуміння проблеми виявлення зловмисних SIP-повідомлень, особливостей мережевих аномалій, атак типу spoofing і DoS, а також методів побудови інтелектуалізованих систем захисту, суттєво вплинули на формування концепції дисертаційної роботи. Надані ним рекомендації сприяли вдосконаленню методології дослідження, а також більш якісній підготовці наукових публікацій для міжнародних видань, що входять до наукометричних баз Web of Science і Scopus.

Публікації. За темою дисертації опубліковано 14 наукових праць, з них: 3 одноосібних статті у наукових фахових виданнях України, рекомендованих МОН України, 4 – у виданнях, що індексуються в міжнародних наукометричних базах Scopus/Web of Science, 7 тез доповідей на міжнародних конференціях, що індексуються в міжнародних наукометричних базах Scopus/Web of Science.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота містить 138 сторінок основного тексту. Загальний об’єм дисертації – 170 сторінок, 1 таблиця, 68 рисунків, 4 додатки, 112 найменування використаних джерел.

РОЗДІЛ 1 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ВИЯВЛЕННЯ ЗЛОВМИСНИХ ПОВІДОМЛЕНЬ IP-ТЕЛЕФОНІЇ

1.1 Структура IP-телефонії

IP-телефонія або VoIP (Voice over Internet Protocol) – це комунікаційна технологія, яка дозволяє здійснювати телефонні дзвінки, використовуючи широкосмугове з'єднання замість стаціонарної телефонної лінії. Ця популярна послуга бізнес-телефонії є сучасним способом здійснення телефонних дзвінків, особливо для малого та середнього бізнесу, який потребує більш ефективного спілкування.

Типове апаратне обладнання включає в себе маршрутизатор для Інтернету з підключеним телефоном. IP-телефон використовує Інтернет для передачі голосу користувача так само, як і фізична стаціонарна телефонна лінія. Єдина відмінність полягає в тому, що в основі технології лежить не стаціонарний телефонний зв'язок, а інтернет. В цьому і полягає проблема, що захист зв'язку постійно потрібно вдосконалювати, так як, завдяки Інтернету, він доступний для проникнення із любої точки світу [2].

Типова схема IP-телефонії включає кілька ключових компонентів (рис.1.1), які забезпечують передачу голосу через IP-мережі, зокрема кінцеві пристрої, сервери сигналізації, медіашлюзи, системи керування дзвінками та маршрутизації, інфраструктура передачі даних, протоколи IP-телефонії, хмарні сервіси та служби додаткових функцій:

- *IP-телефони* (апаратні телефони) – спеціальні телефони, підключені до Інтернету через Ethernet чи Wi-Fi, які дозволяють здійснювати дзвінки за IP-технологією;

- *софтфони* (програмні телефони) – програми, які встановлюються на комп'ютери, смартфони або планшети для здійснення дзвінків через мережу Інтернет;

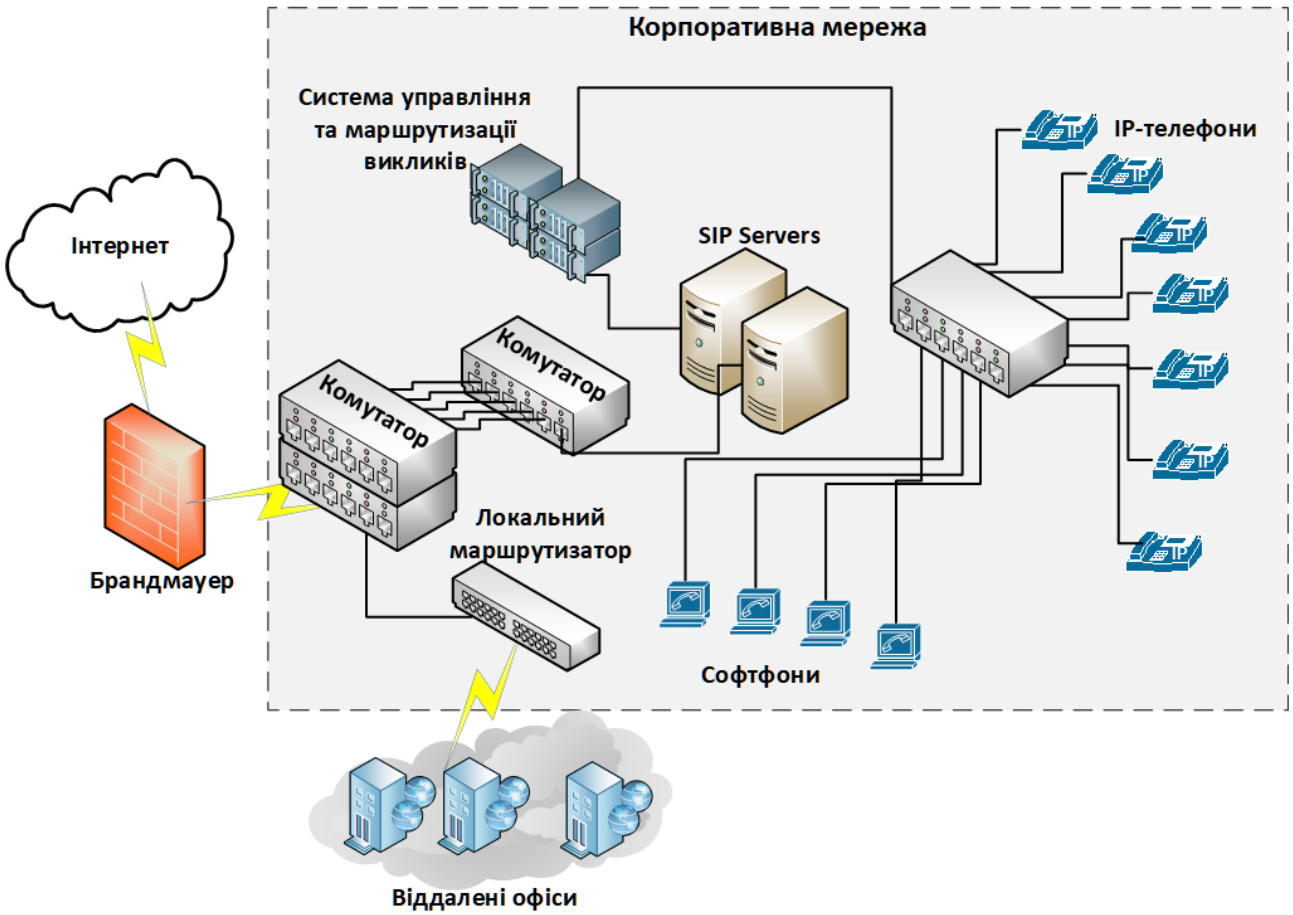


Рис. 1.1. Схема IP-телефонії

- *маршрутизатори та комутатори* – забезпечують передачу голосового трафіку між кінцевими пристроями через локальні та глобальні мережі;

- *брандмауери* – забезпечують безпеку трафіку, фільтруючи пакети та захищаючи мережу від несанкціонованого доступу;

- *SIP (Session Initiation Protocol)* – відповідає за встановлення, модифікацію та завершення дзвінків;

- *сервіси маршрутизації викликів, запису та моніторингу* – дають змогу розширювати функціональність VoIP-систем і придатні для корпоративних потреб.

Коротко охарактеризуємо основні елементи ключових компонентів. Зокрема, кінцеві пристрої включають в себе IP-телефони.

IP-телефон або VoIP телефон.

Звичайний телефон не дуже відрізняється від аналогового телефону. Телефони VoIP виглядають так само й часто мають ті самі функції, що й стаціонарні настільні телефони.

Однак є деякі ключові відмінності, які відрізняють телефони VoIP від інших настільних телефонів.

Телефони VoIP здійснюють і приймають дзвінки через Інтернет. Це означає, що вони можуть використовувати підключення до Інтернету офісу для підключення до телефонної мережі. Іншими словами, якщо офіс уже підключено до мережі Ethernet, то не потрібно вкладати кошти в додаткову мідну проводку, щоб використовувати робочі телефони [5].

Щоб здійснювати телефонні дзвінки, спочатку потрібно зареєструвати IP-телефон у обліковому записі. Це процес підключення телефону до постачальника послуг, щоб мати змогу спілкуватися один з одним. Деякі провайдери VoIP підтримують завантаження IP-телефонів для певних пристроїв, що прискорює процес реєстрації телефону за допомогою сервера завантаження.

Багато телефонів VoIP також підтримують Power over Ethernet (PoE), що дозволяє живити телефон через комутатор PoE замість адаптера живлення [6].

Розглянемо ситуацію: один номер телефону VoIP, кілька телефонних ліній VoIP. Телефони VoIP обробляють виклики інакше, ніж інші бізнес-телефони. Угорі кнопки в жовтому прямокутнику є кнопки перемикання, які дозволяють вибирати між поточними, вхідними та утримуваними викликами. Ці кнопки рідко з’являються на стаціонарних телефонах [6].

Тепер розглянемо подібний варіант IP-телефону – софтфон.

Софтфон - це програмний телефон, що забезпечує голосовий зв’язок через інтернет за допомогою технології голосового зв’язку через IP (VoIP).

На відміну від традиційних апаратних телефонів, які підключаються до стаціонарних ліній, програмні телефони передають голосові дані через смартфони чи комп’ютери.

Технологія програмного телефону використовує динаміки та мікрофони пристрою для передачі голосових пакетів призначеному одержувачу [66].

Ці функції підтримують налаштування дистанційної роботи та роботи з дому, дозволяючи співробітникам відмовитися від фізичних панелей набору номера та дзвонити клієнтам із будь-якого з наведених нижче засобів:

- браузерний інтерфейс;
- мобільний додаток;
- настільний додаток.

Переваги системи програмного телефону:

- клієнтський досвід наступного рівня;
- можливості інтеграції;
- оптимізований виклик;
- масштабованість;
- легкий доступ до записів дзвінків;
- гібридна робота;
- чудова якість зв'язку;
- краща безпека;
- зниження витрат;
- ефективне налаштування системи.

Змінити спосіб обробки вхідних дзвінків так само просто, як змінити налаштування електронної пошти у віртуальних системах програмного телефону. Користувачі можуть ефективно керувати потоком викликів, додавати системи IVR або налаштовувати повідомлення голосової пошти прямо з інформаційної панелі адміністратора [66].

Адаптери для аналогових телефонів (ATA)

Пристрої ATA є ключовими елементами комплексного рішення IP-телефонії. Пристрій ATA забезпечує доступ користувачів до послуг Інтернет-телефонії через один або кілька стандартних телефонних портів RJ-11 за допомогою стандартного аналогового телефонного обладнання. Пристрій ATA підключається до глобальної IP-мережі, наприклад, до Інтернету, через широкосмуговий (DSL або кабельний) модем або маршрутизатор [67].

Шлюз H.323 служить для контролю надходження викликів і послуг переведення з ідентифікаторів E.164 (зазвичай це номер телефону) на IP-адреси в телефонній мережі H.323 . Контролери шлюзу можна об’єднати з функцією шлюзу для проксі-дзвінків H.323, і іноді їх називають контролерами кордону сеансу (SBC). Гейткіпер також може заборонити доступ або обмежити кількість одночасних підключень, щоб запобігти перевантаженню мережі.

Кінцевим точкам H.323 не потрібно реєструватися в гейткіпері, щоб мати можливість здійснювати виклики «точка-точка», але вони є важливими для будь-якої серйозної мережі H.323 для контролю маршрутизації префіксів викликів і пропускної здатності зв’язку серед інших функцій [68].

Комутатори полегшують спільне використання ресурсів, об’єднуючи всі пристрої, включаючи комп’ютери, принтери та сервери, у мережу малого бізнесу. Завдяки комутатору ці підключені пристрої можуть обмінюватися інформацією та спілкуватися один з одним, незалежно від того, де вони знаходяться в будівлі чи на кампусі. Побудова мережі малого бізнесу неможлива без комутаторів для об’єднання пристроїв [69].

Подібно до того, як комутатор з’єднує кілька пристроїв для створення мережі, маршрутизатор з’єднує кілька комутаторів та їхні відповідні мережі, щоб створити ще більшу мережу. Ці мережі можуть бути в одному місці або в кількох місцях. При створенні мережі малого бізнесу знадобиться один або кілька маршрутизаторів. Окрім з’єднання кількох мереж разом, маршрутизатор також дозволяє мережевим пристроям і кільком користувачам отримувати доступ до інтернету.

Зрештою, маршрутизатор працює як диспетчер, направляючи трафік і вибираючи найефективніший маршрут для інформації у формі пакетів даних для переміщення по мережі. Маршрутизатор з'єднує бізнес зі світом, захищає інформацію від загроз безпеці та навіть вирішує, які пристрої мають пріоритет над іншими.

Брандмауер – це пристрій безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік на основі попередньо встановлених політик безпеки організації. За своєю суттю брандмауер – це бар'єр, який стоїть між приватною внутрішньою мережею та загальнодоступним Інтернетом. Основна мета брандмауера – пропускати незагрозливий трафік і запобігати небезпечному трафіку [70].

Абревіатура *SIP* розшифровується як протокол ініціації сеансу (Session Initiation Protocol) і відноситься до мережевого протоколу на основі TCP/IP, який можна використовувати для встановлення та керування комунікаційними з'єднаннями кількох абонентів. SIP часто використовується в телефонії Voice-over-IP для встановлення з'єднання для телефонних дзвінків. Ключові особливості протоколу ініціації сеансу визначені в RFC3261. Оскільки протокол ініціації сесії є відкритим стандартом, то він широко використовується в усьому світі. Майже всі телефонні системи на основі IP мають протокол SIP [70].

Транспортний протокол реального часу (RTP) – це мережевий протокол для передачі аудіо та відео через IP-мережі. RTP використовується в комунікаційних і розважальних системах, які включають потокове медіа, наприклад телефонію, програми для відеотелеконференцій, включаючи WebRTC, телевізійні служби та веб-функції push-to-talk [71] .

Протокол керування шлюзом медіа (MGCP) – це телекомунікаційний протокол для сигналізації та керування викликами в гібридних системах передачі голосу через IP (VoIP) і традиційних телекомунікаційних системах. Він реалізує архітектуру протоколу керування медіа-шлюзом для керування медіа-шлюзами, підключеними до комутованої телефонної мережі загального користування (ТМЗК). Медіашлюзи забезпечують перетворення традиційних електронних

носіїв інформації в мережу Інтернет-протоколу (IP). Протокол є наступником протоколу Simple Gateway Control Protocol (SGCP), який був розроблений Bellcore і Cisco , і Internet Protocol Device Control (IPDC) [72].

Системи відеоконференцій дозволяють проводити зустрічі між людьми в різних місцях. Вони включають конференц-дзвінки, місця для онлайн-зустрічей і відеоконференції, де учасники можуть бачити один одного на екранах. Бізнес-конференції можуть скоротити витрати, а також спростити проведення регулярних зустрічей і обмін інформацією.

Хоча бізнес-конференція не може замінити кожну особисту зустріч, вона особливо корисна для [73]:

- міжофісного зв'язку (ділова конференція – ефективний спосіб проведення регулярних зустрічей між людьми в різних офісах. Це може допомогти покращити спілкування та співпрацю, особливо якщо над спільним проектом працюють люди з різних місць);
- гнучкості працівників (наприклад, якщо багато людей у компанії працюють вдома, це хороший спосіб провести зустріч);
- регулярних зустрічей з клієнтами (бізнес-конференції – це хороший спосіб тримати клієнтів у курсі подій, незалежно від того, де вони знаходяться).

Сервіси маршрутизації викликів.

Розширене рішення системи маршрутизації викликів надає бізнесу можливість керувати обсягом вхідних викликів відповідно до клієнтської бази та бізнес-моделі. Завдяки програмному забезпеченню маршрутизації вхідних викликів можна задовольнити потреби клієнтів і надати агентам інструменти, необхідні для досягнення успіху.

Маршрутизація викликів – це система керування телефоном, яка дозволяє контролювати розподіл і чергування телефонних ліній підприємства. Цю чергу потім можна спрямувати до певної особи чи відділу в межах компанії, переконавшись, що вхідний дзвінок обробляє правильний відділ, покращуючи зовнішній зв’язок і забезпечуючи більш ефективне керування.

Наявність правильно налаштованої та керованої системи маршрутизації викликів може значно скоротити час, витрачений на перенаправлення абонентів до правильного контакту чи відділу, покращуючи продуктивність, якість обслуговування клієнтів і потенційно скорочуючи витрати на персонал.

Багато різних змінних можуть визначати тип потрібної системи маршрутизації викликів. Зараз багато систем бізнес-телефонії працюють за допомогою VoIP, що полегшує керування маршрутизацією викликів, моніторингом викликів і керуванням системою [74].

Це може бути щось таке просте, як кількість дзвінків, які активують систему маршрутизації викликів, час доби, відділ, який вимагає абонент, чи доступний агент для розмови по телефону.

Кожен компонент розташований по рівнях і зв'язаний стрілками, що відображають напрямок потоку інформації між компонентами. Це допомагає візуалізувати, як кінцеві пристрої, сервери сигналізації, медіашлюзи та інші елементи взаємодіють у системі IP-телефонії (рис.1.2.).

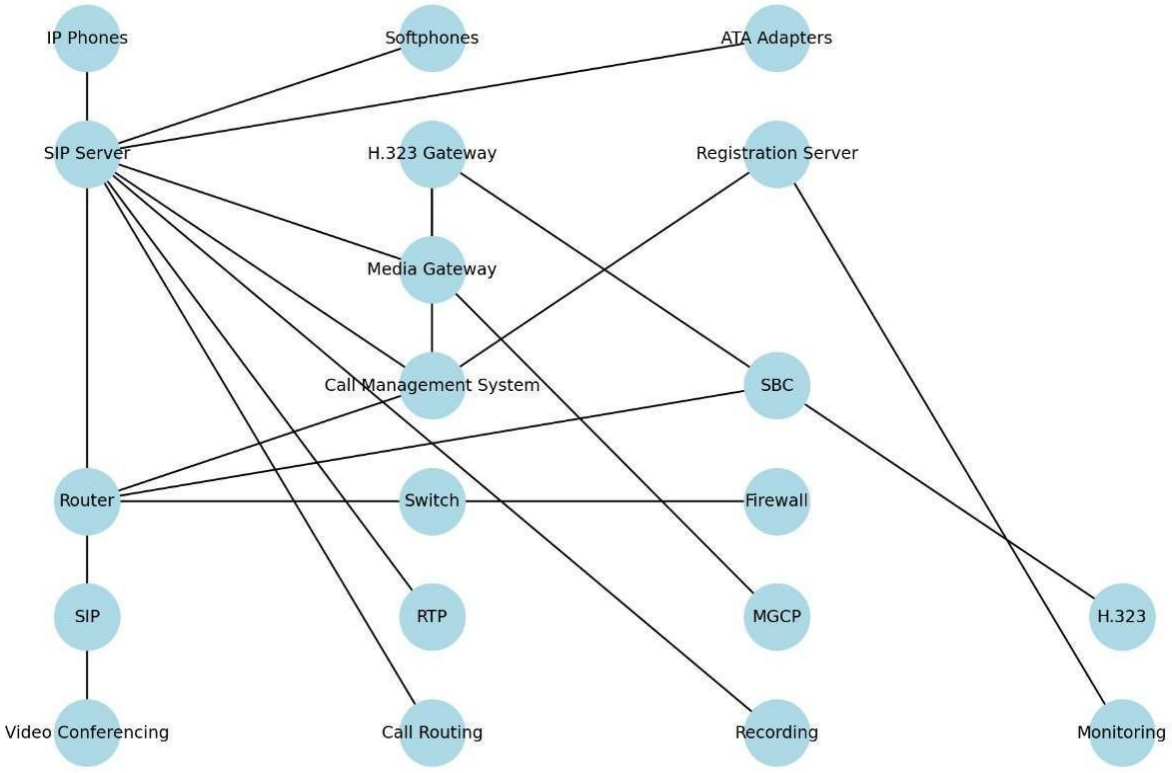


Рис. 1.2. Графічне представлення структури IP-телефонії

1.1.1 Особливості IP-телефонії

До особливостей IP-телефонії слід віднести:

1. Оцифрування голосу – аудіосигнал оцифровується та кодується.
2. Пакетування даних – голосові дані розбиваються на пакети для передачі через IP-мережу.
3. Транспортування – пакети передаються через мережу, використовуючи IP-протокол.
4. Збір та декодування – на стороні отримувача пакети збираються, декодуються і знову перетворюються в голосовий сигнал.

Розглянемо детальніше особливості IP-телефонії.

Коли голос оцифровується, відбувається перетворення на потік одиниць і нулів для передачі через телекомунікаційну мережу IP-пакетів [75]. Це необхідний крок для передачі голосу через IP.

Існує три етапи оцифрування голосу:

- квантування;
- вибірка;
- кодування.

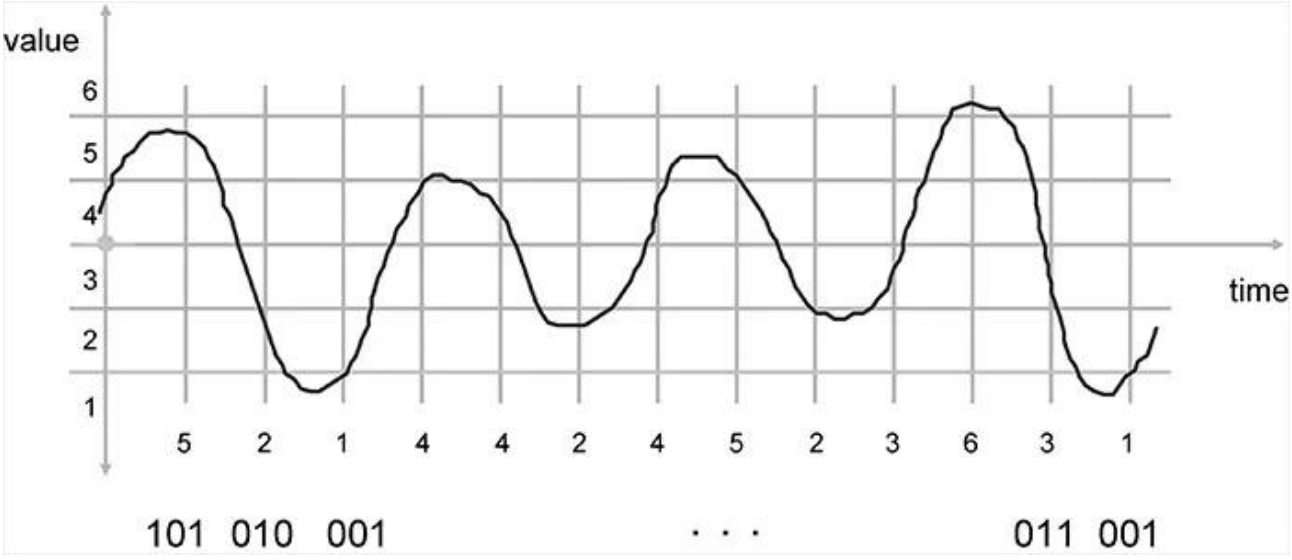


Рис.1.3. Дискретизація та квантування аналогового сигналу [75].

Квантування - це процес переходу від безперервного за значенням сигналу до дискретного. Це досягається шляхом поділу можливого діапазону значень на певну кількість "засіків", рівнів або кроків, і присвоєння кожному з цих рівнів певного числа.

Другий крок – це дискретизація. Дискретизація – це процес зміни сигналу з безперервного в часі на дискретний. Значення сигналу – це номер рівня.

Третій крок – кодування. Значення сигналу, взятого на кожному відліку (номер рівня), має бути закодоване в 1 і 0, щоб його можна було передати через цифрову систему передачі даних або зберегти в комп'ютері.

На дальньому кінці ми виконуємо зворотний процес: відтворюємо аналогову форму сигналу з отриманих кодів шляхом декодування номера рівня, генеруючи напругу зі значенням, що дорівнює значенню в центрі рівня, і плавно змінюючи напругу таким чином, коли кожен новий код спускається вниз по лінії.

Суть цього процесу полягає в тому, щоб перемістити аналоговий голосовий сигнал від ближнього до дальнього контуру без додавання шуму [75].

Фактично є невелика кількість шуму, що додається наперед, як частина аналого-цифрового перетворення. Це помилка квантування, різниця в значенні між центром рівня і тим, де насправді був сигнал.

Пакетування даних

Пакети даних - це дискретні одиниці даних, які передаються через мережу. Вони містять адреси джерела та призначення, а також частину більшого повідомлення даних, яке передається. Щоб ефективно та безпечно передавати великі обсяги даних, їх розділяють на пакети. Поділ даних на менші пакети дозволяє передавати інформацію паралельно, зменшуючи затримку і забезпечуючи більш впорядкований потік даних. Крім того, це підвищує цілісність даних, оскільки в разі втрати або пошкодження пакета під час передачі потрібно переробити лише цей пакет, а не все повідомлення, що підвищує надійність процесу. [76].

Пакети даних є важливими будівельними блоками передачі даних у комп'ютерних мережах. Це фрагменти інформації, які розбиваються на частини

і надсилаються мережею від одного пристрою до іншого. Незалежно від типу даних, що надсилаються – веб-сторінки, електронні листи чи відео - кожен фрагмент інформації перед передачею розбивається на менші пакети. Ці пакети містять частину даних і додаткові інструкції для правильної доставки. Поділ даних на пакети слугує кільком ключовим цілям. Він забезпечує ефективне використання мережевих ресурсів, розбиваючи великі файли на керовані частини. У випадках недосконалості мережі, таких як перевантаження або перешкоди, поділ пакетів дозволяє повторно передавати лише ті частини даних, які зазнали впливу, що підвищує надійність. Крім того, він забезпечує оптимальну маршрутизацію через складні мережеві шляхи, полегшує паралельну обробку для прискорення передачі даних, надає контроль над управлінням якістю обслуговування (QoS), а також покращує виявлення та виправлення помилок. По суті, концепція пакетів даних з їхнім поділом і впорядкованою передачею є фундаментальною для безперебійної роботи сучасного мережевого зв'язку [76].

Транспортування.

IP-транспорт фокусується на переміщенні пакетів даних в одній мережі або між тісно пов’язаними мережами. Він передбачає фізичну передачу пакетів даних від однієї точки до іншої, часто з використанням різних технологій, таких як Ethernet, MPLS (багатопротокольна комутація міток) або виділені лінії. IP-транспорт схожий на внутрішні дороги в межах міста, що дозволяє ефективно передавати дані в межах обмеженої території [77].

На відміну від IP-транзиту, який передбачає доступ до зовнішніх мереж, IP-транспорт залишається обмеженим певною мережевою інфраструктурою. Це робить його придатним для підприємств, які прагнуть оптимізувати внутрішні процеси зв’язку та обміну даними.

Збір та декодування.

Процес "збору та декодування" на стороні отримувача в IP-телефонії передбачає кілька основних етапів:

1. Отримання пакетів: після передачі через IP-мережу пакети голосових даних надходять до пристрою або додатку одержувача. Ці пакети можуть приходити з невеликим запізненням або в неправильному порядку.

2. Буферизація: для забезпечення неперервності звуку пакети зберігаються в буфері на короткий час. Це дозволяє компенсувати затримки і забезпечити плавний потік голосу.

3. Збір: пакети організовуються в правильному порядку відповідно до їх послідовності.

4. Декодування: після збирання пакетів відбувається їх декодування з цифрового формату, наприклад, із кодека G.711 або G.729, у аналоговий голосовий сигнал.

5. Відтворення голосу: декодовані дані передаються на динаміки або інші аудіопристрої одержувача для відтворення, що дозволяє чути повідомлення у режимі реального часу.

Таким чином, процес включає всі етапи – від прийому, буферизації та декодування до безпосереднього відтворення, що забезпечує якість зв'язку в IP-телефонії.

Рисунок 1.4 показує ключові елементи та їхні зв'язки, відображаючи, як кінцеві пристрої, сервери сигналізації, медіашлюзи та інші компоненти взаємодіють у мережі IP-телефонії.

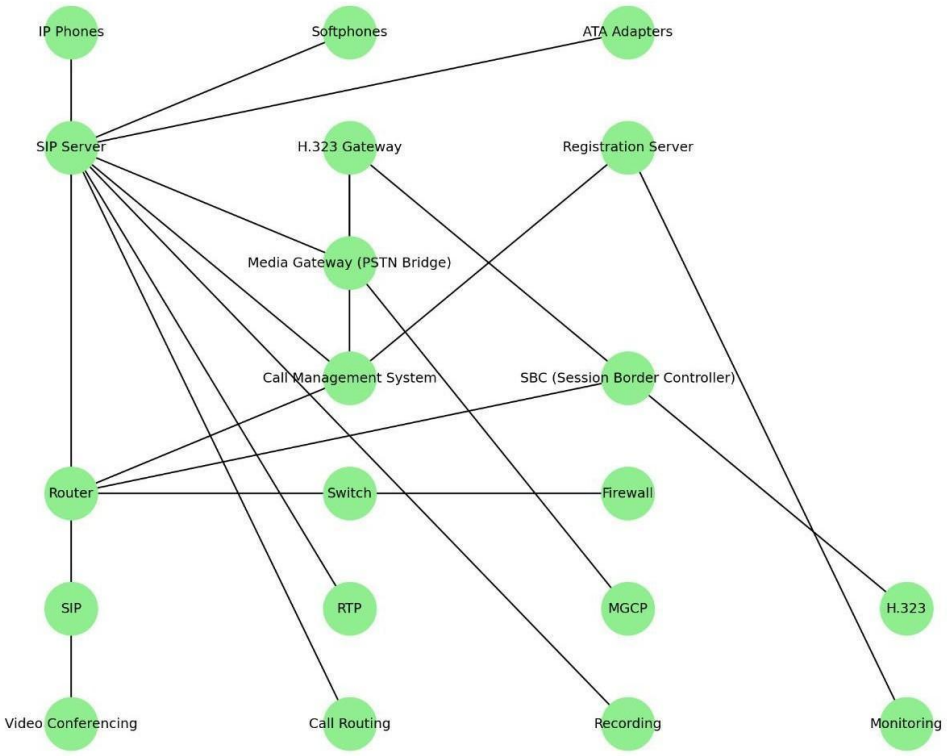


Рис.1.4. Ключові елементи IP-телефонії та їх зв’язки

1.2 Аналіз існуючих методів і засобів виявлення зловмисних повідомлень IP-телефонії

Як видно із підрозділу 1.1, існуючі системи IP-телефонії мають ряд недоліків, основним з яких є недостатній рівень безпеки. Тому необхідно розглянути існуючі методи та засоби, спрямовані на захист від типових загроз, таких як перехоплення даних, фішингові атаки, несанкціонований доступ, відмова в обслуговуванні (DoS), спуфінг і шахрайство. Основні напрями захисту включають шифрування трафіку, аутентифікацію, контроль доступу, моніторинг трафіку, аналіз поведінки і застосування методів штучного інтелекту.

Шифрування – це спосіб захисту даних, який перетворює звичайну інформацію, яку можна прочитати, у незрозумілий шифр. Зокрема, у статті [78] стверджується, що коли голос передається за технологією VoIP і потрібне шифрування, використовується транспортний протокол Secure Real-time Transport Protocol (SRTP). Він забезпечує шифрування трафіку, аутентифікацію

повідомлень та захист від атак повторного відтворення. Це простий та швидкий криптографічний протокол. Він захищає інформацію під час передачі у відкритих мережах. Другий протокол – Transport Layer Security (TLS) – шифрує іншу інформацію. Під час дзвінка передаються службові повідомлення – телефонні номери, імена користувачів тощо, які також слід надійно «заховати». Цей протокол захищає від перехоплення та модифікації повідомлень SIP. Таким чином, хоча TLS та SRTP – це два криптографічні протоколи, вони захищають різні типи інформації: SRTP – сам голос, TLS – службову інформацію [78].

Надійне шифрування має вирішальне значення для захисту конфіденційних ділових і особистих даних. Зловмисники не можуть отримати доступ до зашифрованого мережевого трафіку, тому не отримують жодних переваг [79].

Аутентифікація на основі пароля є найпростішим і найпоширенішим методом перевірки особи користувача або пристрою VoIP. Автори статті [80] описують аутентифікацію, яка працює за допомогою апаратних засобів за однією з двох альтернативних схем: за схемою запит-відповідь; за схемою аутентифікації з синхронізацією за часом. У схемі запит-відповідь користувач підключається до сервера аутентифікації, який, у свою чергу, пропонує ввести персональний ідентифікаційний номер (PIN) або користувацький ідентифікатор (user ID). Користувач передає PIN або user ID на сервер, який потім робить «запит» (передає випадкове число, яке з’являється на екрані користувача). Користувач вводить це число в спеціальний апаратний пристрій, подібний на кредитну картку, де число запиту шифрується за допомогою користувацького шифрувального ключа.

Контроль доступу вважається важливим аспектом конфіденційності, який потребує подальшого вивчення. Політика контролю доступу (або ж політика доступу) є частиною політики безпеки організації. Щоб перевірити політику контролю доступу, використовують модель контролю доступу. Загальні політики безпеки вимагають розробки або вибору відповідних засобів контролю безпеки, політики доступу так само вимагають від організації розробки або вибору засобів контролю доступу [80].

Інструменти *моніторингу мережі* – це програми, які збирають і аналізують дані з мережевих пристроїв, таких як маршрутизатори, комутатори, брандмауери, сервери та кінцеві точки.

Автори статті [81] описують методи моніторингу, засновані на маршрутизаторах – вшиті в роутери і, отже, мають низьку гнучкість. На відміну від оперативного моніторингу мережі, моніторинг мережевої безпеки і аналітики, які його використовують, повинні вміти виявляти вторгнення і всі форми атак, включаючи нові (нульові атаки) і складні загрози, щоб приймати управлінські рішення, засновані на доказах.

Жоден фахівець з безпеки не може гарантувати 100% захист від атак, але технології неперервного моніторингу і аналізу мережі надають можливості, які можуть значно знизити наслідки атаки або злому.

Моніторинг мережевої безпеки включає в себе три основних завдання, а саме: збір мережевих даних; виявлення мережевих даних; аналіз мережевих даних, пов`язаних з безпекою.

1.2.1 Методи штучного інтелекту для виявлення зловмисних повідомлень IP-телефонії

Методи штучного інтелекту (ШІ) використовуються для аналізу трафіку, виявлення аномалій і забезпечення автоматизованого виявлення загроз. Основні застосування ШІ в захисті IP-телефонії включають: машинне навчання, нейронні мережі, алгоритми глибокого навчання, експертні системи.

Машинне навчання (ML) застосовується для створення моделей поведінки нормального трафіку IP-телефонії, що допомагає у виявленні аномальних дій. Машинне навчання ефективно працює з великими обсягами даних і дозволяє адаптуватися до нових загроз.

У 2019 році індійськими дослідниками запропоновано три підходи на основі машинного навчання для виявлення аномалій у трафіку IP-мереж [45]. Розроблена стратегія багатовимірного гауссівського розподілу використовує

нестандартний підхід з використанням поліфітів для виявлення аномалій на основі адаптивного порогу. Запропонована процедура K-середніх демонструє скорочення часу виконання, але спостерігається збільшення кількості хибних спрацьовувань при обробці нормальних даних. Хоча метод є досить перспективним, для досягнення високої точності потрібно більше навчальних даних.

Нейронні мережі застосовуються для розпізнавання складних патернів у трафіку, що пов'язані з підозрілими або шкідливими діями, наприклад, виявлення фішингових дзвінків.

Алгоритми глибокого навчання використовуються для багатофакторного аналізу даних у режимі реального часу. Завдяки глибоким нейронним мережам можливо здійснювати точніший аналіз та забезпечувати високий рівень виявлення прихованих загроз.

Експертні системи можуть приймати рішення на основі правил, що визначаються експертами, і забезпечують автоматичне блокування викликів, які підпадають під категорії небезпечних або підозрілих.

Нейронні мережі.

У статті [82] розглядається метод із використанням випадкової нейронної мережі (Random Neural Network, RNN) для точного прогнозування якості голосу, що сприймається, і, що більш важливо, для виконання цього в трафіку в реальному часі, щоб подолати недоліки доступних методів. Модель RNN забезпечує ненав'язливий метод точного прогнозування та моніторингу сприйнятої якості голосу як для голосу на прослуховуванні, так і для розмовного голосу. Цей метод має здатність до навчання, що дає змогу адаптуватися до будь-яких змін мережі без втручання людини. Модель використовує три вхідні змінні (нейрони): затримку, джиттер і втрату пакетів, а також кодек G711.a. Результати показують хороший ступінь точності в обчисленні середнього балу за варіант (MOS) порівняно з алгоритмом перцептивної оцінки якості мовлення (PESQ)[82].

Алгоритми глибокого навчання.

У статті [83] запропоновано підхід глибокого навчання для виявлення шаблонів сигналізації мультимедійних сеансів, встановлених за допомогою протоколу ініціації сеансу (SIP). Підхід базується на рекурентній нейронній мережі (RNN). Досліджується продуктивність різних архітектур довгострокової короткочасної пам'яті (LSTM) RNN, які навчаються за допомогою набору даних сигналізації SIP із надійних діалогових вікон SIP, захоплених сервером SIP. Потім навчені RNN використовуються для виявлення діалогів SIP у реальному часі. Після характеристики набору даних, прийнятого для навчання, перевірки та тестування, представлені експериментальні результати, отримані для різних архітектур RNN, показують, що ймовірність класифікації надійних діалогів SIP перевищує 93% на етапі тестування. Представлено дві методології для виявлення ненормальних діалогів SIP, тобто таких, що не містяться в надійному навчальному наборі даних. Після детального аналізу асиметрії та ексцесу, обчислених за допомогою числових результатів RNN, показано, що їх можна використовувати як ознаки класифікації. Перший метод базується на неконтрольованому класифікаторі K-середніх, а другий – на напівконтрольованому пороговому класифікаторі. Експериментальні результати показують, що класифікатор на основі порогового значення досягає 99,45% ймовірності виявлення, демонструючи ефективну корисність запропонованої методології для виявлення аномальних послідовностей SIP за короткий проміжок часу [83].

Експертні системи.

Експертні системи для передачі голосу через Інтернет-протокол (VoIP) - це складний клас інтелектуальних систем, призначених для покращення управління мережею, якості дзвінків та надійності обслуговування. Ці системи використовують штучний інтелект і логіку, засновану на правилах, для автоматизації прийняття рішень, усунення несправностей і оптимізації в мережах VoIP. Розглянемо, як експертні системи сприяють розвитку VoIP-середовищ:

1. Управління якістю дзвінків:

− аналіз джиттера, затримок і втрат пакетів: експертні системи можуть відстежувати такі ключові показники, як джиттер (часткове відхилення в передачі голосового сигналу), латентність (затримка в передачі пакетів) і втрата пакетів. Використовуючи заздалегідь визначені правила та алгоритми навчання, система може виявляти проблеми та ініціювати коригувальні дії, такі як коригування розподілу смуги пропускання або надання пріоритету певним пакетам даних для підтримки якості зв'язку;

− динамічний вибір кодека: залежно від умов мережі, експертні системи можуть перемикатися між різними кодеками для оптимізації використання пропускної здатності без шкоди для якості дзвінків. Наприклад, під час високого перевантаження мережі може бути автоматично обрано кодек з нижчим бітрейтом.

2. Виявлення та діагностика несправностей:

− аналіз першопричин (RCA): коли виникають проблеми (наприклад, обриви дзвінків або низька якість звуку), експертна система може діагностувати першопричину, дотримуючись структурованого підходу до діагностики. Вона може враховувати такі фактори, як пропускна здатність, навантаження на сервер і зовнішні перешкоди, щоб точно визначити проблему;

− прогнозоване обслуговування: аналізуючи шаблони в журналах викликів і показники продуктивності системи, експертна система може передбачити потенційні збої в мережі. Наприклад, якщо маршрутизатор або сервер демонструє ознаки перевантаження, система може запланувати технічне обслуговування до того, як станеться справжня поломка.

3. Оптимізація мережевого трафіку:

− балансування навантаження трафіку: експертні системи можуть розподіляти навантаження між кількома серверами або каналами передачі даних на основі аналізу використання мережі в реальному часі, допомагаючи запобігти виникненню вузьких місць і підвищити ефективність;

− розподіл смуги пропускання: на основі шаблонів трафіку система може динамічно розподіляти смугу пропускання для надання пріоритету VoIP-трафіку над менш важливими даними, забезпечуючи стабільну якість зв'язку навіть під час високого навантаження на мережу.

4. Безпека та виявлення шахрайства:

− виявлення аномалій для запобігання шахрайству: експертні системи корисні для виявлення незвичайних патернів, що вказують на шахрайство, таких як сплеск міжнародних дзвінків або спроби несанкціонованого доступу. Встановивши правила для виявлення цих аномалій, система може позначати підозрілі дії та сповіщати адміністраторів;

− виявлення вторгнень: експертні системи можуть відстежувати несанкціонований доступ або порушення безпеки в мережі VoIP. Вони можуть бути налаштовані на розпізнавання потенційних загроз на основі відомих векторів атаки, сповіщення адміністраторів або навіть ініціювання контрзаходів.

5. Автоматизоване усунення несправностей і підтримка:

− здатність до самовідновлення: виявивши проблеми, експертні системи можуть ініціювати автоматизовані дії для їх вирішення. Наприклад, якщо якість зв'язку погіршується через високу втрату пакетів, система може спробувати перенаправити трафік або переключитися на альтернативні мережеві шляхи;

− підтримка клієнтів: деякі провайдери VoIP використовують експертні системи для допомоги командам обслуговування клієнтів. Ці системи можуть рекомендувати рішення на основі попередніх проблем і контексту, що дозволяє агентам служби підтримки вирішувати проблеми швидше.

6. Масштабованість та адаптивне навчання:

− масштабоване розгортання: експертні системи допомагають керувати великомасштабними мережами VoIP, автоматизуючи різні завдання управління, забезпечуючи стабільну роботу в різних місцях і на різних серверах;

− інтеграція машинного навчання: сучасні експертні системи часто інтегрують машинне навчання для вдосконалення з часом, уточнюючи правила і

відповіді на основі історичних даних, що підвищує їх діагностичні та прогностичні можливості.

Незважаючи на важливість отриманих результатів у вищенаведених публікаціях, їх недоліками є невідповідність змін даних в інформаційній базі управління аномаліям мережі. Таким чином, виявлення характеру різких змін, що відповідають аномальним подіям, є актуальним.

1.2.2 Методи виявлення нетипової поведінки при передачі голосу

Виявлення нетипової поведінки при передачі голосу є критично важливим для забезпечення безпеки в сучасних телекомунікаційних системах, зокрема в системах голосового зв’язку та голосових асистентах. Нетипова поведінка може вказувати на загрози, такі як зловживання послугами, шахрайство, або атаки з використанням автоматичних голосових систем. У зв’язку з цим, було розроблено різноманітні методи аналізу, які дозволяють виявляти аномалії в голосовому трафіку.

Основними методами виявлення нетипової поведінки при передачі голосу є:

1. Методи на основі статистичного аналізу

Статистичний аналіз є одним із базових підходів для виявлення аномалій у голосовому трафіку. Методи цієї групи дозволяють ідентифікувати нетипову поведінку шляхом визначення відхилень від середніх показників, таких як середня тривалість дзвінка, кількість дзвінків від одного абонента, чи географічні аномалії. Одним з популярних методів є використання нормального розподілу для аналізу відхилень у певних параметрах зв'язку.

2. Методи на основі машинного навчання

Методи машинного навчання активно застосовуються для аналізу великих обсягів голосових даних і мають здатність адаптуватися до нових типів загроз. Наприклад, класифікатори, такі як SVM (метод опорних векторів) або нейронні мережі, можуть бути використані для класифікації зразків як «нормальних» або «аномальних» на основі певних параметрів, таких як частота звуку, тембр та інші

особливості голосу. Сучасні глибокі нейронні мережі, такі як рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN), мають ще більшу точність у розпізнаванні нетипової поведінки.

3. Методи на основі аналізу сигналу

У деяких випадках аномалії в голосовому трафіку можна виявити шляхом детального аналізу акустичних характеристик сигналу. Це може включати спектральний аналіз або оцінку параметрів сигналу, таких як частота, амплітуда та тривалість. Нетипова поведінка, така як зміни в частотному спектрі або наявність перешкод, може бути ознакою спроби несанкціонованого втручання.

4. Методи на основі аналізу поведінкових шаблонів

Цей підхід базується на аналізі поведінкових характеристик користувачів, таких як час доби, коли відбувається дзвінок, частота дзвінків або типи номерів, які обираються. Такі методи дозволяють будувати шаблони поведінки користувача і відстежувати відхилення від цих шаблонів. Поведінкові аномалії можуть свідчити про спроби шахрайства, наприклад, багаторазові дзвінки на платні номери з одного облікового запису.

Методи виявлення нетипової поведінки при передачі голосу є важливою складовою сучасних систем захисту голосового трафіку. Різноманітні підходи, включаючи статистичний аналіз, машинне навчання, аналіз сигналів і поведінкових шаблонів, дозволяють не лише забезпечити високу точність у виявленні аномалій, але й адаптуватися до нових типів загроз. Використання комбінації кількох методів є найбільш ефективним, оскільки дозволяє підвищити надійність системи та мінімізувати ризик пропуску нетипової поведінки.

1.3 Перспективні шляхи розвитку предметної області та постановка задачі дослідження

На основі аналізу, проведеного в підрозділі 1.2, можна виділити перспективні шляхи розвитку методів та засобів виявлення зловмисних

повідомлень IP-телефонії в корпоративних мережах, що базуються на новітніх технологіях та підходах:

1. Шифрування трафіку [78].
2. Контроль доступу [80].
3. Моніторинг мережі [81].
4. Методи штучного інтелекту, зокрема, онтології та нечітка логіка [14, 84].

Попередній аналіз показав, що існуючі системи захисту IP-телефонії є недосконалими і використовують стандартні програмні засоби для моніторингу та захисту IP-телефонії [7, 63]. Тому, з урахуванням вказаних перспективних шляхів захисту, метою дисертаційного дослідження є розроблення інтелектуалізованої комп'ютерної системи виявлення зловмисних повідомлень IP-телефонії, яка ефективно ідентифікує загрози, запобігає несанкціонованому доступу, виявляє аномалії та захищає від кіберзагроз. Для цього необхідно вирішити наступні завдання:

1. Розробити онтологічну модель функціонування IP-телефонії.
2. Розробити метод автоматизованого наповнення онтології тематичних повідомлень в корпоративній мережі.
3. Розробити метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень.
4. Розробити узагальнену структуру, архітектуру та структурно-функціональні схеми базових підсистем інтелектуалізованої системи.
5. Розробити алгоритми інтелектуалізованої системи захисту IP-телефонії в корпоративній мережі.
6. Розробити архітектуру програмного забезпечення системи захисту.
7. Програмно реалізувати та впровадити розроблені методи та засоби виявлення аномальних повідомлень у IP-телефонії.

Висновки до розділу 1

1. Проведено всебічний аналіз сучасного стану та перспектив розвитку систем виявлення зловмисних повідомлень в IP-телефонії. Розглянуто ключові

аспекти, що стосуються структури IP-телефонії та її особливостей, які створюють як переваги, так і нові виклики у сфері кібербезпеки. Визначено, що попри значні економічні та функціональні вигоди, притаманні IP-телефонії, її інтеграція з мережею Інтернет робить її вразливою до широкого спектру кібератак, включаючи DoS/DDoS, спуфінг, фішинг та інші зловмисні дії, спрямовані на порушення конфіденційності, цілісності та доступності голосових комунікацій.

2. Проведено аналіз існуючих методів і засобів виявлення зловмисних повідомлень IP-телефонії. Детально розглянуто застосування методів штучного інтелекту, таких як машинне навчання (зокрема, методи класифікації та кластеризації) та глибоке навчання, які демонструють значний потенціал у розпізнаванні складних патернів аномальної поведінки та зловмисних повідомлень. Окрему увагу приділено методам виявлення нетипової поведінки при передачі голосу, що дозволяє ідентифікувати загрози, які не завжди підпадають під відомі сигнатури атак, базуючись на відхиленнях від нормального трафіку та поведінкових шаблонів користувачів. Виявлено, що, попри значні досягнення, існуючі підходи часто стикаються з проблемами масштабованості, високого рівня хибнопозитивних спрацьовувань та складності адаптації до нових типів атак.

3. Визначено перспективні шляхи розвитку предметної області та здійснено постановку задачі дослідження. Встановлено, що подальші дослідження повинні бути зосереджені на розробці та вдосконаленні гібридних методів, які комбінують сигнатурний аналіз з методами штучного інтелекту та аналізом поведінки для підвищення ефективності виявлення зловмисних повідомлень. Особлива увага має бути приділена розробці адаптивних систем, здатних до самонавчання та оперативного реагування на динамічно змінювані загрози. Це дозволить підвищити рівень безпеки та стійкості систем IP-телефонії до сучасних кіберзагроз.

РОЗДІЛ 2 ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ВИЯВЛЕННЯ ЗЛОВМИСНИХ ПОВІДОМЛЕНЬ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

2.1 Передумови розвитку методів виявлення зловмисних повідомлень IP-телефонії та імплементація онтологічного підходу

Використання VoIP на сьогодні дуже швидко розвивається і набуває все більшого значення у бізнесі та особистому користуванні. Це пов’язано насамперед із зміною тенденції та постійним розвитком VoIP технологій. На рисунку 2.1 представлено аналіз основних напрямків, які безпосередньо впливають на розвиток та використання сервісів VoIP.

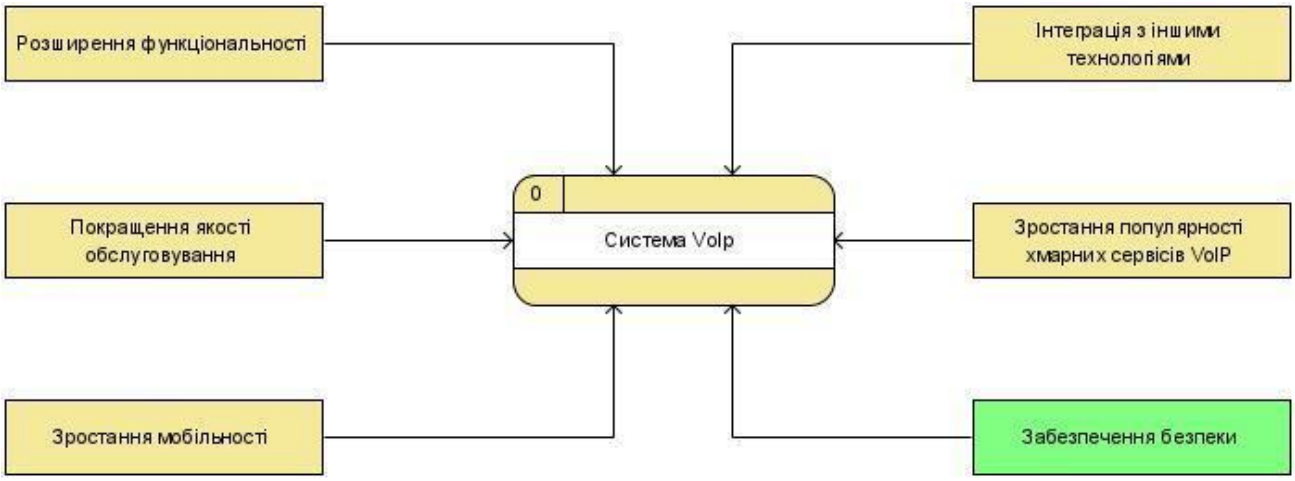


Рис. 2.1. Особливості розширення та використання VoIP технологій

Розглянемо ці напрямки детальніше. Зростання популярності хмарних сервісів VoIP серед бізнесу та окремих користувачів відбувається через їхню гнучкість, швидкість впровадження та економічність [89].

Завдяки постійному розвитку мережевих технологій та протоколів передачі даних, які використовуються в VoIP, якість голосу та зв'язку постійно покращується, що безпосередньо впливає на якість обслуговування.

Сучасні VoIP-системи надають широкий спектр додаткових функцій, таких як конференц-зв'язок, зміна голосу, відеодзвінки, інтеграція з CRM-системами [30, 31].

Зростання мобільності відбувається завдяки використанню мобільних додатків та можливість робити виклики через Інтернет з будь-якого місця. Це надає можливість мобільним користувачам доступу до VoIP-зв'язку незалежно від їхнього місця перебування.

Інтеграція з іншими технологіями – VoIP стає складовою частиною інтегрованих комунікаційних рішень, які включають в себе електронну пошту, чат, відеоконференції та інші засоби спілкування.

Особливо необхідно відзначити такий напрям, як забезпечення безпеки. Розвиток технологій шифрування, аутентифікації та контролю доступу допомагає забезпечити безпеку VoIP-зв'язку та захистити дані користувачів від несанкціонованого доступу та перехоплення. Підсумовуючи, необхідно відзначити, що розвиток VoIP відбувається швидкими темпами, відкриваючи нові можливості для спілкування та покращення бізнес-комунікацій, а напрямок забезпечення безпеки VoIP є особливо актуальним в сучасних умовах [32, 33].

Оскільки забезпечення безпеки функціонування VoIP є одним із ключових аспектів, які безпосередньо впливають на якість IP-телефонії та розширення сфер її використання, то проаналізуємо більш детально відомі методи та засоби, які використовуються для захисту інформації у VoIP (рисунок 2.2).

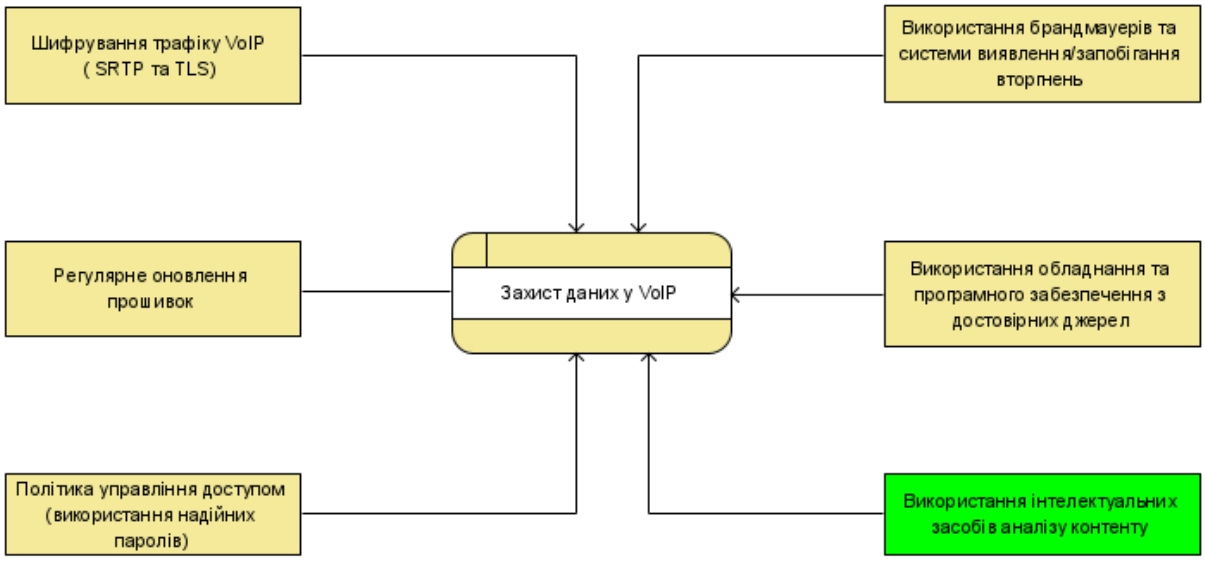


Рис. 2.2. Підходи до захисту інформації в системі VoIP

Системи VoIP вразливі до різних загроз безпеки, включаючи підслуховування, фішинг і атаки на відмову в обслуговуванні (DoS). Відомими підходами до зміцнення безпеки в IP-телефонії є наступні [34, 35]:

- шифрування трафіку VoIP за допомогою різних протоколів, таких як безпечний транспортний протокол реального часу (SRTP) і безпечний протокол транспортного рівня (TLS);
- ефективна політика управління доступом, що включає використання надійних паролей та контроль доступу, щоб запобігти несанкціонованому проникненню;
- регулярне оновлення прошивок та програмного забезпечення для виправлення вразливостей безпеки;
- використання брандмауерів та систем виявлення/запобігання вторгненням для захисту від кіберзагроз;
- використання обладнання та програмного забезпечення VoIP від перевірених постачальників, які дотримуються відповідних стандартів та протоколів;
- використання інтелектуальних засобів аналізу контенту.

З постійним розвитком технологій штучного інтелекту, особливо цікавим є напрямок використання інтелектуальних засобів для аналізу контенту в системі VoIP. Розглянемо основні сучасні підходи, які можна використовувати для аналізу VoIP контенту (рисунок 2.3).

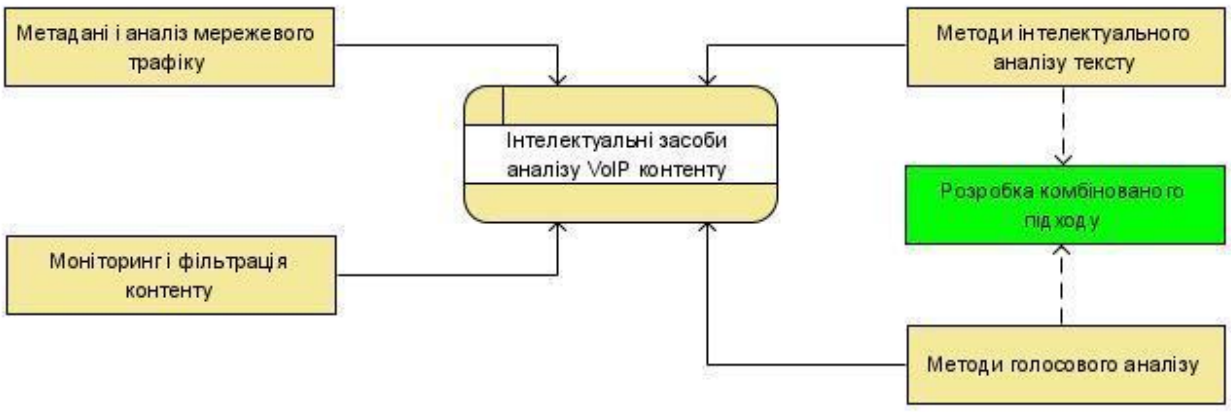


Рис. 2.3. Підходи до інтелектуального аналізу контенту в системі VoIP

Використання алгоритмів машинного навчання та обробки природної мови (NLP) для сканування тексту VoIP-повідомлень на ключові слова, фрази або семантичні зв'язки дозволяють знаходити інформацію, яка носить зловмисний характер. Використання методів та спеціалізованого програмного забезпечення для голосового аналізу допомагає визначати специфічні звуки, мовні ознаки або відтінки, що характеризують пропаганду чи загрози. Дослідження метаданих VoIP-повідомлень, таких як IP-адреси, час і тривалість дзвінка, здійснюється для виявлення аномалій або звичайних патернів, що можуть вказувати на можливу злочинну діяльність. Моніторинг і фільтрація контенту у поєднанні з використанням спеціалізованого програмного забезпечення для моніторингу та фільтрації VoIP-повідомлень на основі заздалегідь визначених критеріїв. Використання інформації з аналізу для формування блеклистів IP-адрес, номерів телефонів чи інших ідентифікаторів, а також для виявлення повторюваних патернів комунікацій, які можуть вказувати на злочинну діяльність.

Важливо відзначити, що ефективність аналізу VoIP-повідомлень (як голосових, так і текстових) на вміст злочинної інформації може залежати від комбінації цих методів та технологій, а також від постійного вдосконалення і адаптації до нових загроз.

Особливо актуальним є розвиток методів аналізу мовлення та відповідної обробки природної мови, який дозволяє створювати більш точні та ефективні системи виявлення аномального трафіку та потенційно небезпечних комунікацій. Метою є розробка онтологічної моделі [26, 27] функціонування IP-телефонії, та методу автоматизованого наповнення онтології тематичних повідомлень в корпоративній мережі, і методу виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень для покращення безпеки використання VoIP.

2.2 Онтологічна модель функціонування IP-телефонії

Створення онтології функціонування VoIP вимагає співпраці між експертами в предметній області, інженерами та дослідниками, які знайомі з

технологіями, стандартами та найкращими підходами до організації VoIP. Така онтологія сприятиме полегшенню взаємодії, семантичній інтеграції та допомагатиме в системному проектуванні, управлінні, виправленні несправностей, а також сприятиме покращенню системи захисту інформації в VoIP.

Онтологія даної предметної області формується на основі структурованого представлення концептів, сутностей, зв'язків у сфері технології VoIP. Вона дозволить отримати формалізовану та семантично насичену структуру для розуміння та представлення знань про протоколи, компоненти та їх взаємодію.

Онтологія VoIP повинна включати [39-41]:

- поняття та сутності: стек протоколів VoIP, представлення багаторівневої архітектури протоколів VoIP, включаючи такі протоколи, як SIP (протокол ініціації сеансу), RTP (транспортний протокол реального часу), SDP (протокол опису сеансу) та інші; компоненти VoIP: об'єкти, залучені до зв'язку VoIP, такі як користувацькі додатки (мобільні телефони з додатками, IP-телефони), шлюзи VoIP, проксі-сервери, реєстратори та медіа-сервери; опис життєвого циклу VoIP виклику: представлення різних етапів VoIP виклику, включаючи встановлення виклику, узгодження, розрив виклику та систему управління викликом;
- відношення: комунікаційні зв'язки: зв'язки між об'єктами VoIP, такі як зв'язок користувач-користувач, зв'язок користувач-сервер, зв'язок сервер-сервер і зв'язок медіа-потоку; відношення залежностей між компонентами та протоколами VoIP, такі як залежність SIP від базових транспортних протоколів, таких як UDP або TCP, і залежність RTP від RTCP для зворотного зв'язку та управління;
- властивості та атрибути: властивості протоколу VoIP, такі як формати повідомлень, заголовки, методи, параметри та коди стану, визначені SIP, RTP та іншими відповідними протоколами; атрибути компонентів: атрибути компонентів VoIP, наприклад IP-адреси, порти, кодеки, підтримувані функції, можливості та конфігурації; події VoIP: події, пов'язані зі зв'язком VoIP, такі як ініціювання виклику, завершення виклику, утримання/відновлення виклику,

переадресація виклику, переадресація виклику та події медіапотоку; дії: дії, які виконують об’єкти VoIP у відповідь на події, такі як надсилання SIP-повідомлень, узгодження параметрів медіа, встановлення та розрив медіа-сеансів і обробка сигналів управління викликами;

- ієрархічна таксономія: класифікація об’єктів і протоколів VoIP в ієрархічні таксономії на основі їхніх ролей, функцій і зв’язків; категоризація технологій VoIP на основі моделей розгортання (локальні, хмарні), мережевих архітектур (однорангові, клієнт-сервер) і сценаріїв використання (корпоративні VoIP, мобільний VoIP);
- семантичні обмеження: обмеження на зв’язки та взаємодію між об’єктами VoIP, що забезпечують узгодженість в онтології; правила протоколу: правила, що регулюють поведінку та використання протоколів VoIP, включаючи правила обробки повідомлень, встановлення сеансу та узгодження медіа для окремих протоколів.

При побудові онтології опису VoIP повідомлень в системі IP-телефонії необхідно здійснити формалізацію основних понять у формі окремих концептів та описати зв’язки між цими поняттями. Розробка онтології для повідомлень VoIP передбачає створення структурованого представлення концептів, сутностей та зв’язків у межах відповідного домену [41, 42]. На рисунку 2.4 представлено онтологічний граф для формалізованого опису VoIP повідомлень.

На першому етапі здійснюємо ідентифікацію домену, яка включає визначення області та меж описуваної онтології. У нашому випадку це буде зв’язок за протоколом передачі голосових повідомлень через Інтернет (VoIP), що охоплює концепції, пов’язані з передачею голосових даних через IP-мережі [43].

На другому етапі визначаємо основні поняття та сутності, які пов’язані з VoIP повідомленнями:

- протоколи VoIP (SIP, RTP, RTCP);
- компоненти VoIP (клієнт VoIP, сервер VoIP, шлюз VoIP);
- типи повідомлень VoIP (пакети INVITE, ACK, BYE, RTP);

- параметри VoIP (IP-адреса клієнта, IP-адреса призначення, номери портів, тип корисного навантаження);

- повідомлення (голосові та текстові), текстові повідомлення характеризуються основної частиною, автором, переліком ключових слів, оцінкою та комбінаційним представленням.

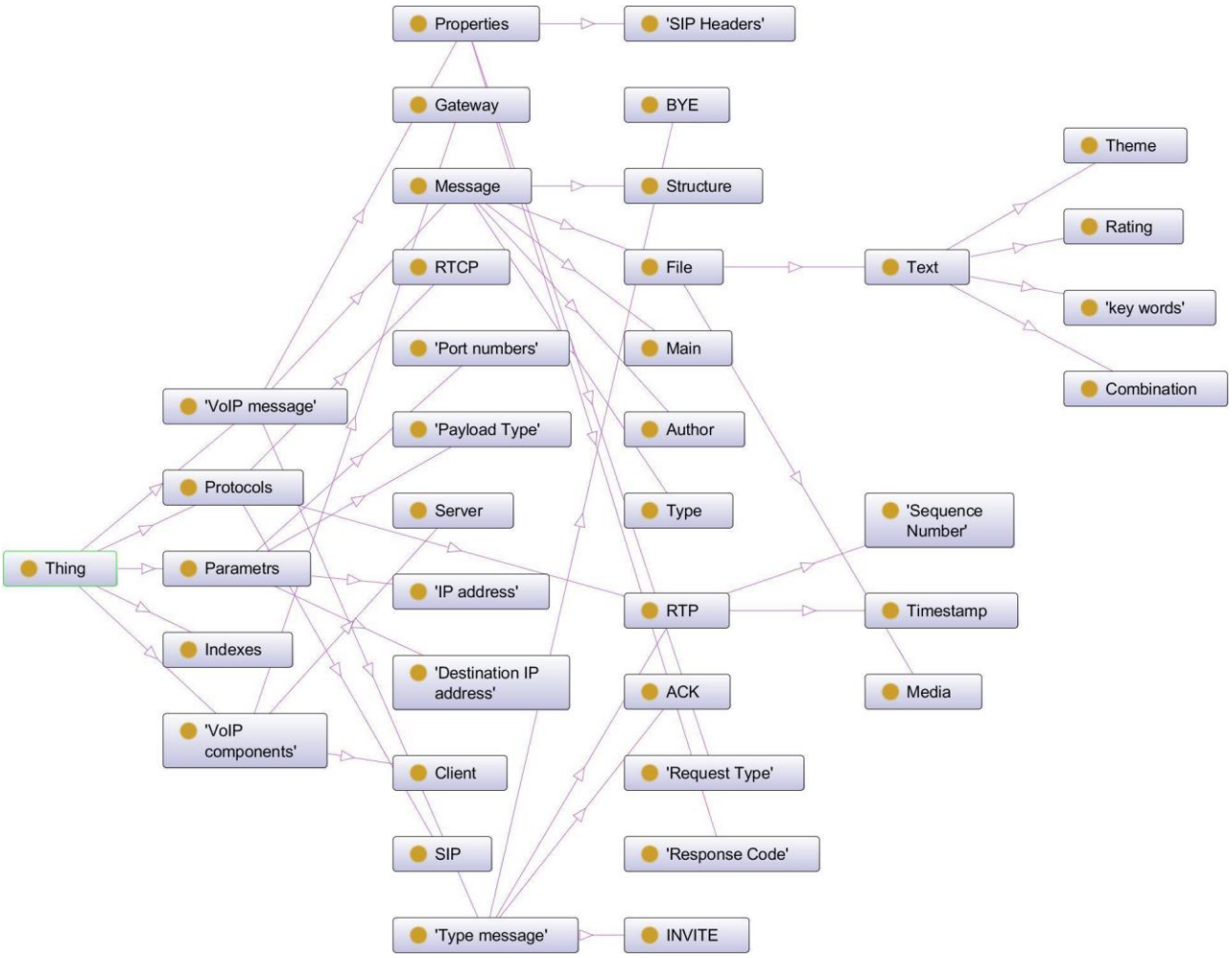


Рис. 2.4. Представлення формалізованої предметної області «VoIP повідомлення» у вигляді онтологічного графу

На третьому етапі формуємо опис ієрархічних зв’язків та будуємо таксономію класів, наприклад: протоколи VoIP (SIP, RTP, RTCP), компоненти VoIP (клієнт, сервер, шлюз). Будуємо відповідні відношення між класами, тобто визначаємо відношення між різними поняттями. Цей процес може включати такі

зв’язки «є» (успадкування), «частина» (композиція), «має» (асоціація) тощо. Наприклад:

- клієнт VoIP має сеанс SIP;
- пакет RTP є типом пакета даних VoIP;
- сервер VoIP є частиною інфраструктури VoIP.

На четвертому етапі визначаємо властивості та атрибути, пов’язані з кожним поняттям. Вони представляють характеристики або ознаки, які їх описують. Наприклад, SIP-повідомлення має наступні атрибути:

- тип запиту (ACK, BYE);
- код відповіді (200 OK, 404 Not Found);
- заголовки SIP (Call-ID);
- порядковий номер;
- мітка часу.

На п’ятому етапі формуємо систему правил та обмеження для забезпечення узгодженості онтології. Це може включати обмеження відповідності правил домену предметної області, обмеження типів даних.

Заключний етапом є перевірка онтології на реальних сценаріях VoIP, яка включає перевірку адекватності відношення до домену і відповідності до вимог практичного використання.

2.3 Метод автоматизованого наповнення онтології тематичних повідомлень в корпоративній мережі

Згідно [28], онтологія описується деревоподібною системою концептів досліджуваної предметної області. Під концептами предметної області розуміються як базові поняття, так і узагальнюючі поняття, які часто є спільними у багатьох суміжних предметних областях. Онтологію для VoIP можна змоделювати деякою деревовидною структурою наступного виду

$$OC\_Voip =< IdConcept, ParentConcept, Base >, \quad (2.1)$$

де $IdConcept$ - ідентифікатор концепту;

$ParentConcept$ - ідентифікатор батьківського концепту;

$Base$ - атрибут, який використовується для розмежування базових понять від узагальнюючих понять.

Базове поняття відрізняється від узагальнюючого тим, що узагальнюючі поняття не мають посилання на батьківський елемент, тобто $ParentConcept = 0$. Кожне поняття може описуватися деякими лінгвістичними представленнями у вигляді OC_Prs словосполучень. Онтологічні поняття описуються конкретними словоформами OC_Form , а також основами OC_Base цих понять. Словоформи можуть використовуватися для опису понять для користувачів, а основи понять – для автоматичного визначення еквівалентності представлень відповідно до вибраної мови. Атрибути таких понять групуємо в структури:

$$OC\_Base =< IdLanguage, IdBase, WordBase >, \quad (2.2)$$

$$OC\_Form =< IdLanguage, IdForm, IdBase, WordForm >, \quad (2.3)$$

$$OC_{Prs} =< IdConcept, IdLanguage, IdPhrase, IdBase, IdForm, IdParentBase >, \quad (2.4)$$

де $IdLanguage$ - ідентифікатор мови;

$IdBase$ - ідентифікатор визначеної основи слова;

$WordBase$ - визначена основа слова;

$IdForm$ - ідентифікатор визначеної форми слова;

$WordForm$ - визначена словоформа;

$IdConcept$ - ідентифікатор аналізованого концепту;

$IdPhrase$ - ідентифікатор аналізованої фрази;

$IdParentBase$ - ідентифікатор основи поняття, що належить до батьківської категорії.

Для наповнення онтології VoIP можна використовувати:

– аналіз предметної області VoIP, включаючи протоколи, компоненти систем, типи повідомлень, характеристики зв'язку тощо;

– термінологічні словники, які використовуються у VoIP. Це включає технічні терміни, абревіатури, назви протоколів тощо;

– стандарти та специфікації VoIP, такі як SIP (Session Initiation Protocol), RTP (Real-time Transport Protocol), SDP (Session Description Protocol) тощо. Ці документи надають інформацію про протоколи, повідомлення, функції та інші аспекти VoIP;

– інформацію, що опублікована у відкритому доступі, таку як повідомлення в тематичних групах в соціальних мережах, форуми, вікі, які можуть містити корисні відомості про проблеми, вирішення, нові можливості розвитку в галузі VoIP;

– співпрацю з експертами у галузі VoIP, такими як інженери, адміністратори мереж, дослідники, які можуть допомогти у розумінні складних питань;

– програмне засоби VoIP, такі як Asterisk, FreeSWITCH, Kamailio, які містять документацію, код та інші ресурси, які можна використовувати для розуміння архітектури та принципів роботи VoIP;

– для формування бази тематичних медіа-повідомлень, можна також використовувати спеціальні записи з медіа-ресурсів (Youtube, Tiktok, тощо) [12].

Для пошуку та вибірки структурованої інформації, яка відноситься до аналізованої предметної області, формуємо множину $KeyConSet$, що містить ключові поняття, які характеризують її визначення та поведінку. Для аналізу структури VoIP повідомлень визначимо деяку допоміжну множину $AdvSet$:

$$AdvSet =< IdMessAn, IdListElem, IdElement, IdBase, IdForm, IdParentBase >, \quad (2.5)$$

де $IdMessAn$ – ідентифікатор аналізованого повідомлення;

$IdListElem$ – ідентифікатор набору всіх понять;

$IdElement$ – ідентифікатор окремого елемента набору.

Аналіз повторюваних понять дозволяє визначити найбільш значущі поняття і відокремити їх від несуттєвих понять. Для аналізу та контролю важливих понять використаємо деяку структуру $BaseFr$ частот основ:

$$BaseFr =< IdBase, BsFreq, IdLastMess, ConBack >, \quad (2.6)$$

де $IdBase$ – ідентифікатор основи, $BsFreq$ – частота появи основи в різних повідомленнях, $IdLastMess$ - ідентифікатор останнього повідомлення, де була основа поняття, $ConBack$ – відмітка фоновості поняття, що приймає $NULL$ значення за замовчуванням при деякій невизначеності.

При аналізі набору текстових повідомлень, які згруповані за відповідним критерієм, встановлюємо деякий ідентифікатор такого набору:

$$CurrMessId := \left(\pi_{IdLastMess}(BaseFr)\right) + 1. \quad (2.7)$$

Аналізовані елементи сформованої множини розбиваємо на набір елементарних понять із використанням роздільників, списки розбиваються на елементарні поняття $ElemCon$ із використанням роздільників.

До частин елементарного поняття необхідно застосувати процедуру $BaseConcept$ для формування їх основ. Ця процедура реалізовується шляхом відсікання закінчень від слів. При умові, що

$$BaseConcept(ElemCon_{Mess,List}) \subset BaseConcept(KeyConSet), \quad (2.8)$$

всі елементарні поняття з аналізованої множини з відповідними атрибутами додаємо в визначену структуру $AdvSet$. Словоформи вибираємо з елементів списку $ElemCon_{Mess,List}$ і розпізнаємо за допомогою відношення OC_Form або поповнюємо його.

Нехай $Word_k(ElemCon_{Mess,List})$ – k – те слово, яке відокремлене із елемента списку $ElemCon_{Mess,List}$. Якщо основа слова вже існує в аналізованій множині, то цей ідентифікатор $IdBaseWord$ визначаємо з відношення OC_Base:

$$IdBaseWord =$$

$$= \pi_{IdBase}\left(\sigma_{WordBase=BaseConcept(Word_k(ElemCon_{Mess,List}))}(OC\_Base)\right). \quad (2.9)$$

Якщо основа слова вже знаходиться у відношенні $BaseFr$ і номер аналізованого повідомлення не співпадає із номером зарахованого на попередньому кроці, то частотний індекс $BsFreq$ збільшуємо на 1, а номер поточного повідомлення заноситься в поле $IdLastMess$:

$$\left(Count\left(\pi_{IdBase}\left(\sigma_{IdBase=IdBaseWord\ AND\ IdLastMess<>CurrMessId}(BaseFr)\right)\right) \neq 0\right)$$
$$\Rightarrow (BaseFr.BsFreq \coloneqq BaseFr.BsFreq + 1) \wedge$$
$$\wedge (BaseFr.IdLastMess := CurrMessId). \quad (2.10)$$

Такий підхід забезпечує врахування частот використання основ у різних повідомленнях. Коли основа у відношенні $BaseFr$ не знайдена, її враховуємо з частотним індексом, який рівний 1, та додаємо у відношення, а також враховуємо номеру поточного повідомлення:

$$\left(Count\left(\pi_{IdBase}\left(\sigma_{IdBase=IdBaseWord}(BaseFr)\right)\right) = 0\right) \Rightarrow$$
$$\Rightarrow (BaseFr.IdBase \coloneqq IdBaseWord) \wedge (BaseFr.BsFreq \coloneqq 1) \wedge$$
$$\wedge (BaseFr.IdLastMess := CurrMessId). \quad (2.11)$$

Якщо основа $Word_k(ElemCon_{Mess,List})$ не визначена, то вона додається у список основ, слово додається в множину словоформ, а відношення часто визначається на основі (2.11).

Для додавання поняття в онтологію експерту із знанням предметної області у IP-телефонії пропонуються тільки основи з частотою, яка більша за визначене мінімальне значення $BaseFr_0 \geq 2$, яке вибирається користувачем. Експерт із запропонованого списку основ здійснює вибір і включення в онтологію, коли дану умову задовольняє не менше $BaseFr_0$ основ

$$Count\left(\pi_{IdBase}\left(\sigma_{BaseFr>=BaseFr_0}(BaseFr)\right)\right) > BaseFr_0. \quad (2.12)$$

В процесі прийняття відповідного рішення, основи відображаються лише з контексту аналізованих повідомлень. Це дозволяє формувати поняття з кількох слів і не повторювати основи, які не обрані спеціалістом для включення в онтологію. Основу для контексту $ContextBase$ вибираємо виходячи із критерію максимальної частоти $MaxBsFreq$:

$$MaxBsFreq = \left(\pi_{BsFreq}(\sigma_{ConBack=Null})\right), \quad (2.13)$$

$$ContextBase = rand\left(\pi_{IdBase}\left(\sigma_{BsFreq=MaxBsFreq}\right)\right). \quad (2.14)$$

Формування контексту визначеної основи здійснюється із використанням двовимірного масиву $ArrayCont$, який містить словоформні ідентифікатори. Перший індекс характеризує номер фрази в контексті, а інший – ідентифікатор номера слова у фразі. $NumbPhrCont$ – показник, який характеризує кількість фраз контексту:

$$NumbPhrCont = count\left(\pi_{IdElement}\left(\sigma_{IdBase=CBase}(AdvSet)\right)\right). \quad (2.15)$$

Ідентифікатори усіх елементів з аналізованої структури заносимо в сформований масив $AdvPhrId$, який носить допоміжний характер:

$$AdvPhrId = \pi_{IdElement}\left(\sigma_{IdBase=CBase}(AdvSet)\right) \quad (2.16)$$

розмірності $NumbPhrCont$. І-та стрічка даного контекстного масиву визначається за наступним правилом:

$$AdvContext[i] =$$

$$= \left(\pi_{IdForm}\left(\sigma_{\substack{IdElement=AdvPhrN[i]\wedge \\ \wedge IdParentBase=NULL}}(AdvSet)\right) AS\ HeadLine\right) \cup$$

$$\cup$$

$$\left(\pi_{IdForm}\left(\sigma_{\substack{IdElement=AdvPhrN[i]\wedge \\ \wedge\left(\substack{IdParentBase= \\ =HeadLine.IdBase\ OR\ IdParentBase= \\ =HeadLine.IdBase}\right)}}(AdvSet)\right) AS\ HeadLine_1\right) \quad (2.17)$$

Сформований набір словоформ представляється спеціалістові в галузі VoIP та відповідної досліджуваної предметної області для формування елементів, які будуть поповнювати онтологію. Основи, які потрапляють в онтологію, отримують фоновий показник $ConBack := 2$, щоб уникнути процедур повторного аналізу. Основи, які не використовувалися жодного разу, не можуть формувати контекстні основи, і для них показник $ConBack := 1$. Вибрані елементи, які використовуються для онтологічного наповнення, можуть формувати онтологічну ієрархію, яка дозволяє формалізувати експертні знання у формі онтології.

2.4 Метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень

Для аналізу VoIP контенту необхідно формалізувати метод побудови базового повідомлення в IP-телефонії. Для цього необхідно спочатку здійснити перетворення VoIP медіа повідомлення в текстове представлення і таким чином сформувати базу даних вже текстових повідомлень.

Для перетворення голосового повідомлення в текстове використаємо бібліотеки SpeechRecognition для перетворення голосу в текст у мові програмування Python. Фрагмент лістингу програми такого перетворення представлено на рисунку 2.5.

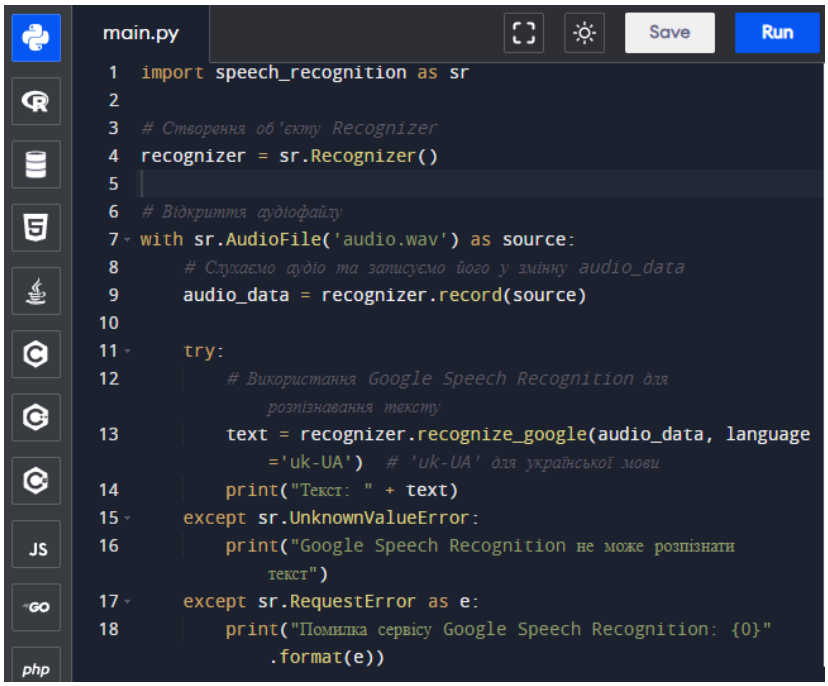


Рис. 2.5. Фрагмент лістингу програмного коду для перетворення VoIP медіа повідомлення в текстове представлення

Тематику таких повідомлень задаємо загальним текстовим ідентифікатором IMP предметної області та відповідним специфікатором SM. За допомогою перетворення голосового повідомлення у текстове представлення та процедури символьної конкатенації $VPS = \text{I}MP \,\&\, SM$ отримаємо множину VP текстових повідомлень, які представлені наборами відповідних компонентів конкретних понять

$$VP(VPS, P) = \{VP_i\}_{i=1}^{P}, \tag{2.18}$$

де P – потужність множини VP ;

VP_i – елемент множини, що визначає набір понять i - того повідомлення.

На наступному кроці для аналізу понять повідомлень використовуємо лише ті поняття, які відносяться до аналізованої предметної області, тобто належать множині VPK, а не здійснюємо повну перевірку усієї множини понять. Критерієм виконання такої умови є наявність ідентифікатора предметної області в темі повідомлення:

$$VPK = \{VP_{i*}^{*} | VP_{i*} \in VP, VP_{i*}.theme \cap \mathrm{I}MP \neq \emptyset\}_{i=1}^{P*}. \quad (2.19)$$

Із набору текстових тверджень необхідно вибрати інформацію, яка визначає тематику повідомлень. У першу чергу, інформація про тематику повідомлення визначається у наборі тверджень, з яких починається повідомлення.

Якщо початок повідомлення не дозволяє визначити його тематику, то інформацію про тематику вибираємо з впорядкованої множини елементів на основі частотного аналізу понять. Інформація такого типу буде впорядкованим списком $LKB(VP_i^*)$ виділених ключових понять:

$$LKB(VP_i^*) =< C_{ik}(VP_i^*) >_{k=1}^{CPi}. \quad (2.20)$$

Така множина може містити також і випадкову інформацію. Однак елементи множини понять, які будуть повторюватися, дають нам інформацію про структуру і тематику такого повідомлення. Тому на основі впорядкованої множини та множини ключових понять сформуємо базову BCM та узагальнену GCM множини пар поняття - частота появи поняття, які визначаємо наступним чином:

$$BCM = \{(CS_l, NCS_l) | CS_l\}, \quad (2.21)$$

$$GCM = \left\{(CS_m, NCS_m) | CS_m \in \bigcup_i LKB(VP_i^*)\right\} \quad (2.22)$$

Для знаходження понять, які будуть релевантними до заданої предметної області, впорядкуємо елементи множини GCM у порядку спадання відповідних

частот елементів, а деяку частину понять включаємо відразу в базову концептуальну множину CSC

$$CSC = \left\{(CS_l, NCS_l) | FCL_l = \frac{NCS_l}{P^*} > FF_0\right\}, \quad (2.23)$$

де величина FF_0 належить інтервалу [0.200; 0.500], а конкретне значення цієї величини вибираємо із врахуванням особливостей та специфіки предметної області.

Далі аналізуємо множину понять, які мають низьку частоту, такий аналіз доцільний, якщо нам не вдалося наповнити множину понять на основі відношення (2.6). Розглянемо деяку визначену і впорядковану вибірку SCMF, яка також включає відповідні частоти понять у повідомленні:

$$SCMF = \{NCS_l | (CS_l, NCS_l) \in BCM\}. \quad (2.24)$$

Частоти з найвищими значеннями перевіряємо за критерієм 4σ на характеристику аномальності. Концепти, що відповідають критерію аномальності, включаємо в сформовану множину CSC.

При формуванні множини SK ключових концептів, що визначають тематику повідомлення, здійснюємо впорядкування цієї множини. Рангові номери присвоюємо лише ключовим концептам. Так CRC_{ik} позначає ранг k-го концепту в і-тому повідомленні. При аналізі повідомлень необхідно також врахувати вплив тривалості голосового повідомлення (довжини перетвореного в текст повідомлення) на предметну аудиторію, оскільки є багато повідомлень, які є короткотривалими. Для того, щоб врахувати таку особливість, використаємо деяку вагову функцію $wcs(i)$.

Оскільки із спаданням тривалості голосових повідомлень їх важливість також буде плавно спадати, то чим коротше повідомлення, тим швидше відбуватиметься це спадання. Для моделювання такого процесу можна використати кубічний сплайн. Для його однозначного визначення необхідно

накласти хоча б чотири умови. Зокрема, найтриваліше повідомлення буде мати важливість для цього аргументу рівну 1, якщо похідна дорівнює 0. Вводимо систему ваг $CSG(i) = \frac{csg(i)}{\sum_i \quad csg(i)}$, яка матиме нормований характер та обчислюємо усереднений ранг k-го концепту наступним співвідношенням:

$$RA_k = \sum_i \quad R_{ik} CSG(i). \tag{2.25}$$

Ранжування концептів здійснюємо на основі усереднення рангів. Узгодженість рангів перевіряємо із використанням коефіцієнта конкордації [35]:

$$CSW = \frac{12 \sum_{k=1}^{K} \quad \left(\sum_{i=1}^{I} \quad R_{ik} CSG(i) - \bar{R}\right)}{I^2 (K^3 - K)}, \tag{2.26}$$

де $\bar{R} = \frac{1}{K} \sum_{k=1}^{K} \quad \sum_{i=1}^{I} \quad R_{ik} CSG(i).$

Якщо виконується наступна умова

$$I(K-1)CSW > \chi^2_{K-1,\alpha} \quad , \tag{2.27}$$

то таке ранжування є значущим [35].

Якщо ранжування повного списку концептів не є значущим, то відкидаємо один елемент із списку в порядку зростання відповідних ваг. Відкидання проводимо до отримання значущого ранжування, починаючи із концепту, який матиме найменшу вагу.

Запропонований метод дозволяє згрупувати повідомлення відповідно до класифікованої структури ключових понять. Таке групування доцільно використовувати для виявлення аномальних повідомлень в спеціалізованій корпоративній мережі з розгорнутою системою IP-телефонії.

Висновки до розділу 2

1. Обґрунтовано доцільність використання методів аналізу мовлення та відповідної обробки природної мови, які дозволяють створювати більш точні та ефективні системи виявлення аномального трафіку та потенційно небезпечних комунікацій в системі VoIP.

2. Виділено напрямок використання інтелектуальних засобів для аналізу контенту в системі VoIP. Запропоновано онтологію опису VoIP повідомлень в системі IP-телефонії, здійснено формалізацію основних понять у формі окремих концептів та описано зв’язки між цими поняттями.

3. Запропоновано метод виявлення аномалій в трафіку IP-телефонії на основі групування VoIP повідомлень, який, на відміну від існуючих, ґрунтується на поєднанні знання-орієнтованого підходу з використанням онтології та контекстно-частотного аналізу.

4. Запропоновано метод автоматизованого наповнення онтології тематичних повідомлень в корпоративній системі IP-телефонії, який ґрунтується на формалізованому представленні повідомлень за допомогою деревовидних структур та на описі операцій взаємодії засобами алгебри кортежів.

5. Здійснено програмну реалізацію перетворення голосових повідомлень в текстові представлення з використанням бібліотеки SpeechRecognition для перетворення голосу в текст у мові програмування Python. Проведено експериментальні дослідження запропонованих підходів, імплементовано програмну підсистему виявлення аномальних повідомлень на основі онтологічного підходу в діючу корпоративну IP-телефонію.

РОЗДІЛ 3 АРХІТЕКТУРА ІНТЕЛЕКТУАЛІЗОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ЗЛОВМИСНИХ ПОВІДОМЛЕНЬ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

3.1 Узагальнена структура інтелектуалізованої системи

На основі проведеного вище аналізу і з врахуванням рішень [18, 23, 48] запропоновано узагальнену структуру інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі (рис 3.1), серцевиною якої є п’ять базових підсистем [84]:

- підсистема моніторингу трафіку;
- підсистема розподілу доступу;
- підсистема аналізу;
- підсистема прийняття рішень;
- підсистема звітності та аналітики.

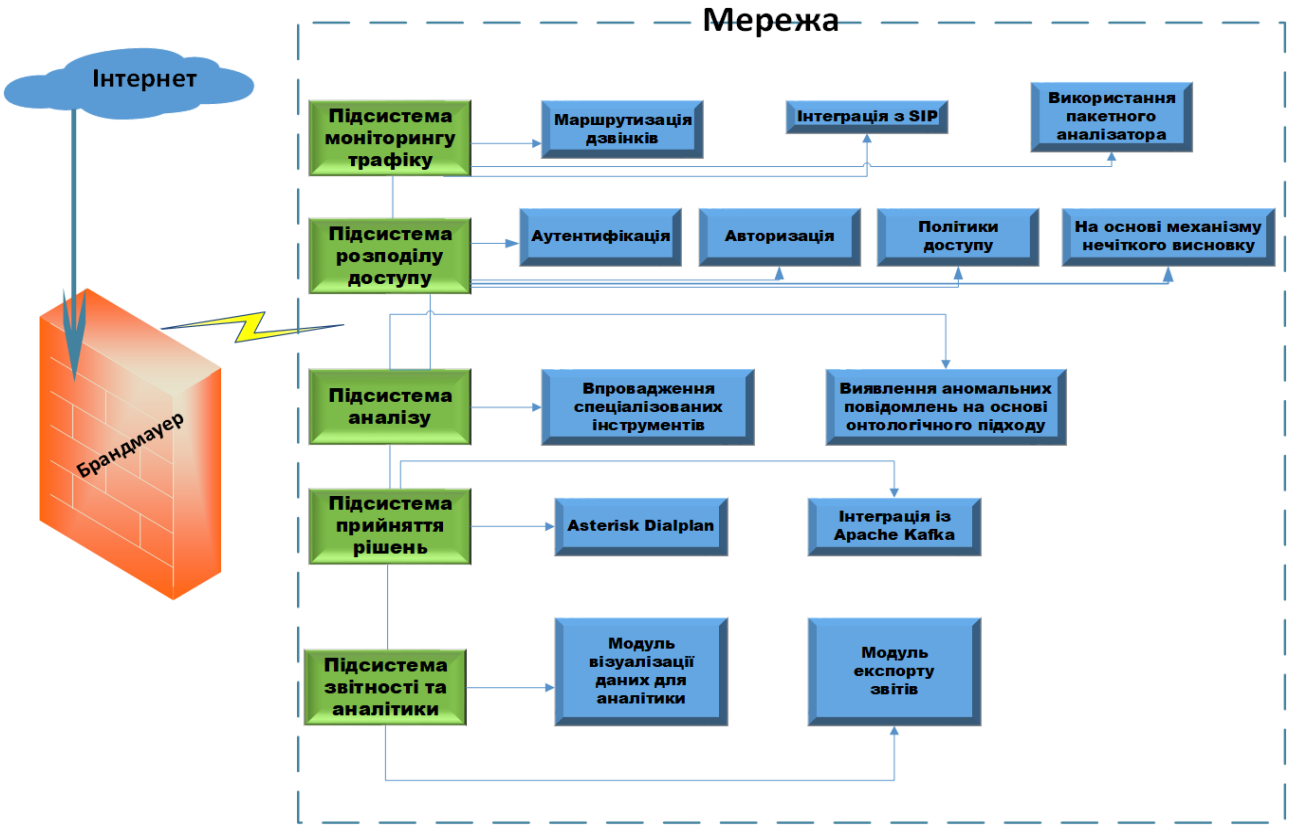


Рис.3.1. Узагальнена структура інтелектуалізованої системи безпеки використання IP-телефонії в корпоративній мережі

3.1.1 Підсистеми узагальненої структури інтелектуалізованої системи

Підсистема розподілу доступу.

Для розподілу доступу в IP-телефонії варто здійснювати аналіз клієнта, який здійснює дзвінок. Зокрема його можна ідентифікувати за IP-адресою клієнта, за якою здійснюється дзвінок. Якщо ця IP-адреса є відомою системі, то може надаватися вищий рівень доступу, аніж для нової. Критерієм може також бути час здійснення дзвінка клієнтом та часовий пояс адресата дзвінка. Наприклад, якщо дзвінок здійснюється у неробочий час або часовий пояс адресата свідчить про його неробочий час, то система може відмовити у доступі, оскільки висока імовірність здійснення особистих дзвінків. Ще одним критерієм успішного здійснення дзвінка є поточна якість зв'язку мережі клієнта. Якщо якість зв'язку є низькою, то система може відмовити у здійсненні дзвінка. Кожен з цих критеріїв задається нечітко, оскільки задаються адміністратором системи. Тому для захисту IP-телефонії необхідно застосувати апарат нечіткої логіки, що дозволить здійснювати розподіл доступу в режимі реального часу та легко масштабувати систему захисту.

На рисунку 3.2 наведена схема розподілу доступу клієнтів до мережі IP-телефонії на основі нечіткої логіки. Схема є узагальненою і може бути адаптована під конкретні вимоги та інфраструктуру.

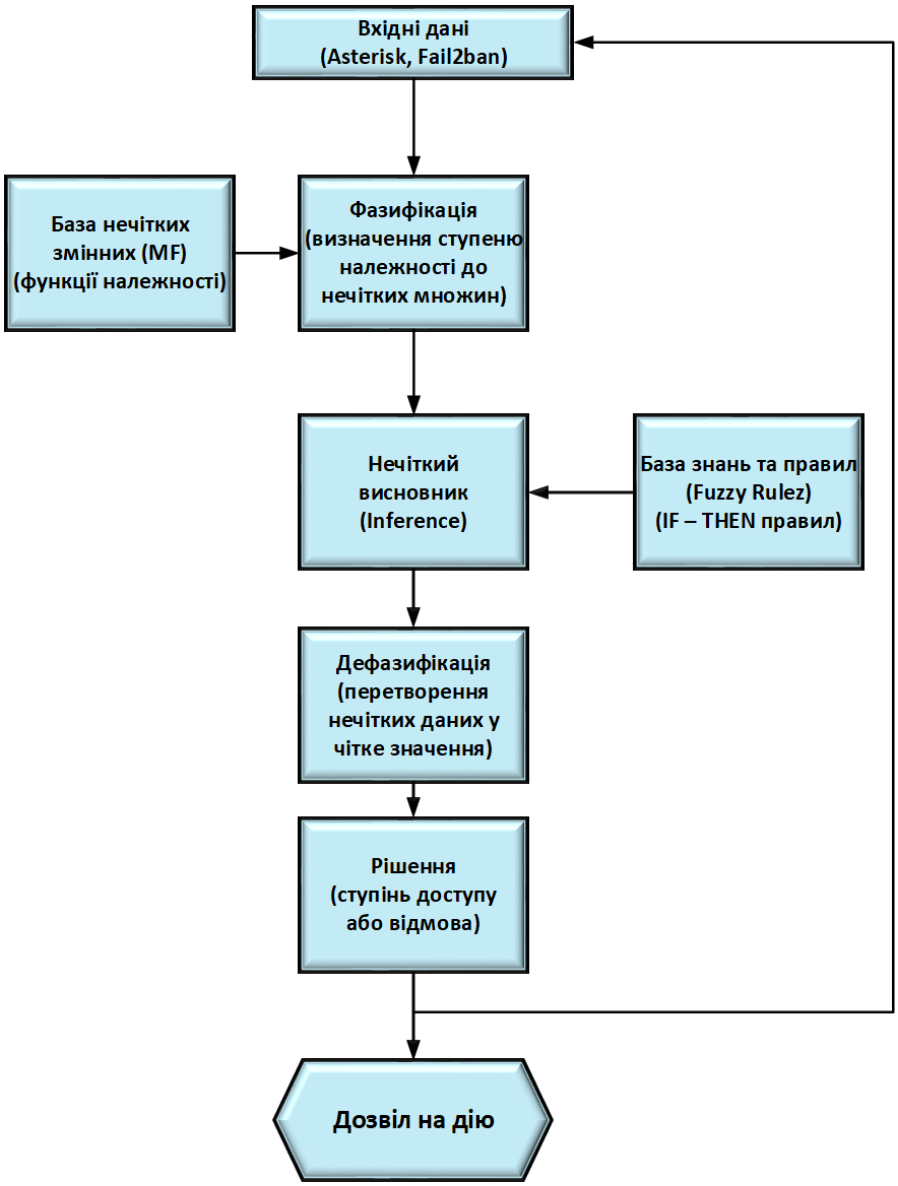


Рис. 3.2. Схема розподілу доступу клієнтів до мережі IP-телефонії на основі нечіткої логіки

Опис основних компонентів та їх функцій:

1. Вхідні дані: різноманітні атрибути, наприклад:
   - атрибути користувача: роль, група, рівень довіри, історія доступу;
   - атрибути ресурсу: класифікація даних (конфіденційність, критичність), вимоги до рівня захисту;
   - контекст середовища: час доби, місце розташування користувача, поточна завантаженість системи, рівень загрози (активність атак, інцидентів безпеки) тощо.

2. База нечітких змінних (функції належності): зберігаються визначення нечітких множин для кожної змінної. Наприклад, для змінної “Час доби” можуть бути множини “Ранок”, “Робочий час”, “Ніч”, кожна з яких має свою функцію належності (трикутна, трапецієподібна, гауссівська тощо).

3. Фазифікація: в даному блоці чіткі (кількісні або логічні) значення вхідних атрибутів перетворюються в нечіткі змінні за допомогою функцій належності. Наприклад, “Рівень загрози = 7 за шкалою від 0 до 10” може бути переведено в нечітке поняття “Висока загроза” з певним ступенем належності 0.8.

4. Нечіткий висновок: застосовує правила з бази знань до фазифікованих вхідних даних. На цьому етапі кожне правило оцінюється, обчислюється нечітке значення вихідної змінної (наприклад, “Рівень доступу”) шляхом об’єднання результатів застосування всіх релевантних правил. Тут використовуються операції мінімуму, максимуму або t-норм/ t-конорм залежно від логічних зв’язок.

5. База знань та правил: містить набір експертно визначених правил виду “Якщо [Умова1] І [Умова2] І …, тоді [Рівень доступу = середній/високий/низький]”. Наприклад: “Якщо (Користувач = високий рівень довіри) І (Ресурс = середня конфіденційність) І (Загроза = низька), тоді Рівень доступу = високий.”

“Якщо (Користувач = низький рівень довіри) АБО (Загроза = висока), тоді Рівень доступу = низький.”

6. Дефазифікація: отримані після inference нечіткі оцінки рівня доступу перетворюються у чітке значення, наприклад, числове значення від 0 до 100, або конкретний рівень (“Доступ дозволено”, “Обмежений доступ”, “Доступ заборонено”). Можуть бути використані різні методи дефазифікації (центр ваги, метод найбільшого максимуму тощо).

7. Рішення: на основі дефазифікованого значення приймається остаточне управлінське рішення: надати повний доступ, частково обмежити права, вимагати додаткову аутентифікацію чи повністю заборонити доступ. Це

рішення надсилається до системи контролю доступу (наприклад, системи керування правами, міжмережевих екранів, систем авторизації ресурсів).

Підсистема функціонує наступним чином:

–зовнішні параметри (користувач, ресурс, контекст) надходять до системи;

–вони перетворюються у нечітку форму;

–нечітка логіка, використовуючи правила та функції належності, виводить рівень доступу;

–отриманий результат знову переводиться у чіткий формат, після чого система визначає, чи надати доступ, обмежити його або заборонити.

Такий підхід дозволяє більш гнучко реагувати на складні контекстні ситуації, ніж традиційні чіткі моделі доступу.

Підсистема розподілу доступу клієнтів до мережі IP-телефонії дозволяє інтегрувати інтелектуальні механізми адаптації доступу до динамічних умов середовища, зменшуючи ризики помилкових рішень та підвищуючи ефективність систем безпеки.

Підсистема моніторингу трафіка

Відповідає за маршрутизацію дзвінків та забезпечення основної функціональності IP-телефонії.

VoIP перетворює голос користувача у цифровий формат, стискає його і надсилає через інтернет. Постачальник послуг VoIP (наприклад, інтернет-провайдер) налаштовує дзвінок. Під час телефонної розмови обмін даними відбувається за допомогою невеликих пакетів даних. Інтернет може надсилати ці пакети даних по всьому світу менш ніж за секунду.

Протокол передачі голосу через інтернет повністю оминає телефонну компанію. Скрізь, де є широкосмугове підключення до інтернету, наприклад, DSL, кабельне або оптоволоконне, може використовуватись VoIP. Це є значним покращенням порівняно з аналоговою телефонною системою [8].

Відрізняючись від традиційних методів телефонної мережі загального користування (ТМЗК), компанії, що надають послуги VoIP, надають

персоналізований VoIP-номер, який дозволяє компанії приймати і здійснювати телефонні дзвінки з будь-якого пристрою, підключеного до інтернету.

Компанії, які надають послуги VoIP-телефонії, мають корисні додатки для всіх – від індивідуальних абонентів до великих підприємств, наприклад, протокол ініціювання сеансу (SIP), який доповнює VoIP [50].

Крім того, в інтелектуалізованій системі доцільно передбачити захист серверів від зловмисних атак шляхом моніторингу лог-файлів на предмет підозрілих дій (наприклад, численні невдалі спроби аутентифікації) та автоматичного блокування IP-адрес, що спричиняють ці дії, за допомогою фаєрволів. Тому, у склад підсистеми аналізу введено Fail2Ban [7] – утиліту для підвищення безпеки VoIP-серверів [23].

Як вже вказувалось у розділі 1, для надійного функціонування системи виявлення зловмисних повідомлень IP-телефонії у корпоративній мережі доцільно забезпечити виконання встановлених правил розподілу доступу. Беручи до уваги цей аргумент, а також особливості функціонування системи виявлення зловмисних повідомлень IP-телефонії, у підсистему аналізу доцільно ввести процедуру розподілу доступу на основі механізму нечіткого висновку Мамдані з врахуванням опрацювання параметрів здійсненого дзвінка [23].

У даний час особливо актуальним є розвиток методів аналізу мовлення та відповідної обробки природної мови, який дозволяє створювати більш точні та ефективні системи виявлення аномального трафіку та потенційно небезпечних комунікацій. При цьому перспективним є використання інтелектуальних засобів для аналізу контенту в системі VoIP. Тому, базуючись на результатах дослідження у розділі 2, у підсистему аналізу доцільно ввести наступні дві процедури [57]:

– виявлення аномалій в трафіку IP-телефонії на основі групування VoIP повідомлень на основі контекстно-частотного аналізу,

–автоматизоване наповнення онтології тематичних повідомлень в корпоративній системі IP-телефонії на основі формалізованого представлення

повідомлень за допомогою деревовидних структур та на описі операцій взаємодії засобами алгебри кортежів.

Підсистема прийняття рішень відіграє одну з ключових ролей в управлінні викликами та маршрутизації дзвінків. ЇЇ доцільно побудувати на основі інструментального засобу Asterisk [58, 59] і засобу розподіленого потокового оброблення Apache Kafka [61, 62].

Комунікаційний інструмент з відкритим кодом Asterisk складається з різних компонентів і правил, які визначають, як система повинна обробляти вхідні та вихідні дзвінки, а також інші події. Приведемо основні компоненти та принципи роботи підсистеми прийняття рішень в Asterisk [84]: Dialplan (план набору), Extensions.conf (основний конфігураційний файл, в якому визначаються правила маршрутизації дзвінкі), AGI (механізм, який дозволяє запускати зовнішні скрипти для обробки дзвінків), AMI (інтерфейс для взаємодії з Asterisk в реальному часі через TCP-з'єднання), розширення та пріоритети, функції та застосунки, контрольні структури, база даних.

Для розширення функціоналу Dialplan слід перейти до інтеграції з системою розподілених потокових обробників на основі Apache Kafka або Apache Flink .

Apache Kafka – це розподілена система, що складається з серверів і клієнтів, які взаємодіють за допомогою високопродуктивного мережевого протоколу TCP. Попередньою розробкою *Apache Kafka* є *Apache Flink* – фреймворк і рушій розподіленої обробки для обчислень з урахуванням стану над необмеженими і обмеженими потоками даних.

Підсистема звітності та аналітики базується на процедурах інтеграції/ візуалізації даних з використанням програмного забезпечення з відкритим вихідним кодом Grafana [63], а також зберігання / експортування результатів у поширені формати.

Grafana дозволяє запитувати, візуалізувати, сповіщати та досліджувати існуючі метрики, журнали та траси, де б вони не зберігалися. Grafana OSS надає інструменти для перетворення даних бази даних часових рядів (TSDB) у наочні

графіки та візуалізації. Крім того, Grafana OSS також дозволяє підключати інші джерела даних, такі як NoSQL/SQL бази даних, Jira або ServiceNow, а також інструменти для CI/CD, наприклад, GitLab. Найпоширенішим використанням Grafana є відображення даних часових рядів, таких як пам'ять або процесор з плином часу, поряд з поточними даними про використання.

Надалі, для забезпечення роботи із отриманими даними, потрібно забезпечити зберігання результатів або їх експортування у поширені формати для подальшого аналізу при потребі. Попередній аналіз показав, що для експортування звітів доцільно вибрати формати PDF та CSV [63].

3.2 Узагальнений алгоритм і структурно-функціональна схема інтелектуалізованої системи

На основі узагальненої структури інтелектуалізованої системи (див. рис. 3.1) та схеми розподілу доступу клієнтів (див. рис. 3.2) запропоновано узагальнений алгоритм функціонування інтелектуалізованої системи (рис. 3.3). Даний алгоритм описує роботу інтелектуалізованої комп’ютерної системи, яка забезпечує управління доступом та моніторингу в корпоративній мережі, також контроль доступу користувачів, моніторинг мережевого трафіку, аналіз потенційних загроз (аномалій), автоматизоване прийняття рішень щодо безпеки та формування звітності про результати.

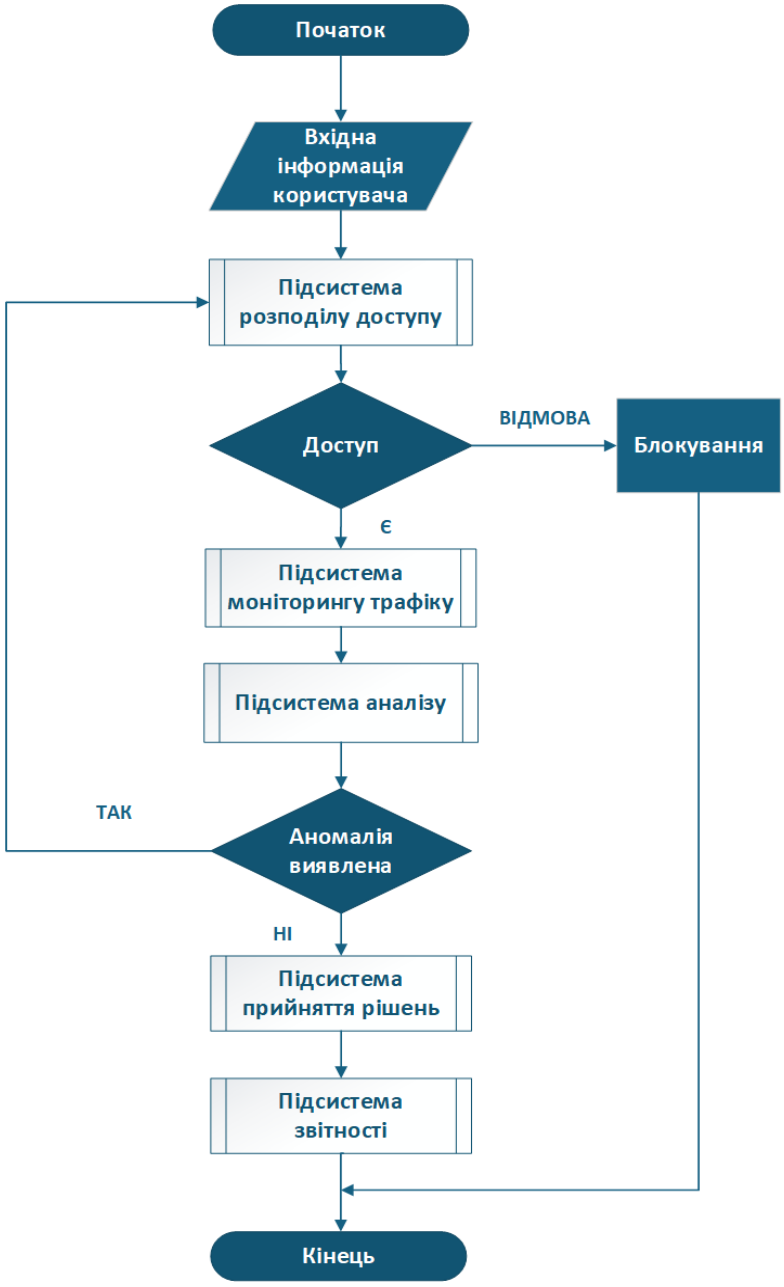


Рис. 3.3. Узагальнений алгоритм функціонування інтелектуалізованої системи

На початку алгоритму ініціалізується процес роботи системи, яка отримує інформацію про користувача (бл. 1), що здійснює спробу доступу. Це можуть бути:

- Облікові дані (логін/пароль);
- Інформація про сесію (IP-адреса, ID сесії);
- Інформація про запит (час, тип ресурсу, що запитується, права доступу тощо).

В блоці 2 здійснюється первинна перевірка та авторизація користувача, зокрема, ідентифікація та автентифікація, перевірка відповідності користувача встановленим правилам доступу. Результатом роботи цієї підсистеми є рішення, яке передається до блоку 3. У блоці 3 аналізується умова на наявність доступу користувача.

При цьому, якщо користувач *не відповідає критеріям доступу*, то система переходить до блоку 4 «Блокування», в іншому випадку надається доступ і активується підсистема моніторингу трафіку (бл. 5). Зокрема, дана підсистема активує модуль моніторингу та здійснює моніторинг за трафіком користувача шляхом аналізу потоків даних, протоколу взаємодії і мережевих пакетів, а також збору статистичних характеристик трафіку для подальшого аналізу.

Отримані дані моніторингу передаються в підсистему аналізу (бл. 6) для детального вивчення. При цьому використовуються алгоритм виявлення аномалій на основі методів штучного інтелекту та статистичного аналізу поведінки трафіку для виявлення нетипових ситуацій або потенційних загроз. У блоці 7 перевіряється умова на виявлення аномалій. Якщо аномалії виявлені, здійснюється повернення до підсистеми розподілу доступу. Це означає перегляд прав доступу, або навіть обмеження чи блокування доступу, якщо аномалії є критичними або потенційно небезпечними. У противному випадку здійснюється перехід на підсистему прийняття рішень (бл. 8). Дана підсистема проводить додаткову оцінку інформації з врахуванням інших факторів безпеки (наприклад, репутацію користувача, історію його поведінки, поточну ситуацію в мережі тощо). У результаті приймається рішення про завершення сеансу або продовження нормального функціонування.

У блоці 9 генеруються звіти про роботу системи, включаючи детальну інформацію про сесію користувача, виявлені аномалії, а також про прийняття рішення. Дані звіти можуть використовуватись для подальших заходів з безпеки, аудиту та вдосконалення роботи системи.

Виходячи із наведеного вище, можна констатувати, що даний алгоритм має наступні характеристики:

1. *Циклічність:* у разі виявлення аномалії система здатна автоматично повернутися до початку процесу для повторної перевірки і адаптації політик безпеки.
2. *Адаптивність:* алгоритм адаптується до нових умов завдяки підсистемам аналізу і прийняття рішень, що використовують сучасні методи обробки даних та штучного інтелекту.
3. *Проактивність:* система здатна попереджувати загрози завдяки безперервному моніторингу та аналізу трафіку.

Тобто, можна вважати, що запропонований алгоритм є ефективним інструментом, орієнтованим на автоматизацію прийняття рішень і швидке реагування на потенційні загрози.

З врахуванням викладеного вище, а також результатів, отриманих у пункті 3.1 розроблено структурно-функціональну схему інтелектуалізованої комп'ютерної системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі (рис. 3.4).

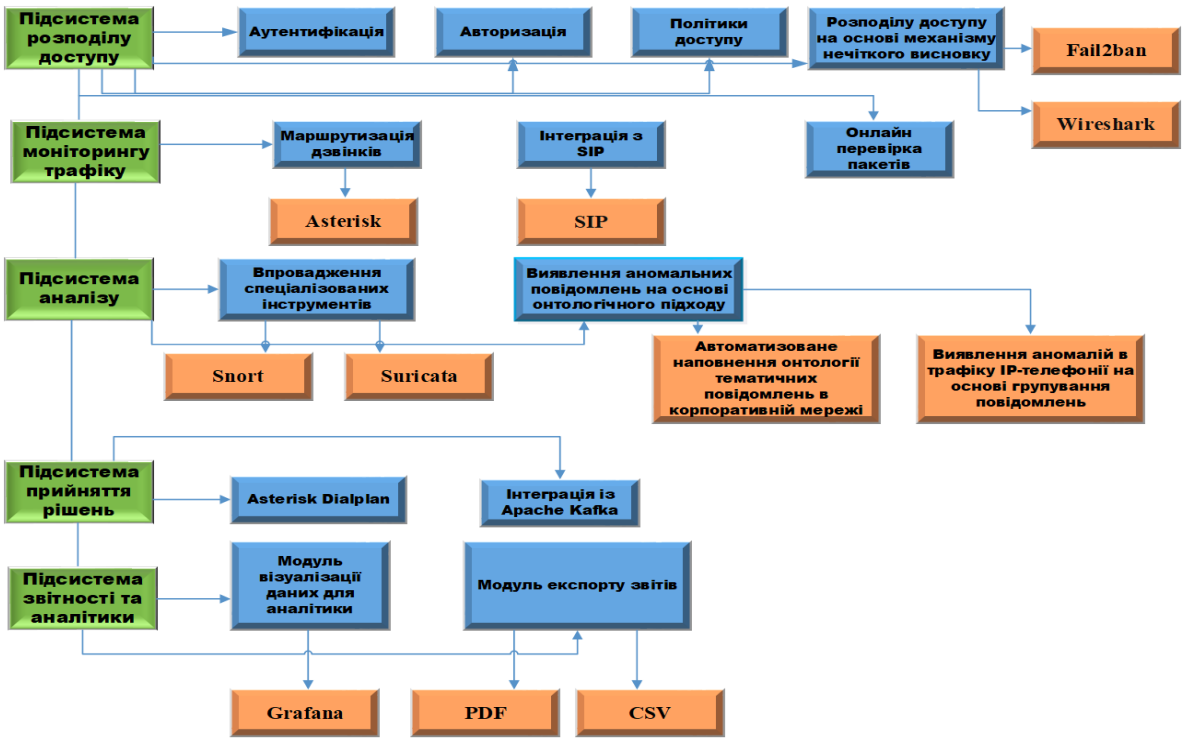


Рис. 3.4. Структурно-функціональна схема інтелектуалізованої системи

3.3 Взаємозв’язок модулів для виявлення аномальних повідомлень на основі онтологічного підходу

На рисунку 3.5 наведено структуру модулів виявлення аномальних повідомлень на основі онтологічного підходу. Розглянемо її основні компоненти та кроки роботи.

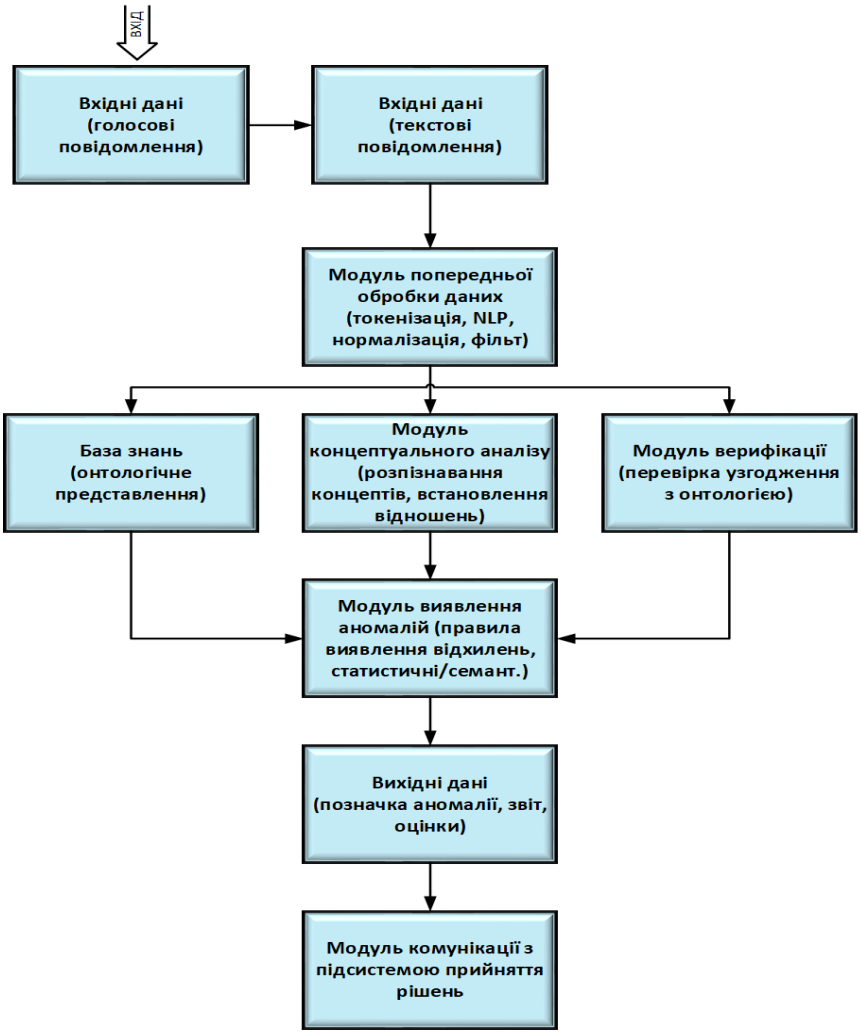


Рис. 3.5. Схема взаємозв’язку модулів для виявлення аномальних повідомлень на основі онтологічного підходу

Опис компонентів та функціоналу:

1. Вхідні дані: голосове повідомлення.
2. Вхідні дані:

– перетворення голосового повідомлення у текстове повідомлення.

3. Модуль попередньої обробки даних:

- токенізація та нормалізація: розбиття тексту на токени (слова, фрази), приведення їх до базових форм (лематизація/стемінг);
- фільтрація шуму: видалення непотрібних символів, HTML-тегів, стоп-слів;
- аналіз природної мови (NLP): визначення частини мови (POS-tagging), виявлення сутностей, перетворення в уніфікований формат для подальшого семантичного аналізу.

4. База знань (онтологічне представлення):

- містить концепти (терміни предметної області), їх визначення, відношення між ними, таксономії, а також правила та аксіоми;
- задає "нормальну" модель знань, яка використовується при пошуку невідповідностей.

5. Модуль концептуального аналізу:

- співставляє оброблений текст із поняттями онтології, встановлює відповідності між сутностями повідомлення та концептами із бази знань;
- визначає семантичні ролі (хто діє, над чим діє, як, коли) та створює семантичну модель повідомлення.

6. Модуль верифікації:

- на основі онтології та заданих правил перевіряє семантичну модель повідомлення на узгодженість;
- використовує механізми дедуктивного чи абдуктивного виведення для визначення, чи повідомлення вкладається у межі нормальної поведінки системи знань.

7. Модуль виявлення аномалій:

- порівнює отримані результати логічного аналізу з типовими патернами, очікуваними поведінковими моделями та статистичними нормами;
- правила виявлення аномалій можуть бути базовані на відхиленнях від семантичних обмежень, непритаманних поєднаннях концептів, некоректних зв’язках між сутностями або статистично рідкісних патернах у тексті;

- при виявленні аномальних ознак формує відповідні ознаки/мітки аномальності.

8. Вихідні дані:

- система формує висновок: чи є повідомлення аномальним, ступінь впевненості у цьому, тип аномалії, рекомендації щодо подальших дій;

- результат може бути використаний для фільтрації спаму, виявлення шахрайських повідомлень, аналізу негативних соціальних патернів або інформаційних атак.

9. Модуль комунікації з підсистемою прийняття рішень:

- здійснює передачу проміжних результатів аналізу та ідентифікованих аномалій до підсистеми прийняття рішень;

- забезпечує узгоджене та послідовне виконання завдань між модулем виявлення аномалій та механізмом прийняття рішень, підтримуючи актуальність та узгодженість даних.

Представлена схема та опис показують цілісний процес обробки та аналізу текстових повідомлень на семантичному рівні за допомогою онтологічного підходу. Він дозволяє враховувати значення, контекст та логічну узгодженість повідомлень для виявлення прихованих чи нетривіальних аномалій, які складно ідентифікувати лише статистичними чи поверхневими методами.

3.3.1 Автоматизоване наповнення онтології тематичних повідомлень у корпоративній мережі.

Автоматизоване наповнення онтології тематичних повідомлень у корпоративній мережі зазвичай передбачає використання комплексного підходу, що поєднує технології обробки природної мови, семантичного аналізу та методи керованого або напівкерованого навчання моделей. Нижче наведено детальний опис основних етапів та принципів, які можуть бути покладені в основу такого підходу:

1. Формування початкової онтологічної структури:

- Визначення домену та предметної області: спочатку необхідно чітко окреслити тематичні області, які відображатиме онтологія. Наприклад, для корпоративної мережі це можуть бути: проекти, відділи, продукти, процеси, співробітники, ролі, технології.

- Створення початкової онтології: на основі аналізу домену експертами формуються базові концепти (класи), властивості (атрибути, відношення) та ієрархії. Для цього можуть використовуватися онтологічні редактори (Protégé) і стандартні формати (OWL, RDF/S).

2. Попередня обробка та нормалізація даних:

Збір тематичних повідомлень: автоматичне вилучення повідомлень та їх метаданих з корпоративних каналів (електронна пошта, внутрішні форуми, чати, системи управління завданнями).

Фільтрація та очищення даних: видалення дублікатів, спаму, нерелевантної інформації, формування корпусу текстів для подальшої обробки.

Лінгвістична нормалізація: токенізація, лематизація або стемінг, частковий морфологічний аналіз (для української мови – врахування відмінкових форм та синтаксичних залежностей), видалення стоп-слів, уніфікація термінології.

3. Розпізнавання сутностей та відношень:

Витяг іменованих сутностей (Named Entity Recognition, NER): застосування моделей машинного навчання (наприклад, CRF, BERT, spaCy або Stanza для української мови) з попередньо навченими векторами або ембедінгами. На цьому етапі визначаються сутності, що відповідають вже наявним класам в онтології (наприклад, назви проєктів, відділів, технологій, згадки про осіб).

Розпізнавання термінів та понять на основі словників і патернів: використання доменно-специфічних словників, глосаріїв та правил для ідентифікації ключових понять, які відповідають концептам онтології.

Ідентифікація відношень (Relation Extraction): виявлення семантичних зв’язків між сутностями (хто керує проєктом, які технології використовуються в певному відділі, які процеси описано в конкретному повідомленні). Методи

можуть включати глибинне навчання (RNN, Transformers) або правило-орієнтовані підходи.

4. Порівняння з онтологією та оновлення структури:

Мапінг сутностей до концептів онтології: виявлені у текстах сутності співвідносять з існуючими класами і особами (індивідами) в онтології. Якщо сутність не відповідає жодному вже наявному елементу, система може створити новий індивід чи уточнити класифікацію.

Уточнення та формування нових властивостей: якщо в повідомленнях виявлено нові типи відношень або атрибутів, які раніше не були враховані, онтологію доповнюють новими властивостями.

Керування синонімами та варіативними формами: на основі дистрибутивних семантичних моделей (word2vec, fastText, BERT-ембедінги) можна виявити, що різні лексичні одиниці відповідають одному концепту, і додати їх як синоніми чи альтернативні мітки.

5. Перевірка якості та валідація:

Експертний контроль: періодично експерти домену переглядають нові сутності та відношення, що додаються до онтології, вносять корективи, вилучають помилкові.

Автоматична валідація: використання правил цілісності (наприклад, у SHACL), логічних консистентних перевірок та евристик, що дозволяють виявити суперечності чи некоректні зв’язки.

6. Постійне оновлення та інтеграція:

Ітеративне вдосконалення моделей: навчання моделей розпізнавання сутностей та відношень на розширеному корпусі, врахування зворотного зв’язку від експертів.

Автоматичний розподіл по концептах: додавання нових даних в онтологію у режимі реального часу або за розкладом, залежно від потреб компанії.

Інтеграція з іншими джерелами даних: можливе використання даних з внутрішніх БД, CRM, ERP-систем, документів політик та інструкцій, що підвищує повноту і релевантність онтології.

Очікувані переваги такого методу:

- централізація знань: зведення неструктурованих даних (повідомлень) у структуру знань;
- покращений пошук та аналітика: семантичний пошук за темами, автоматичне групування контенту за концептами онтології;
- адаптивність: постійне оновлення онтології з урахуванням нових термінів і понять;
- прозорість та узгодженість: зменшення дублювання інформації, можливість виявляти конфлікти знань, підвищення якості корпоративної бази знань.

Отже, метод автоматизованого наповнення онтології тематичних повідомлень у корпоративній мережі базується на поєднанні семантичних технологій, НЛП (не було пояснень) та машинного навчання з експертною перевіркою. Такий підхід забезпечує динамічне розширення та вдосконалення корпоративної онтології, підвищуючи ефективність обробки та використання внутрішнього інформаційного ресурсу [88].

3.3.2 Виявлення аномалій у трафіку IP-телефонії на основі групування повідомлень

Виявлення аномалій у трафіку IP-телефонії на основі групування повідомлень спрямований на автоматичне розпізнавання нестандартної поведінки в мережевому середовищі VoIP. Основна ідея підходу полягає у використанні технік кластеризації для аналізу та структуризації трафіку за патернами повідомлень (як правило, сигналізаційних пакетів протоколів SIP, H.323), а потім виявлення тих елементів, що не належать жодному стабільному кластеру або суттєво відрізняються за своїми параметрами.

Основними етапами та принципами такого підходу є:

1. Збір даних та попередня обробка трафіку:

Збір даних: перехоплення та накопичення даних сигналізації IP-телефонії (наприклад, SIP-повідомлення INVITE, REGISTER, ACK, BYE тощо) з мережевого каналу або журналів.

Фільтрація та нормалізація: вилучення лише тих повідомлень, що мають значення для аномалій (наприклад, виклики, транзакції реєстрації), видалення дублікатів, корекція пошкоджених полів.

Екстракція ознак: перетворення сирих повідомлень на вектор ознак. Це можуть бути часові проміжки між повідомленнями, типи та послідовність повідомлень у виклику, параметри заголовків SIP (From, To, Contact), тривалість викликів, статистика RTP-потоку (якщо враховується медіа-трафік), індикатори якості (Jitter, Packet Loss), IP-адреси та порти учасників, геолокаційні дані.
Стандартизація ознак: масштабування або нормування даних для забезпечення коректної роботи алгоритмів кластеризації.

2. Кластеризація повідомлень та сесій:

Визначення кластера як патерна поведінки: кластер має відображати типову модель взаємодії: наприклад, нормальний виклик A→B, реєстрація телефону, повідомлення про оновлення статусу
Алгоритми кластеризації:

1) K-Means: підходить для чітко розмежованих кластерів, але вимагає наперед задану кількість кластерів.
2) DBSCAN, OPTICS: дозволяють виявляти довільні форми кластерів та знаходити точки-аномалії як елементи, що не належать жодному кластеру.
3) Hierarchical Clustering: може застосовуватися для побудови деревоподібної структури схожості та подальшого вибору оптимального рівня кластеризації.

Результат кластеризації: Формування набору "типових" патернів трафіку. Звичайно, кожен кластер відображає певну категорію поведінки в мережі (наприклад, стандартний реєстраційний сеанс, звичайний виклик, внутрішній виклик між співробітниками, виклик назовні, типові помилки з’єднання).

3. Виявлення аномалій:

Аномалії як позакластерні точки: повідомлення або їх групи, які не входять до жодного з кластерів, вважаються потенційними аномаліями.

Аномалії як "далекі" елементи кластера: якщо використовується метод на кшталт K-Means, можна визначити міру "віддаленості" точки від центру кластера. Ті пункти, у яких відстань більша за певний поріг, можуть вважатися аномаліями.

Перевірка стабільності кластерів у часі: аномальні ситуації можуть виникати, якщо з’являються нові несподівані патерни (наприклад, масова поява спроб реєстрації з невідомих IP-адрес) або суттєво змінюється структура вже наявних кластерів.

4. Інтеграція з експертним аналізом і правилами безпеки:

Доменно-специфічні правила: після виявлення "підозрілих" пунктів можна застосувати додаткові евристики (наприклад, чорні списки IP-адрес, незвичні часові проміжки активності, спроби підбору паролів для реєстрації SIP).

Ітеративне вдосконалення: експерт мережевої безпеки може переглянути виявлені аномалії, позначити їх як істинно шкідливі або хибні спрацювання, і на основі цього вдосконалити параметри кластеризації, критерії ознак або правила обробки.

5. Автоматизація та моніторинг у режимі реального часу:

Потокова обробка: для швидкого виявлення аномалій можна інтегрувати метод у системи моніторингу трафіку в реальному часі. Використання системи обробки потоків (Apache Kafka) дозволить оперативно реагувати на підозрілі ситуації.

Адаптивне оновлення моделей: періодична повторна кластеризація з урахуванням нових даних для адаптації до змін у шаблонах мережевого трафіку.

6. Технологічний стек та інструментарій:

Збір та аналіз даних: Tshark, tcpdump, VoIPmonitor, Homer SIP Capture, або спеціалізовані SIEM-системи.

Аналітика та кластеризація: Python (scikit-learn, numpy, pandas), R, Apache Spark MLlib.

Візуалізація: Grafana, або спеціальні інструменти візуалізації для інцидентів безпеки.

Очікувані переваги методу виявлення аномалій у трафіку IP-телефонії:

- виявлення невідомих загроз: на відміну від методів, що базуються на сигнатурах, кластеризація дозволяє виявити нові, раніше невідомі типи атак чи зловживань.
- мінімізація людської участі: зменшення потреби в ручному аналізі великих обсягів даних завдяки автоматизації обробки.
- адаптивність: модель може бути постійно вдосконалена за рахунок інтерактивного зворотного зв'язку та самооновлення кластерів.

Таким чином, метод виявлення аномалій у трафіку IP-телефонії на основі групування повідомлень полягає у побудові моделей типових патернів поведінки (кластерів) та виявленні тих спостережень, що істотно від них відхиляються, забезпечуючи швидку та масштабовану ідентифікацію потенційно шкідливих або нетипових активностей у VoIP-мережах.

З метою глибшого розкриття суті запропонованої архітектури доцільно дослідити структурно-функціональні схеми її базових компонентів, зокрема, інтелектуальних засобів захисту IP-телефонії на основі онтології та розподілу доступу в режимі реального часу на основі нечіткої логіки.

3.4 Архітектура програмного комплексу виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі

Архітектура програмного комплексу систем виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі призначена для забезпечення безпечного функціонування мережі, захисту голосового трафіку та конфіденційності інформації, що передається через IP-мережі. Основна мета такої архітектури – мінімізувати ризики від зовнішніх та внутрішніх загроз, забезпечуючи при цьому якісну та безперебійну роботу IP-телефонії.

На рисунку 3.6 представлено загальну архітектуру програмного забезпечення для захисту IP-телефонії. Необхідно відзначити, що така архітектура відображає взаємодію по рівнях:

– апаратний рівень, який включає всі пристрої, що використовують IP-телефонію, зокрема IP-телефони, софтфони (програмні телефони) та мобільні додатки;

– комутаційний рівень, який характеризує інфраструктуру локальної мережі (комутатори та маршрутизатори, віртуальні локальні мережі (VLAN) для сегментації трафіку);

– серверний рівень, який характеризує управління дзвінками та відповідними характеристиками (SIP-сервери, медіасервери, DNS та NAT сервери для маршрутизації);

– рівень безпеки, який складається з засобів виявлення та попередження атак та включає фільтри SIP-трафіку, інтелектуальні методи захисту IP-телефонії;

– рівень моніторингу та управління, який включає централізоване управління всією інфраструктурою (консолі моніторингу, системи аналізу трафіку, інтелектуальні методи захисту IP-телефонії).

Програмне забезпечення належить до класу об’єкто-орієнтованих систем, розроблене з використанням мови програмування PHP, а також СУБД MySQL. Система працює як інтегроване програмне забезпечення в середовищі Asterisk під управлінням операційною системою Linux. Загальна архітектура програмних компонентів представлена на рисунку 3.7.

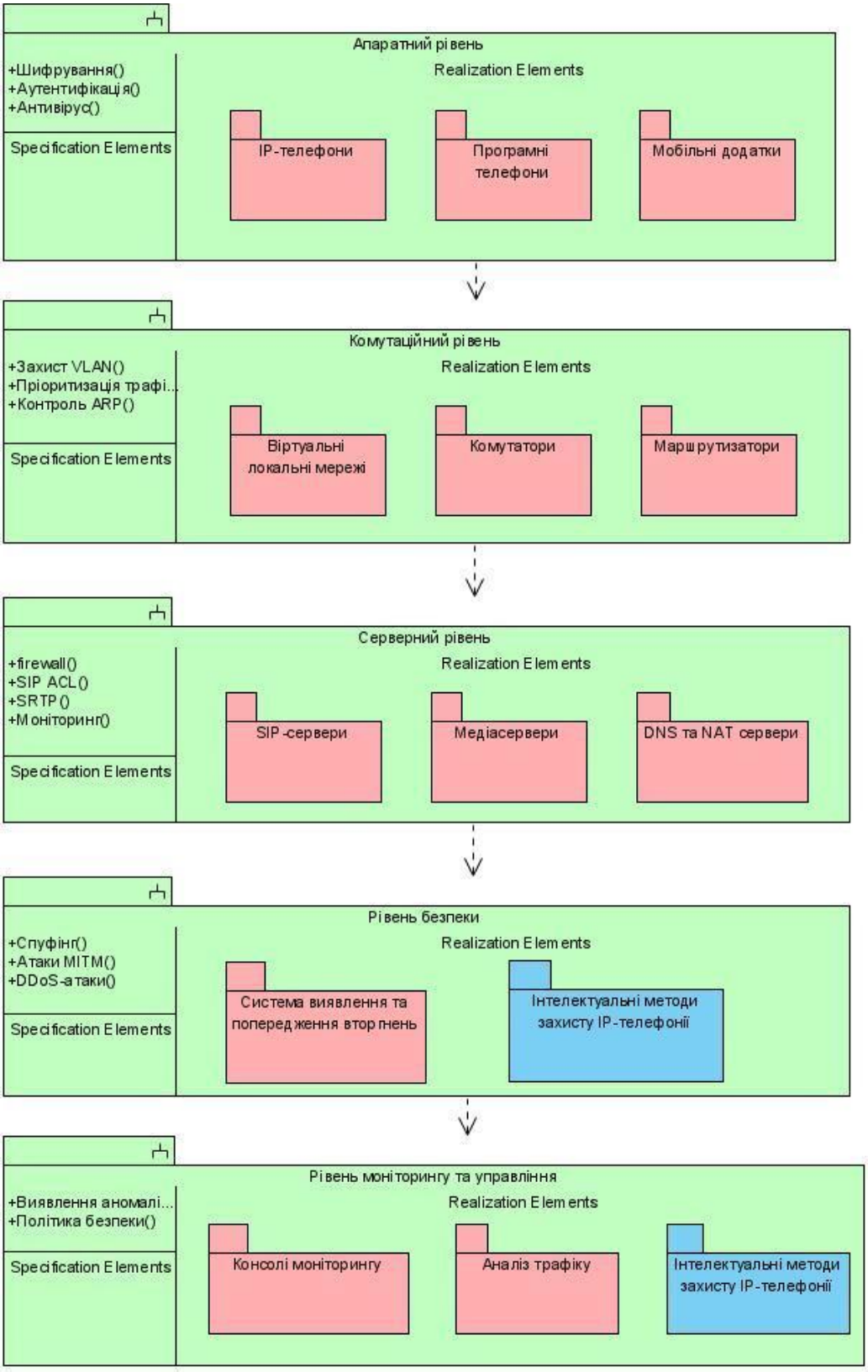


Рис. 3.6. Загальна архітектура програмного забезпечення для захисту IP-телефонії

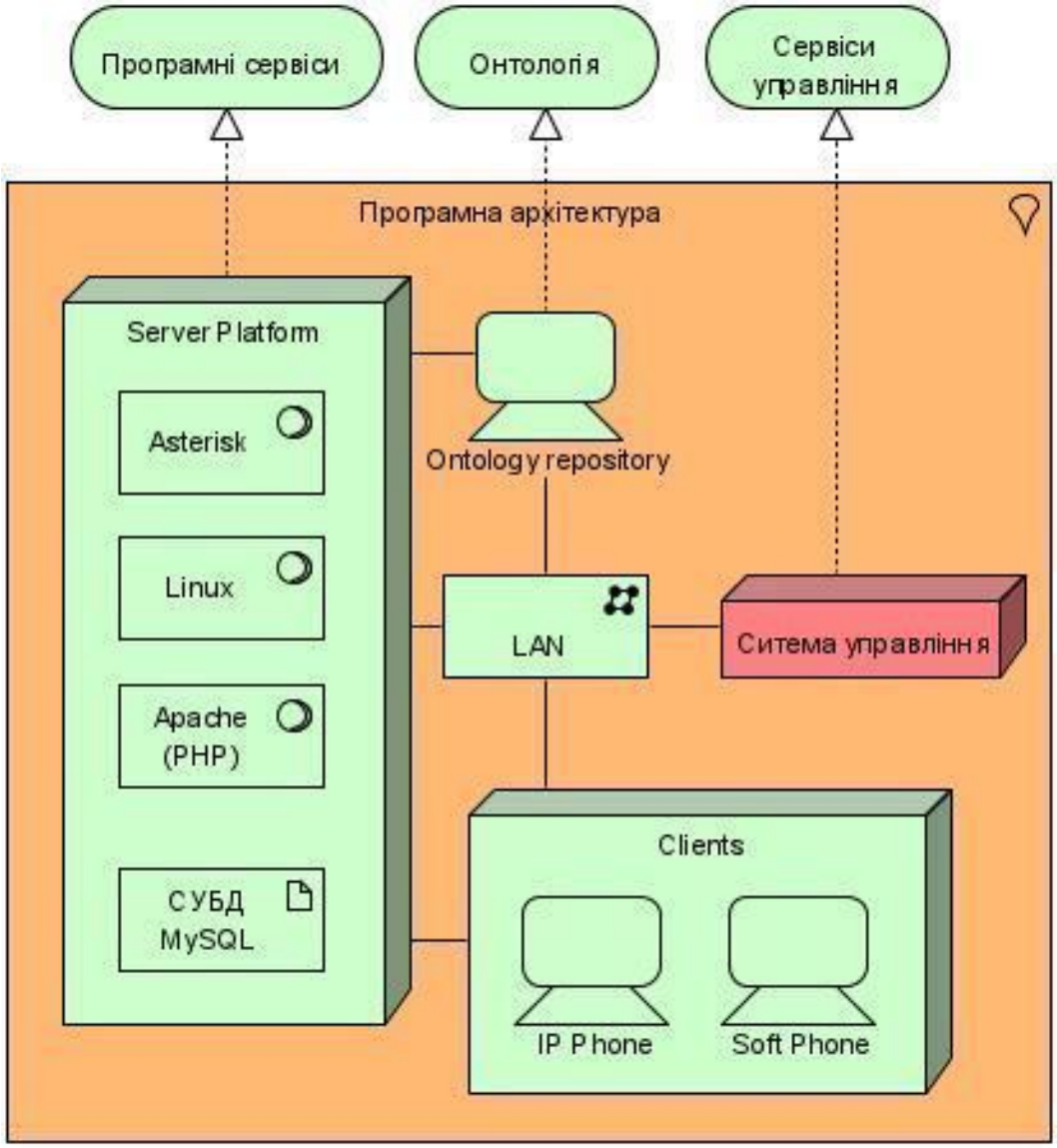


Рис. 3.7. Загальна архітектура програмних компонентів

На рисунку 3.8 представлено загальну діаграму варіантів використання інтелектуалізованої системи захисту IP-телефонії в корпоративній мережі. Основними користувачами системи є адміністратор та користувач, які можуть виконувати визначений набір функції.

Як показано на рисунку 3.8, користувач має можливість здійснювати виконання голосових дзвінків після аутентифікації в системі. Адміністратор відповідає за налаштування та управління системою захисту IP-телефонії та має доступ до адміністративних функцій, таких як конфігурація, моніторинг та аудит. Необхідно також відзначити, що адміністратор може здійснювати

налаштування параметрів інтелектуалізованих методів захисту IP-телефонії в корпоративній мережі.

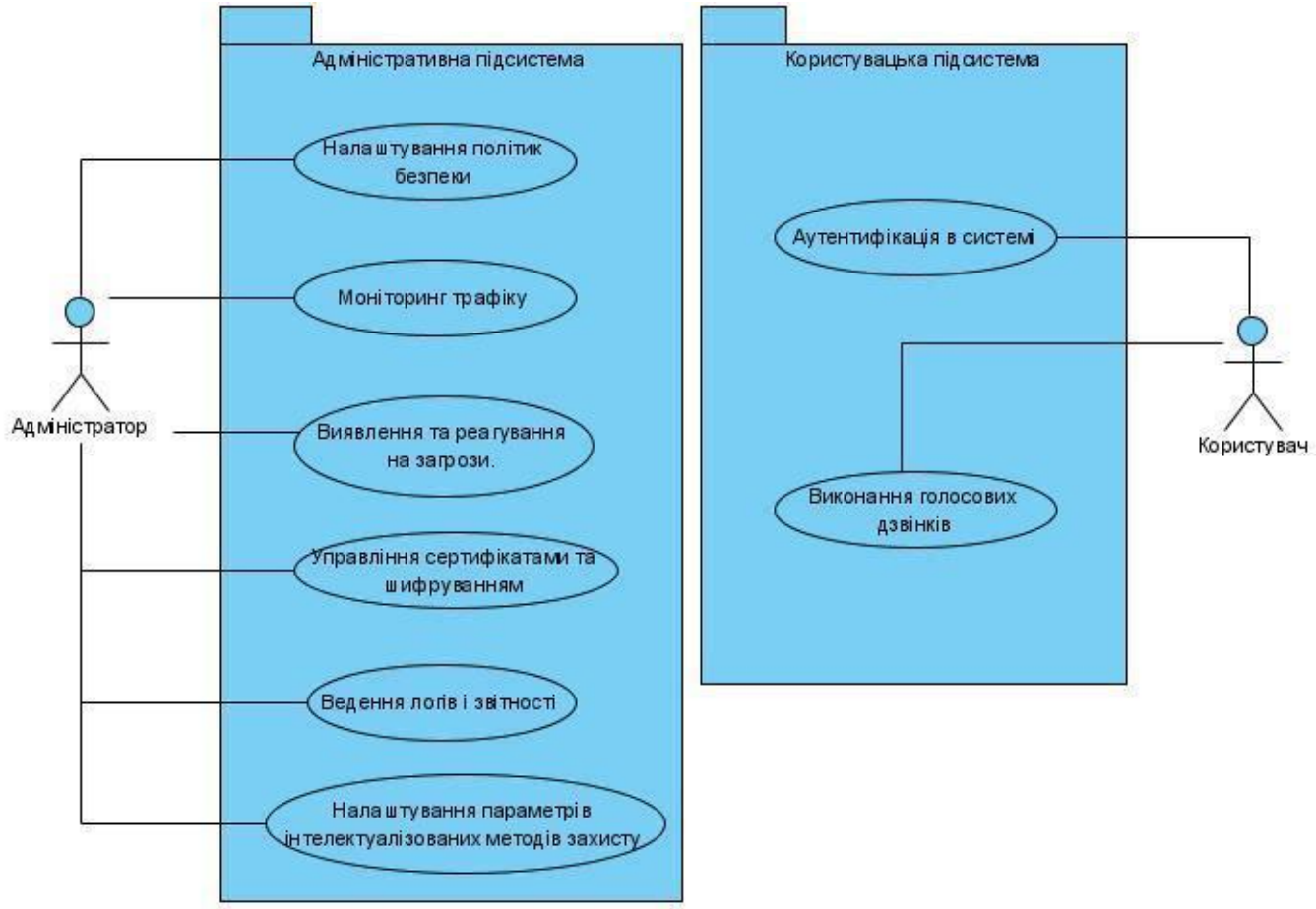


Рис. 3.8. Діаграма варіантів використання

На рисунку 3.9 представлено відповідну діаграму послідовності для адміністратора в процесі налаштування параметрів інтелектуалізованих методів захисту IP-телефонії в корпоративній мережі.

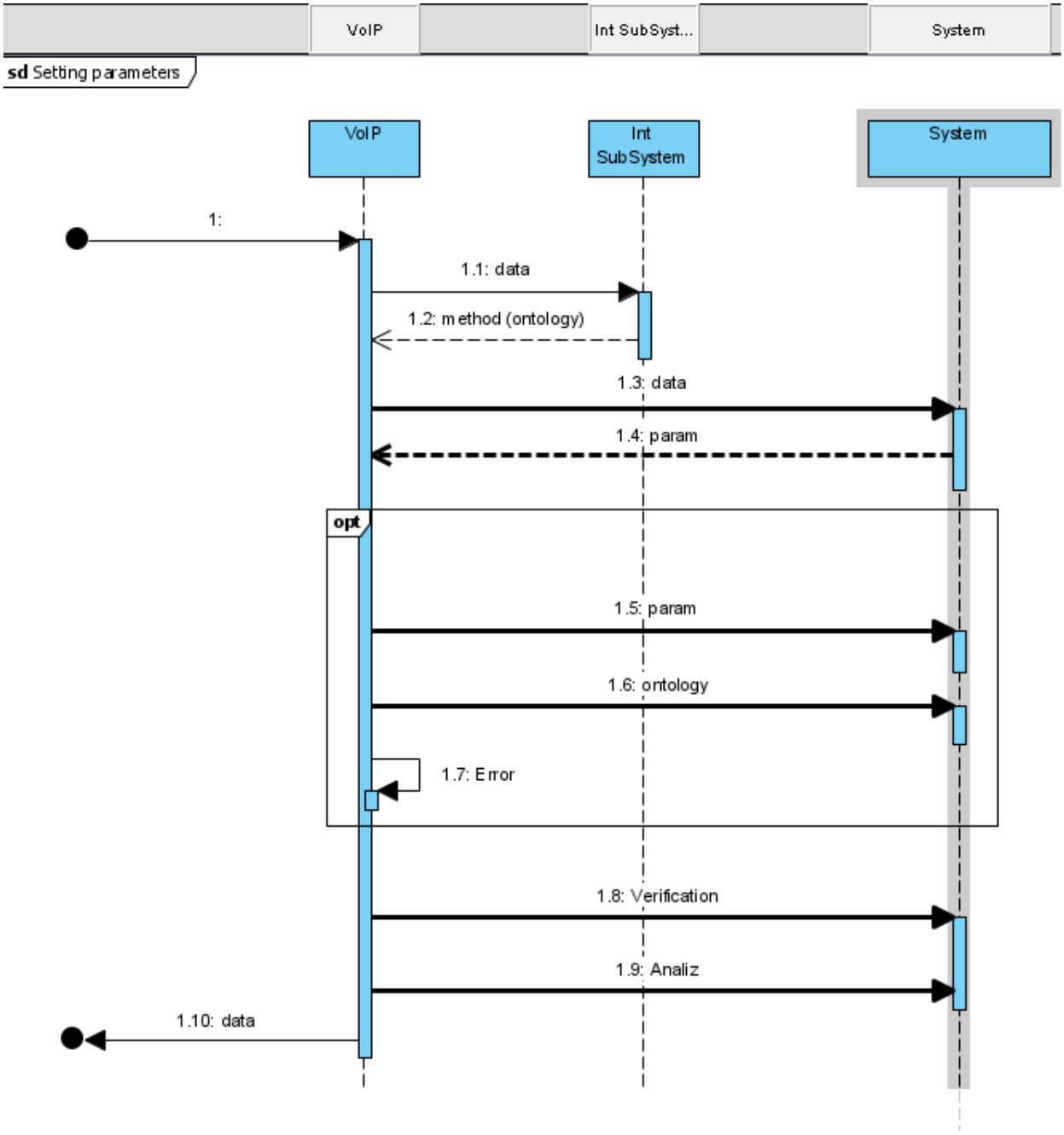


Рис. 3.9. Діаграма послідовності налаштування параметрів інтелектуалізованих методів захисту IP-телефонії в корпоративній мережі

Системний адміністратор має можливість адмініструвати систему, здійснювати управління процесом логування та звітністю, а також оновлювати програмне забезпечення. На рисунку 3.10 представлена діаграма послідовності, яка описує процеси аналізу голосових повідомлень з використанням інтелектуалізованого підходу.

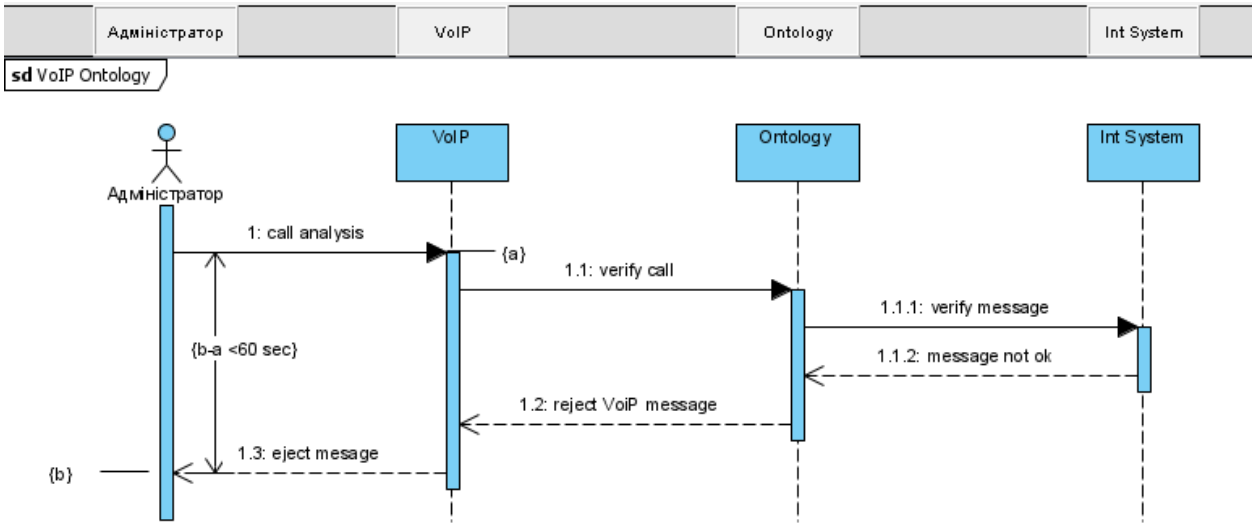


Рис. 3.10. Діаграма послідовності формування та наповнення онтологічних даних

На рисунку 3.11 представлена діаграма класів програмного комплексу інтелектуалізованої системи виявлення аномальних повідомлень IP-телефонії в корпоративній мережі. Розглянемо детальніше основні реалізовані класи та їх призначення:

–User (користувач): відповідає за управління інформацією про користувачів системи, зберігає логін, пароль, роль (адміністратор, користувач);

–SessionManager (менеджер сесій): управляє аутентифікацією та авторизацією, відповідає за контроль активних сесій;

–callManager (менеджер дзвінків): обробляє запити на встановлення дзвінків, відповідає за шифрування медіа та управління дзвінками;

–SecurityManager (менеджер безпеки): виявляє та запобігає атакам, таким як DDoS, SIP-spoofing, включає інструменти для моніторингу та аналізу трафіку;

–LogManager (менеджер логів): зберігає інформацію про всі дії в системі, забезпечує аудит та перегляд подій;

–ConfigManager (менеджер конфігурації): зберігає та управляє налаштуваннями системи, включає налаштування шифрування, політик безпеки.

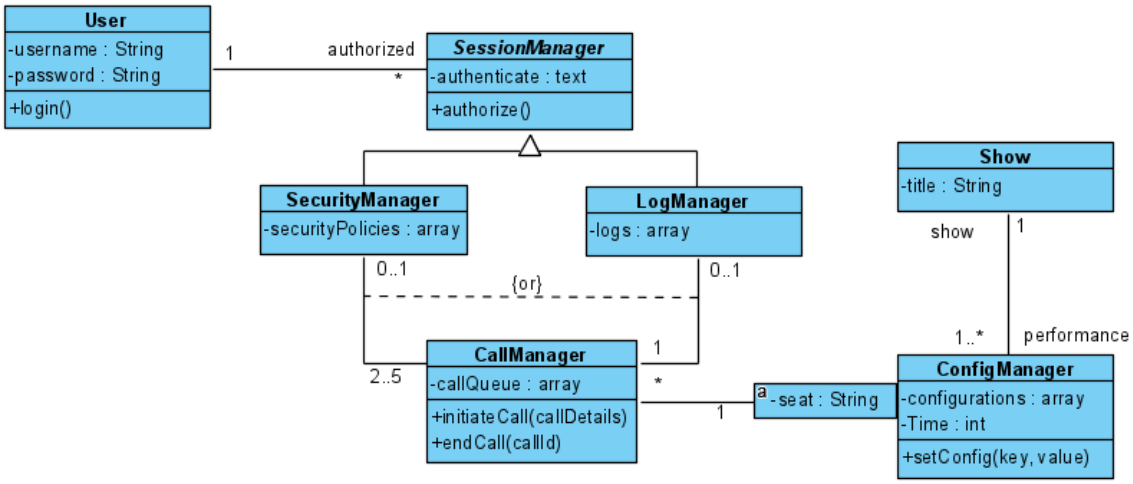


Рис. 3.11. Діаграма класів програмного комплексу інтелектуалізованої системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі

Важливим етапом реалізації інтелектуалізованої системи захисту ip-телефонії в корпоративній мережі є проектування системи зберігання інформації.

Для програмної реалізації комплексу було обрано СУБД MySQL. Ключовими чинниками цього вибору є висока ефективність обробки даних та наявність різноманітних інструментів для взаємодії з іншими інформаційними системами.

MySQL забезпечує швидку обробку транзакцій з оптимальною швидкістю, підтримує кешування результатів, що підвищує продуктивність читання даних. Реплікація та кластеризація покращують паралельність та дають можливість динамічно керувати навантаженням. Для покращення обробки великих обсягів даних та пришвидшення пошуку, в MySQL індекси бази даних інтегровані в загальну схему організації системної продуктивності [85].

На рисунку 3.12 представлено загальну ER діаграму бази даних, яка використовується для зберігання інформації.

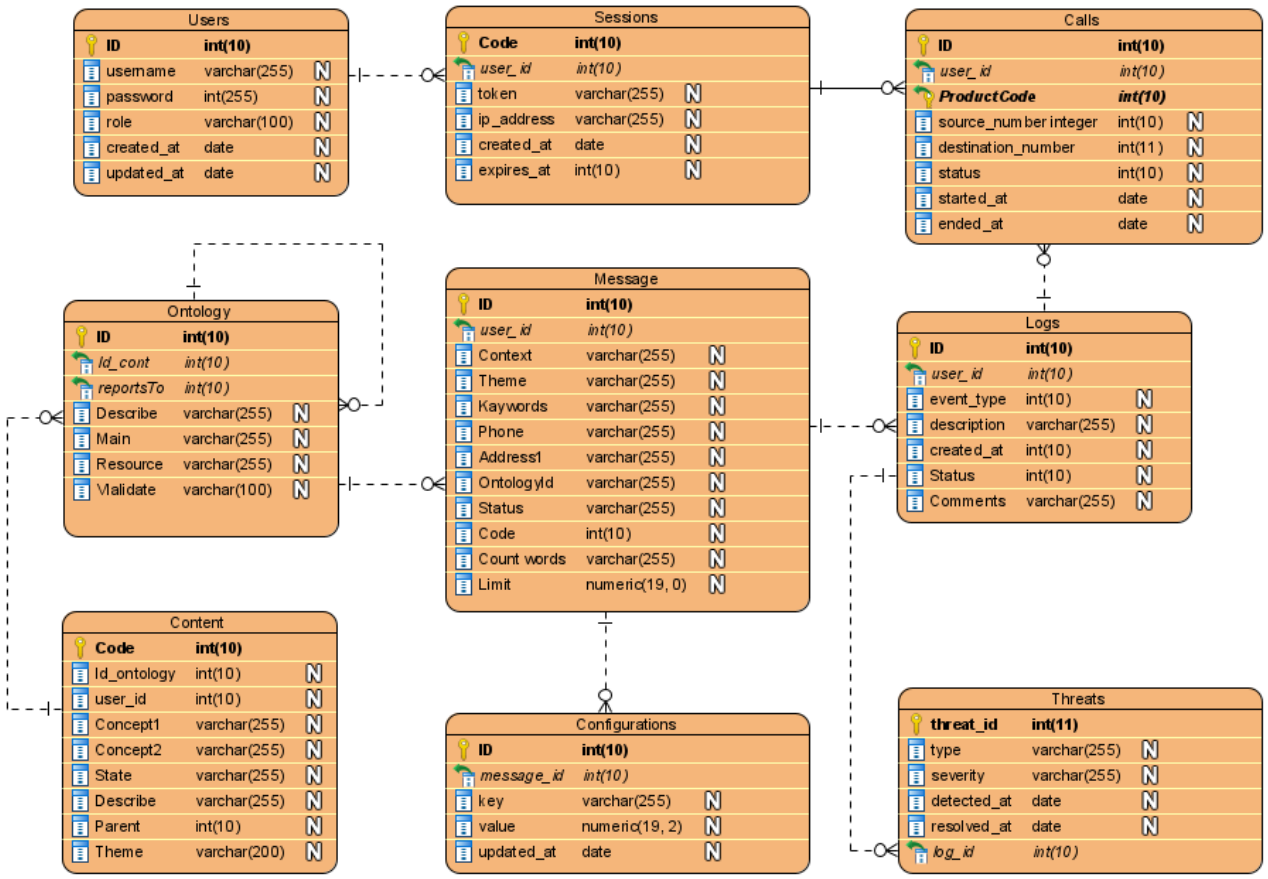


Рис. 3.12. ER діаграма бази даних інтелектуалізованої системи виявлення аномальних повідомлень IP-телефонії в корпоративній мережі

Для забезпечення основного функціоналу системи були реалізовані як основні, так і допоміжні відношення. Детальніше розглянемо спроектовані відношення. Атрибути відношень відображають ключові характеристики виділених сутностей, а типи даних і розмірність цих атрибутів визначались з урахуванням їх фізичної інтерпретації.

1) Users (Користувачі):

- user_id (PK): унікальний ідентифікатор користувача;
- username: ім'я користувача;
- password: хеш пароля користувача;
- role: роль користувача (адміністратор, звичайний користувач);
- created_at: дата створення користувача;
- updated_at: дата останнього оновлення даних;

2) Sessions (Сесії):

- session_id (PK):унікальний ідентифікатор сесії;
- user_id (FK): зв'язок із таблицею Users;
- token: унікальний токен для авторизації;
- ip_address: IP-адреса користувача;
- created_at: дата створення сесії;
- expires_at: дата завершення сесії;

3) Calls (Дзвінки):

- call_id (PK): унікальний ідентифікатор дзвінка;
- user_id (FK): зв'язок із таблицею Users;
- source_number: номер телефону, з якого виконується дзвінок;
- destination_number: номер телефону, на який виконується дзвінок;
- status: статус дзвінка (успішний, невдалий);
- started_at: час початку дзвінка;
- ended_at: час завершення дзвінка;

4) Logs (Логи):

- log_id (PK): унікальний ідентифікатор логу;
- user_id (FK): зв'язок із таблицею Users (необов'язковий).
- event_type: тип події (автентифікація, дзвінок, атака тощо);
- description: опис події;
- created_at: час створення запису;

5) Threats (Загрози):

- threat_id (PK): унікальний ідентифікатор загрози;
- type: тип загрози (DDoS, SIP-spoofing, MITM);
- severity: рівень небезпеки (низький, середній, високий);
- detected_at: час виявлення загрози;
- resolved_at: час усунення загрози (якщо застосовно);
- log_id (FK): зв'язок із таблицею Logs;

6) Configurations (конфігурації):

- config_id (PK): унікальний ідентифікатор конфігурації;

- key: назва параметра конфігурації;
- value: значення параметра;
- updated_at: час останнього оновлення.

7) Ontology (онтологія):

– ID (PK): унікальний ідентифікатор;
– Id_cont int – ідентифікатор контенту;
– reportsTo - приналежність;
– Describe - опис;
– Main - основа;
– Resource – джерело;
– Validate – відмітка про верифікацію онтології;

8) Message (повідомлення):

– ID (PK): унікальний ідентифікатор;
– user_id (FK): зв'язок із таблицею Users;
– Context – зміст повідомлення;
– Theme – тема повідомлення;
– Keywords – ключові слова;
– Phone – телефон;
– OntologyId – ідентифікатор наповнення спеціалізованої онтологічної моделі;
– Status – статус;
– Code – код;
– Count_words – кількість слів;
– Limit – обмеження на розмірність;

9) Content (контент):

- Id_ontology - ідентифікатор приналежності до онтології;
- user_id - ідентифікатор користувача;
- Concept1 - основний концепт;
- Concept2 - доповнюючий концепт;
- State - статус;

- Describe - опис змісту контенту;
- Parent - приналежність до основного або доповнюючого контенту;
- Theme - тема, або предметна область.

Висновки до розділу 3

1. Розроблено та детально описано архітектуру інтелектуалізованої системи виявлення зловмисних повідомлень IP-телефонії в умовах корпоративної мережі. Враховуючи виклики, ідентифіковані в попередніх розділах, ця архітектура спрямована на ефективне виявлення та нейтралізацію загроз, використовуючи сучасні підходи до обробки даних та аналізу поведінки.

2. Представлено узагальнену структуру інтелектуалізованої системи, яка включає низку взаємодіючих підсистем. Кожна підсистема виконує конкретні функції, від збору та попередньої обробки даних IP-телефонії до їх глибокого аналізу та прийняття рішень щодо виявлення аномалій. Такий модульний підхід забезпечує гнучкість, масштабованість та можливість інтеграції з існуючими системами безпеки.

3. Розроблено узагальнений алгоритм і структурно-функціональну схему інтелектуалізованої системи. Ця схема наочно ілюструє послідовність операцій, починаючи від перехоплення мережевого трафіку і закінчуючи генерацією сповіщень про виявлені загрози. Деталізація алгоритму дозволила формалізувати процеси виявлення, підвищивши їх прозорість та керованість.

4. Запропоновано механізм взаємозв’язку модулів для виявлення аномальних повідомлень на основі онтологічного підходу. Також запропоновано механізм автоматизованого наповнення онтології тематичних повідомлень у корпоративній мережі, що дозволяє системі постійно оновлювати свої знання про нормальні та аномальні патерни комунікації. Це є ключовим для підвищення точності виявлення нових та раніше невідомих атак. Крім того, представлено метод виявлення аномалій у трафіку IP-телефонії на основі групування повідомлень, який дозволяє ідентифікувати відхилення у поведінці трафіку за допомогою методів кластеризації та класифікації.

5. Деталізовано архітектуру програмного комплексу виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі. Ця архітектура ляже в основу практичної реалізації запропонованої системи, забезпечуючи її функціональність, надійність та ефективність у реальних умовах експлуатації.

РОЗДІЛ 4 РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНИХ МЕТОДІВ ТА ЗАСОБІВ

4.1 Інтелектуалізована система виявлення зловмисних повідомлень IP-телефонії корпоративної мережі ЗУНУ

Розроблена система ICSDMM-VoIP (Intelligent Computer System for Detection of Malicious Messages) у порівнянні з існуючими рішеннями [10-12] має потужну підсистему для аналітики та звітності з можливістю інтелектуального аналізу даних та наявністю засобів для адаптивної інтеграції в зовнішні спеціалізовані інформаційні системи та можливість інтеграції спеціалізованих програмних модулів.

Однією із частин інтелектуалізованої система виявлення зловмисних повідомлень у IP-телефонії корпоративної мережі ЗУНУ є її апаратне забезпечення (рисунок 4.1).

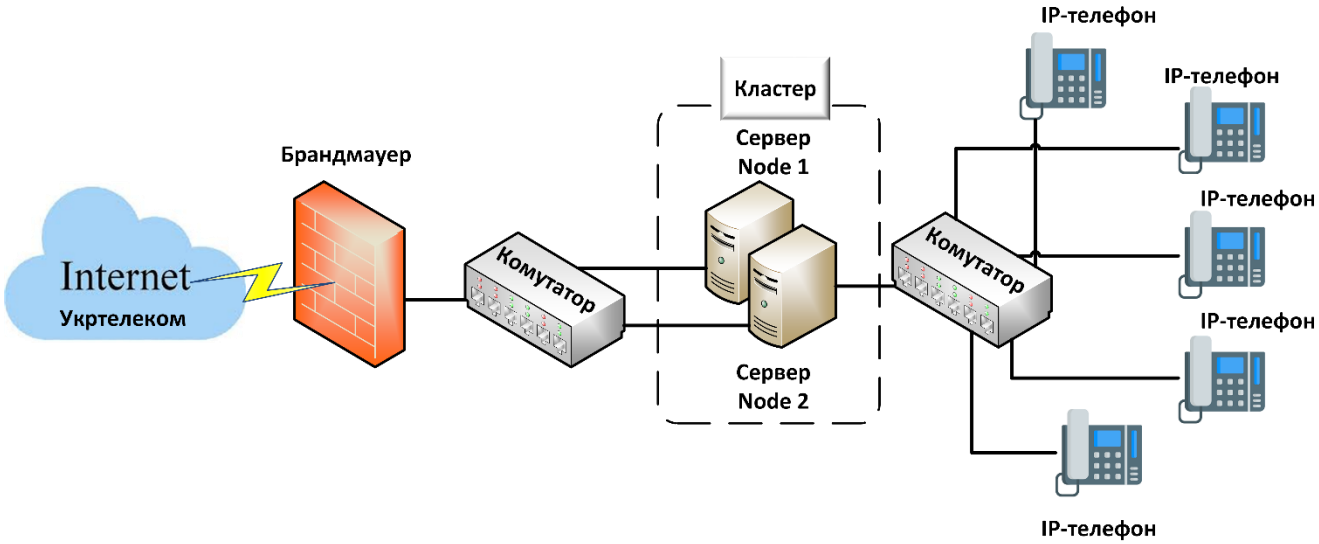


Рис. 4.1. Апаратна структура IP-телефонії ЗУНУ

Як видно із рисунку 4.1, з Укртелекому через інтернет університет підключено за допомогою технології SIP-Trunk (віртуальна IP-лінія, завдяки якій можна об'єднати декілька АТС в один канал). Для підключення послуги потрібний лише доступ до Інтернету. Далі йде міжмережевий екран (брандмауер), який забезпечує безпеку внутрішньої мережі від загроз ззовні.

Існує три типи міжмережевих екранів: мережевого рівня, прикладного рівня та рівня з'єднання. В ЗУНУ використовують всі три типи, але в даний момент для захисту IP-телефонії використовується міжмережевий екран рівня з’єднань. Він обслуговує велику кількість протоколів, в даному випадку протокол SIP. Розглянемо більш детальніше, що таке брандмауер в ЗУНУ.

Апаратний брандмауер – це сервер на основі сервера фірми Dell на базі операційної системи Linux Debian 12. Розглянемо більш детальніше апаратну частину сервера. Сервера Dell на початку адмініструють за допомогою системи віддаленого керування Integrated Dell Remote Access Controller (iDRAC) (рисунок 4.2). Інтегрований контролер віддаленого доступу Dell призначений для безпечного локального та віддаленого керування серверами, служить для розгортання, оновлення та контролювання серверів Dell PowerEdge будь-де та будь-коли.

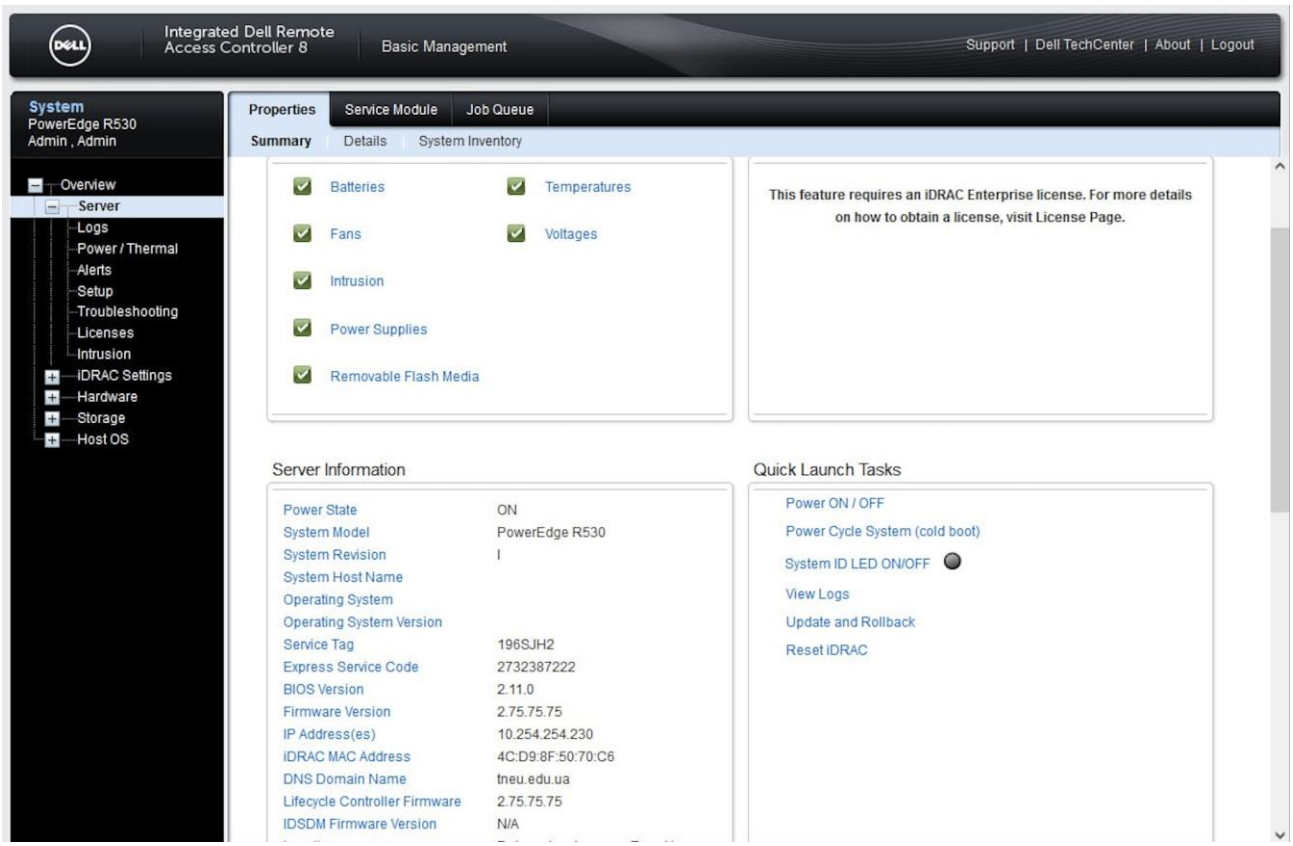


Рис. 4.2. Інтегрований контролер віддаленого доступу Dell (iDRAC)

На рисунку 4.3 можна побачити його системну інвентаризацію (System Inventory): кількість процесорів, пам’яті, жорстких дисків і т.д.

iDRAC має в собі багато функціональних можливостей для його адміністрування, зокрема, в реальному часі можна побачити навантаження на сервер, температурний режим (рис. 4.4).

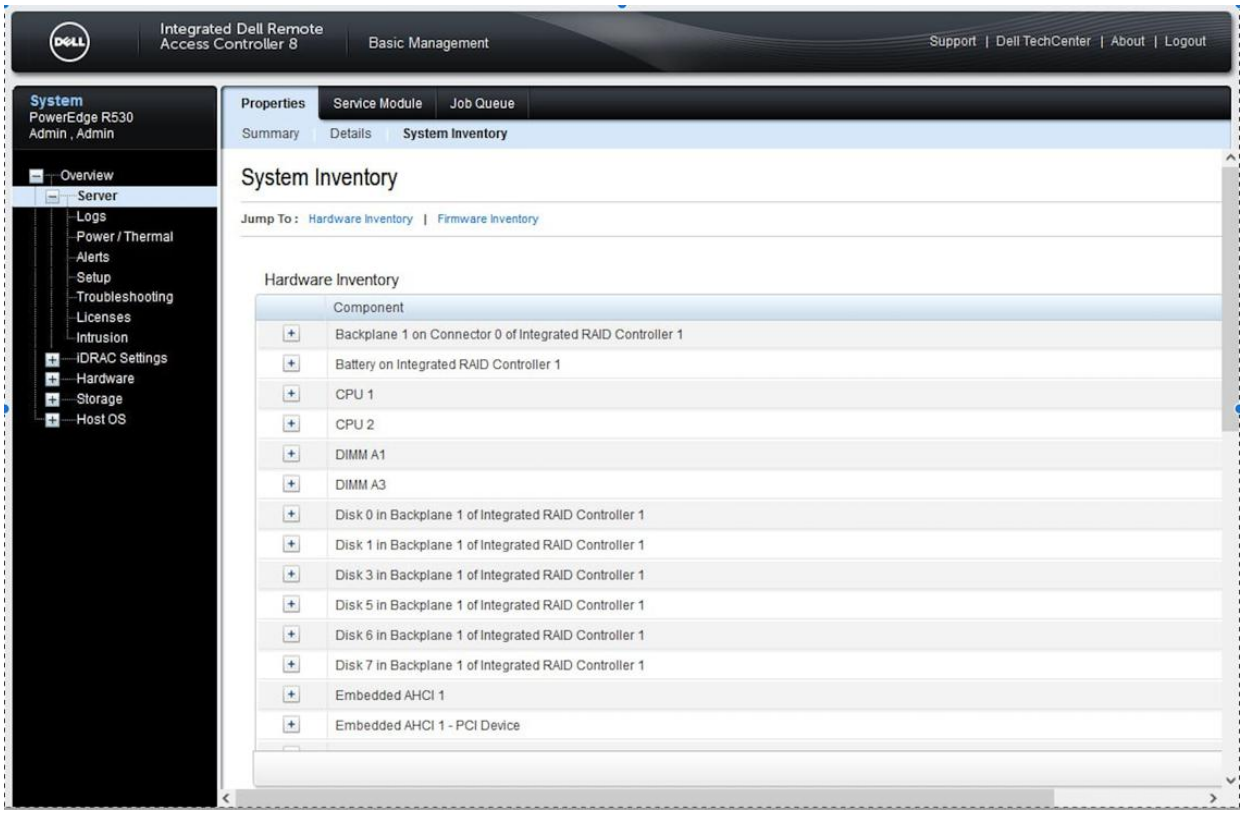


Рис.4.3. Системна інвентаризація сервера

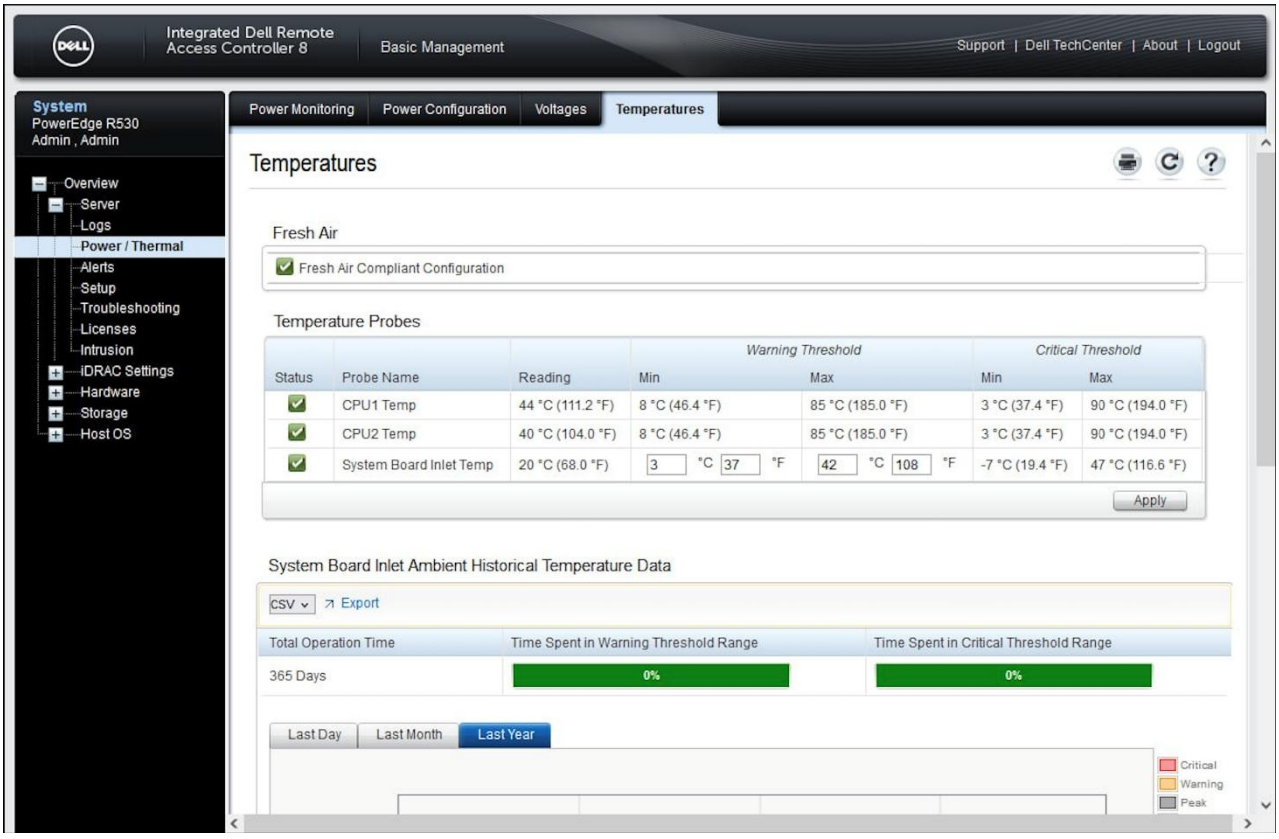


Рис.4.4 .Температурний режим сервера в реальному часі

Як показано на рисунку 4.3, сервер працює на двох процесорах. Вказано температуру на даний час, а також максимальну та мінімальну температури, при яких у сервера спрацює захист від перегріву чи переохолодження і він дасть команду на виключення.

Як зазначалося вище, сервер працює на операційній системі Debian 12. Це операційна система на базі Linux для широкого діапазону пристроїв, включаючи ноутбуки, настільні ПК і сервери.

Розглянемо архітектуру сервера за допомогою команди ***lscpu***, яка збирає дані щодо архітектури процесорів з sysfs, /proc/cpuinfo та усіх відповідних специфічних для архітектури бібліотек (наприклад librtas у Powerpc). Виведення команди може бути оптимізовано для обробки або для зручного читання людьми. До даних буде включено, наприклад, кількість процесорів, потоків, ядер, сокетів та вузлів Non-UniformMemory Access (NUMA). Також буде наведено дані щодо кешів процесорів, спільного використання кешів, сімейства, моделі, швидкодії у bogoMIPS, порядку байтів та модифікацій (рисунок 4.5).

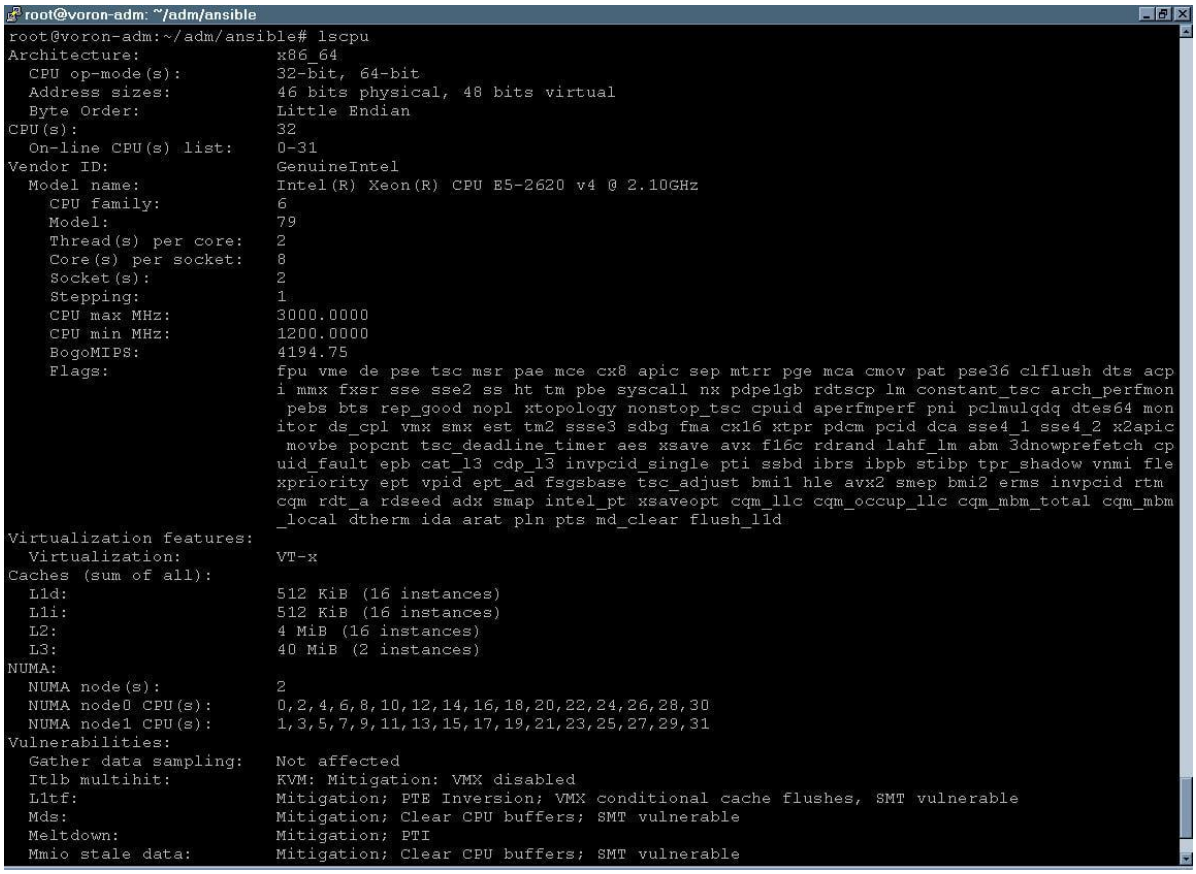


Рис.4.5. Виведення даних щодо архітектури процесорів

Як видно з рисунку 4.5, сервер має два процесори Intel Xeon E-5-2620 v4 із частотою 2.10 Ghz, кожен процесор має 16 ядер, дві планки оперативної пам’яті по 32 Гб. Сумарно на сервері 64 Гб оперативної пам’яті.

За допомогою команди **`top`** програма надає динамічний перегляд запущеної системи у реальному часі. Можна отримати зведену інформацію про систему, а також список процесів або потоків, якими наразі керує ядро Linux. Типи інформації про систему, що відображається, а також типи, порядок і розмір інформації, що відображається для процесів, налаштовуються користувачем, і цю конфігурацію можна зберегти після перезапуску системи (рис.4.6).

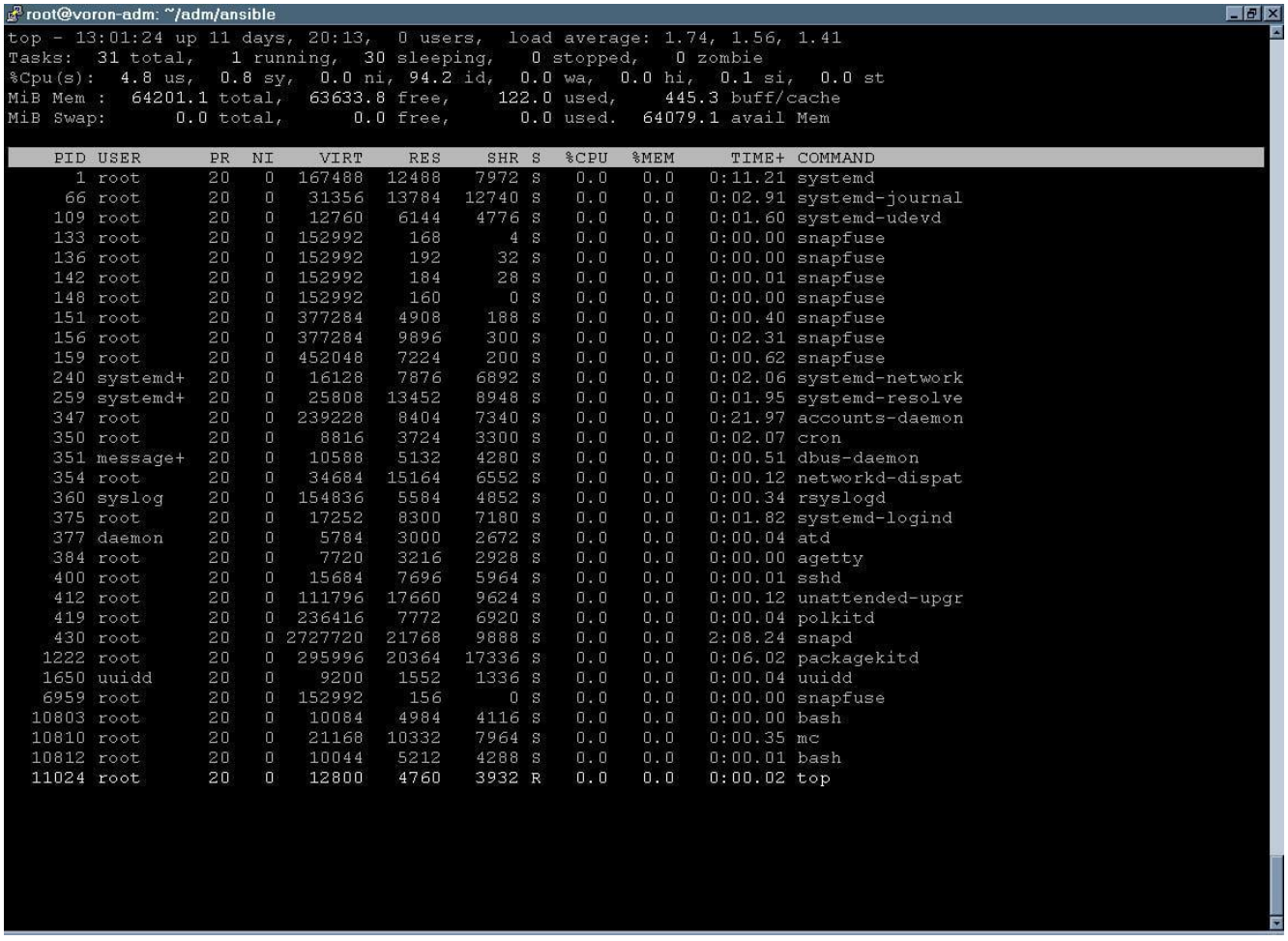


Рис. 4.6. Відображення процесів Linux

Як видно на рисунку 4.6, в даний момент на сервері було запущено 31 процес, з них 1 процес працює, решту 30 у сплячому режимі, навантаження на процесор 4.8%.

Розглянемо основну задачу сервера - його роботу як міжмережевого екрану. Для фільтрації пакетів, які заходять у корпоративну мережу ЗУНУ, застосовуємо Iptables – утиліту командного рядка, стандартний інтерфейс керування роботою міжмережевого екрана (брандмауера). Iptables використовуються для налаштування, підтримки і перевірки таблиць правил фільтрації пакетів IPv4 в ядрі Linux. Можна визначити декілька різних таблиць. Кожна таблиця містить декілька вбудованих ланцюжків, а також може містити ланцюжки, визначені користувачем. Кожен ланцюжок – це список правил, які можуть відповідати певному набору пакетів. Кожне правило визначає, що робити з відповідним пакетом. Це називається "ціль", яка може бути переходом до визначеного користувачем ланцюжка у тій самій таблиці (рис.4.7).

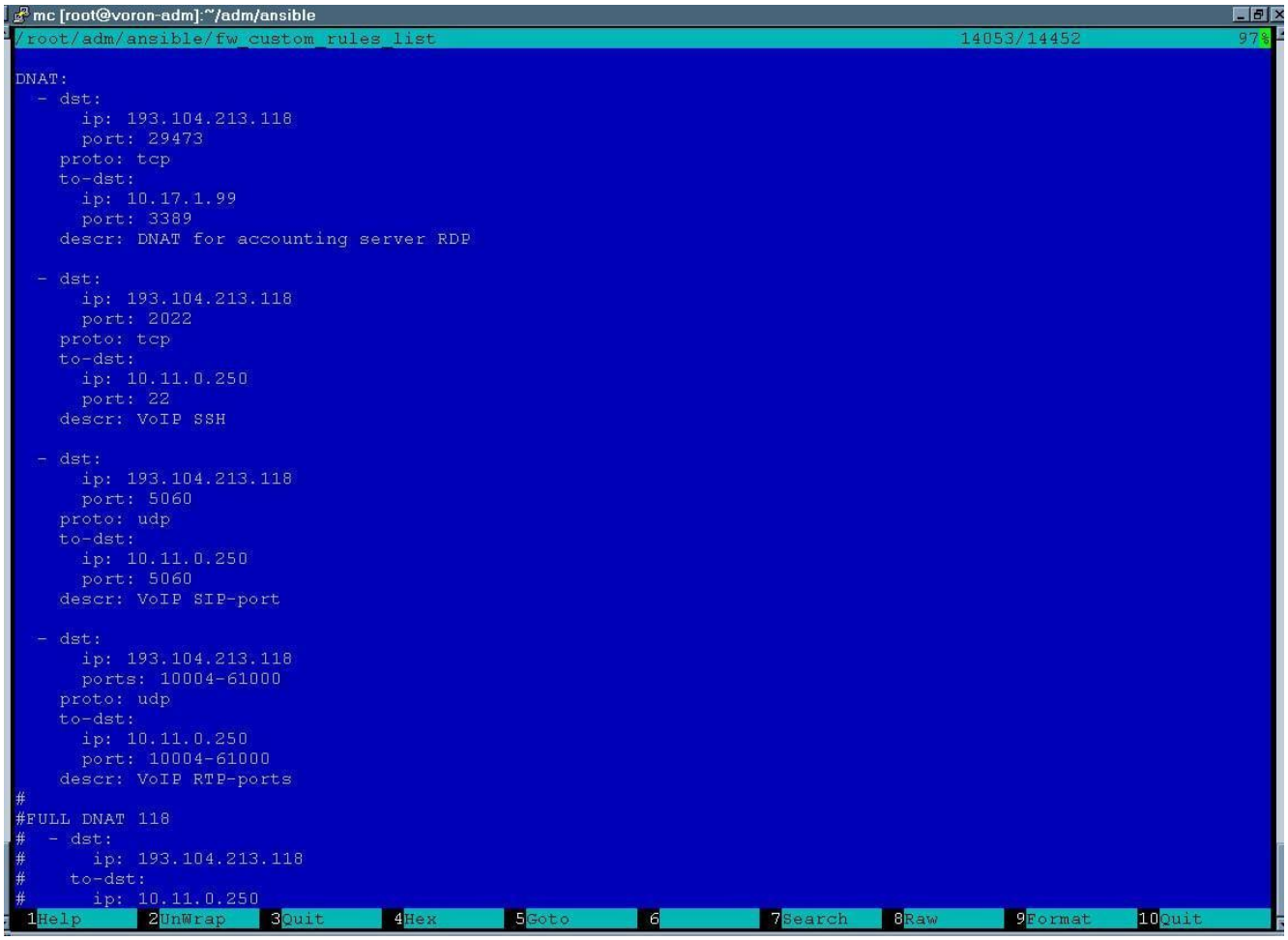


Рис. 4.7 Таблиця Iptables, що відповідає за IP-телефонію

На рисунку 4.7 видно ряд правил, які відповідають за порти 5060 та за прокидку із зовнішньої IP-адреси на внутрішні адреси серверів IP-телефонії, зокрема із зовнішньої IP 193.104.213.118 перенаправляє на внутрішню адресу 10.11.0.250. Правило брандмауера визначає критерії для пакета і цілі. Якщо пакет не відповідає критеріям, перевіряється наступне правило в ланцюжку; якщо відповідає, то наступне правило вказується значенням цілі, яка може бути назвою визначеного користувачем ланцюжка, однією з цілей, описаних в iptables-extensions, або одним із спеціальних значень ACCEPT (пропустити пакет через себе), DROP (скинути пакет) чи RETURN (припинити проходження цього ланцюжка і продовжити з наступного правила у попередньому (викликаючому) ланцюжку). Якщо досягнуто кінця вбудованого ланцюжка або збіглося правило у вбудованому ланцюжку з метою RETURN, то доля пакета визначається метою, визначеною політикою ланцюжка.

На рисунку 4.8 показано в реальному часі виконання команди iptables, що витягує із таблиць записи команд, які фільтрують пакети, що проходять через брандмауер, які стосуються портів та IP адресів IP-телефонії ЗУНУ.

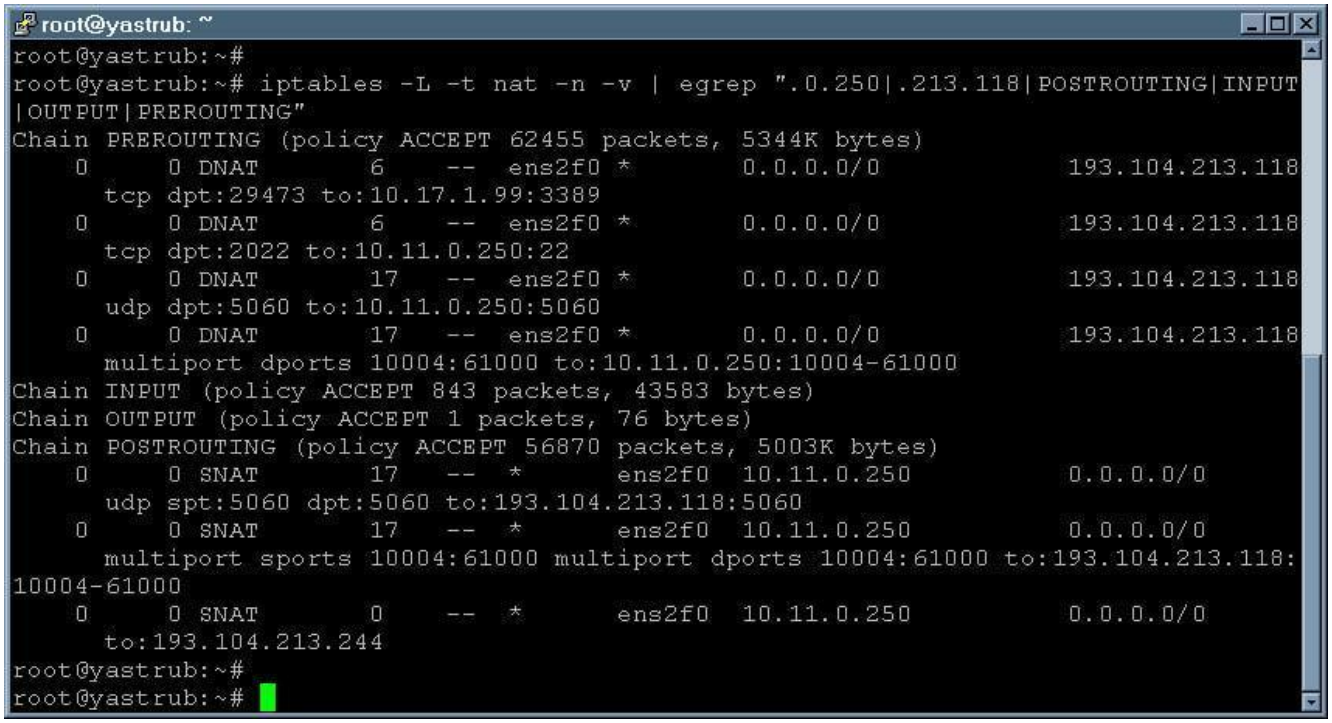


Рис. 4.8. Виконання команди iptables для фільтрації пакетів IP-телефонії ЗУНУ.

Як правило, міжмережевий екран у великих корпоративних мережах будується не на одному сервері, а на декількох серверах. На рисунку 4.9 показано перевірку правил на чотирьох серверах міжмережевого екрану ЗУНУ.

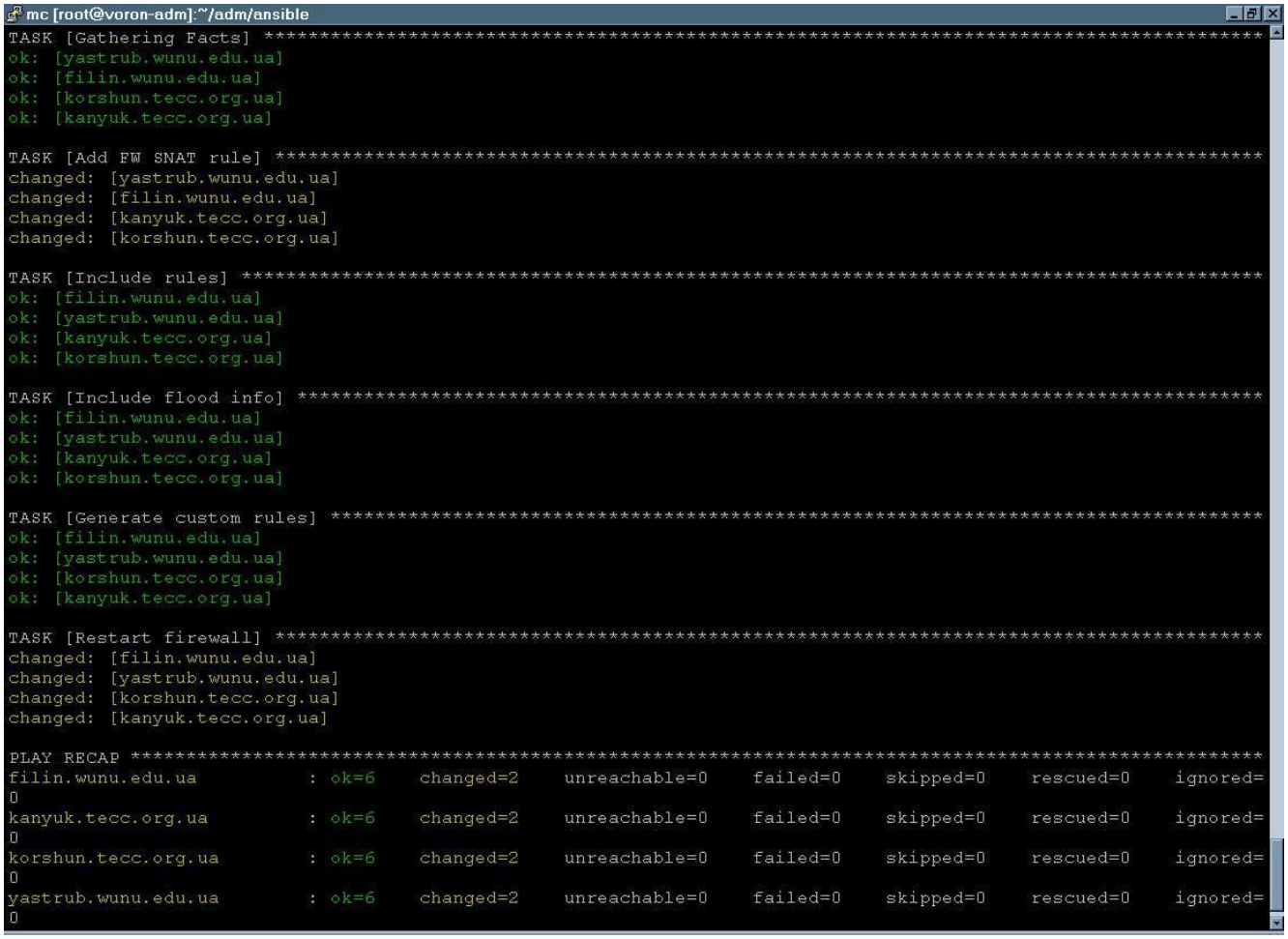


Рис.4.9. Перезапуск правил та синхронізація їх на всіх серверах міжмережевого екрану.

Крім фаєрволу, описаного вище, у корпоративній мережі ЗУНУ існує ще один апаратний міжмережевий екран фірми D-Link, а саме DFL-2500.

Брандмауер корпоративного класу D-Link DFL-2500 надає повний набір розширених функцій безпеки для управління, моніторингу та підтримки працездатної і захищеної мережі. Функції управління мережею включають в себе віддалене керування, політики контролю пропускної здатності, чорні/білі списки URL-адрес, політики доступу та SNMP. Для моніторингу мережі цей брандмауер

підтримує сповіщення електронною поштою, системні журнали, перевірку узгодженості та статистику в реальному часі.

Цей брандмауер забезпечує зв'язок IP-телефонії центрального офісу ЗУНУ з Тернополя із філіями по Україні.

На рисунку 4.10 представлено загальний вигляд панелі, коротку інформацію про конфігурацію, оновлення системи, завантаженість процесора, кількість підключень, кількість прописаних VLAN, кількість правил тощо.

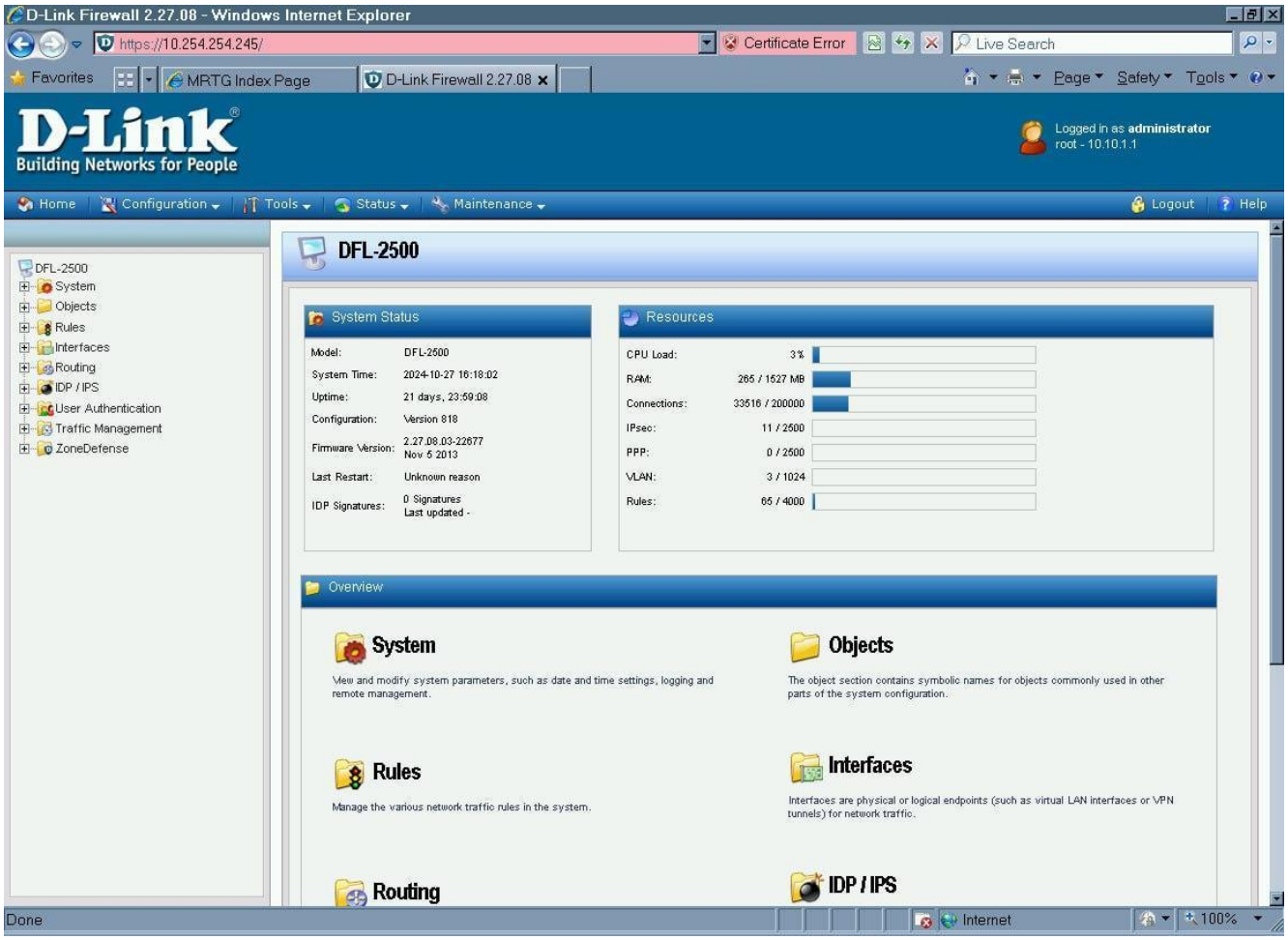


Рис. 4.10. Вид адміністративної панелі DFL-2500

На рисунку 4.11 показано системну інформацію про міжмережевий екран, зокрема інформацію про завантаженість процесора за останню добу, а також трафік, який проходив через брандмауер теж за останню добу.

На рисунках 4.12 та 4.13 показано проходження трафіка у мережу та вихід трафіка із мережі.

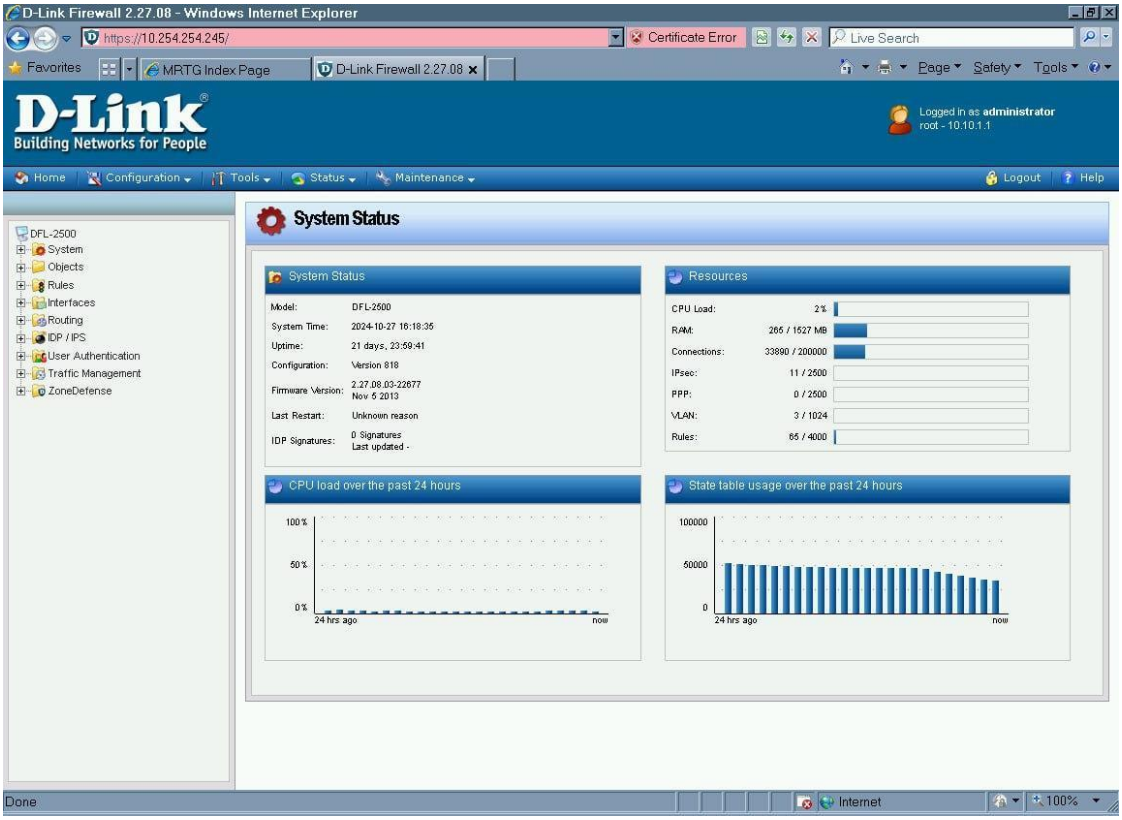


Рис. 4.11. Системна інформація на панелі адміністрування брандмауера

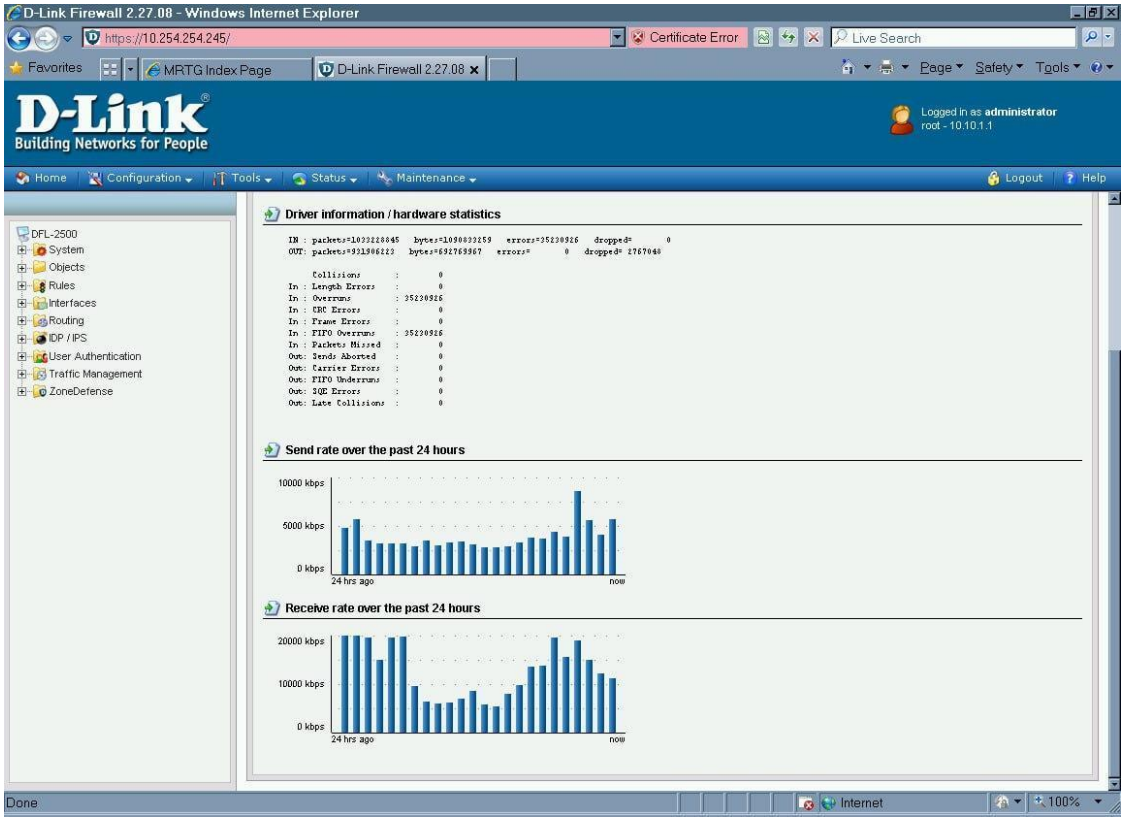


Рис. 4.12. Вхідний трафік у мережу

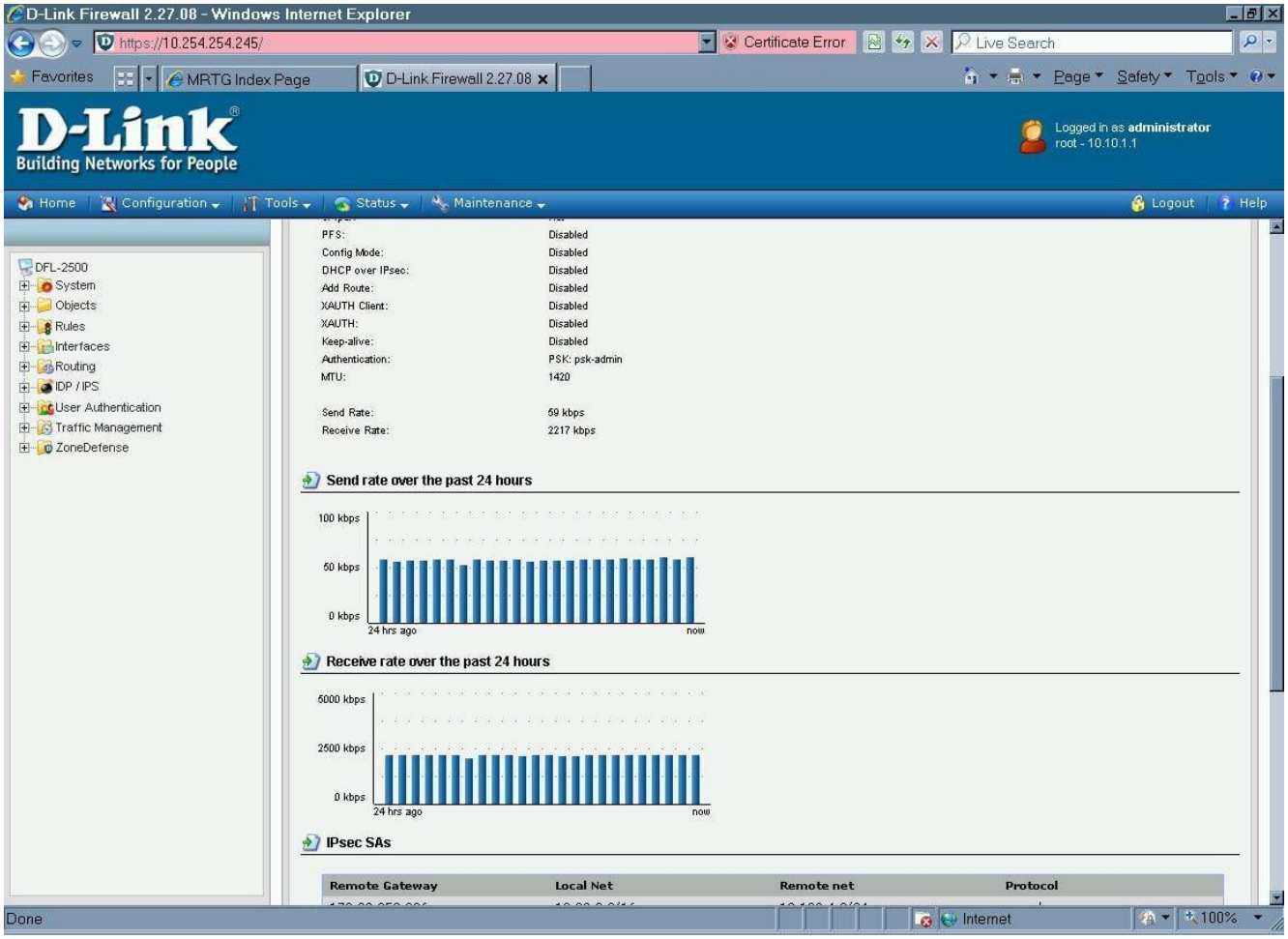


Рис. 4.13. Вихідний трафік із мережі

Після фільтрації трафіка на міжмережевому екрані він попадає в головний комутатор Cisco Nexus N5K-C5548UP.

Cisco N5K-C5548UP-FA – це шасі Nexus 5548 UP з 32 фіксованими уніфікованими портами, фронтальним повітряним потоком, 2 блоками живлення змінного струму потужністю 750 Вт, лотками для вентиляторів, 1 слотом розширення. Уніфіковані порти підтримують традиційний Ethernet, Fibre Channel (FC) і Fibre Channel через Ethernet (FCoE).

На рисунку 4.14 зображено команду, яка виводить на екран 30 VLAN перелік всіх серверів IP-телефонії ЗУНУ.

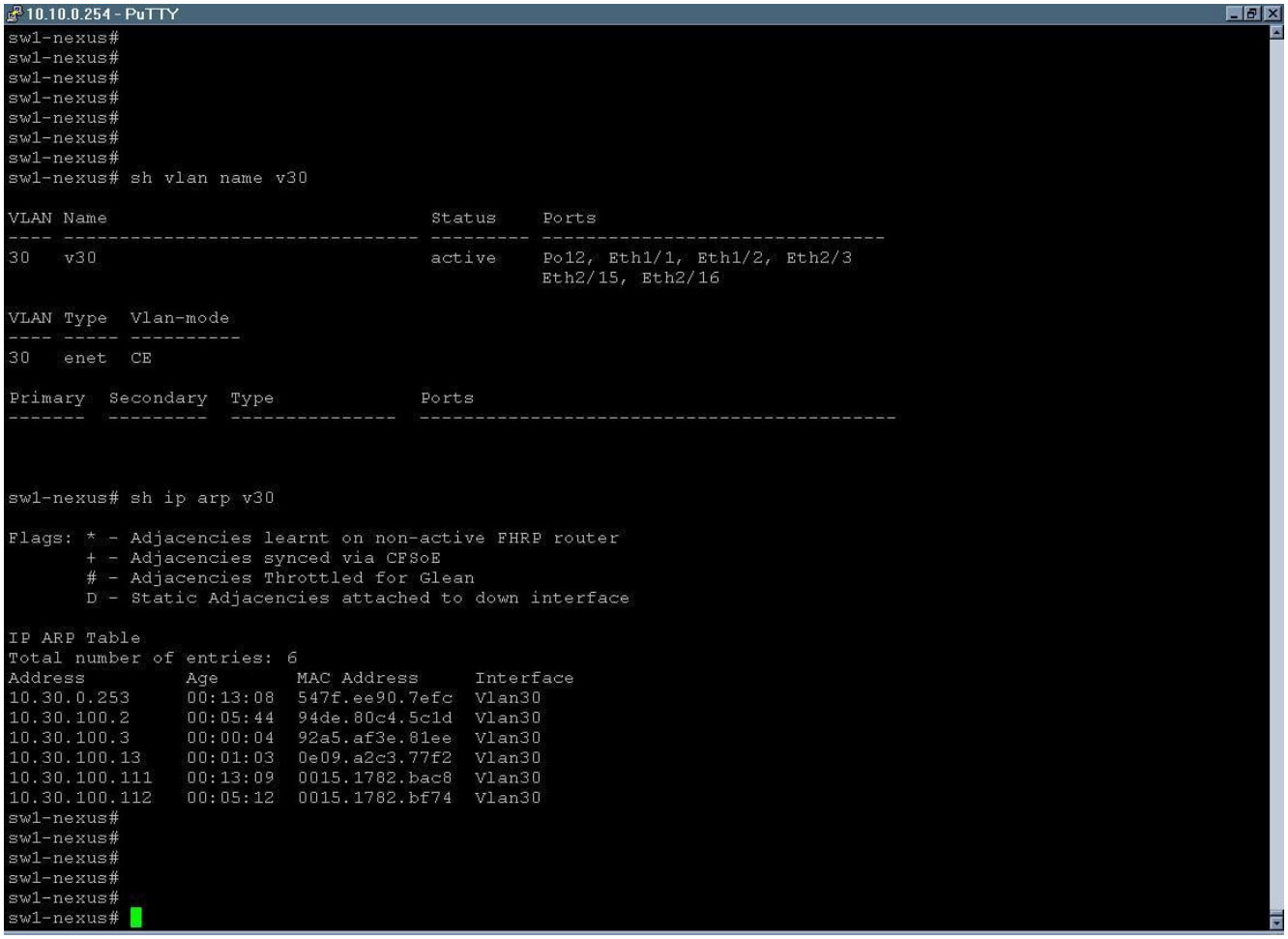


Рис.4.14. Виведення на екран серверів IP-телефонії

На рисунку 4.15 подано статистику по IP-адресах IP-телефонії університету, зокрема IP-адреса сервера, скільки часу він знаходиться у мережі, наведено його MAC-адреса та до якого VLAN він належить.

Після проходження комутатора трафік направляється до сервера IP-телефонії. В ЗУНУ сервер складається із двох серверів, які об’єднані в один кластер за допомогою Proxmox.

Двовузловий кластер Proxmox VE складається з двох серверів, підключених один до одного, здатних працювати разом, щоб забезпечити ресурси обробки та зберігання.

Розглянемо детальніше, з чого складається 2-вузловий кластер Proxmox VE, а також переваги, які він може запропонувати: безперервна синхронізація (або реплікація) між двома вузлами, оперативна міграція віртуальних машин (рис.4.16).

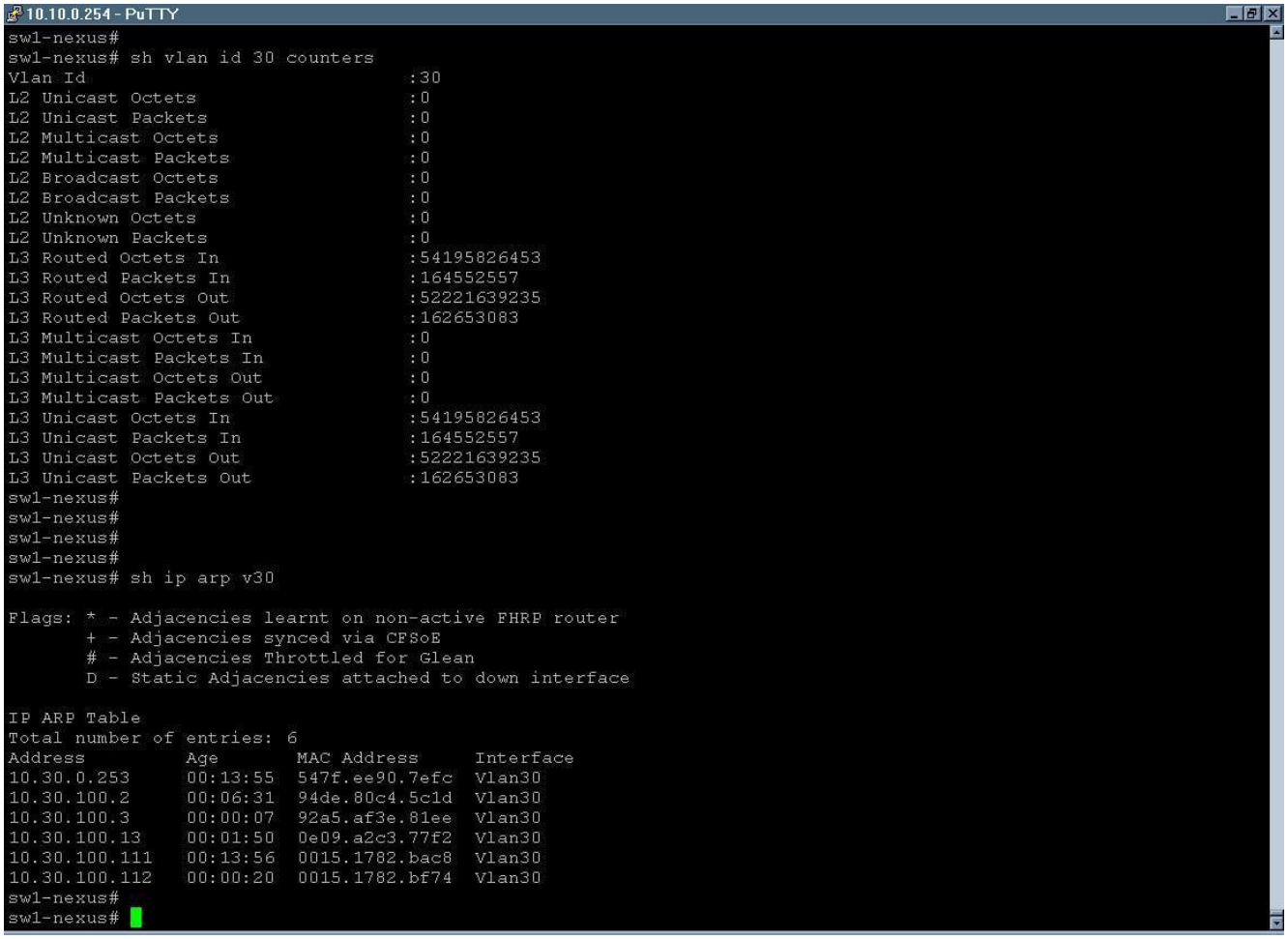


Рис. 4.15. Виведення на екран статистики по IP-адресах IP-телефонії

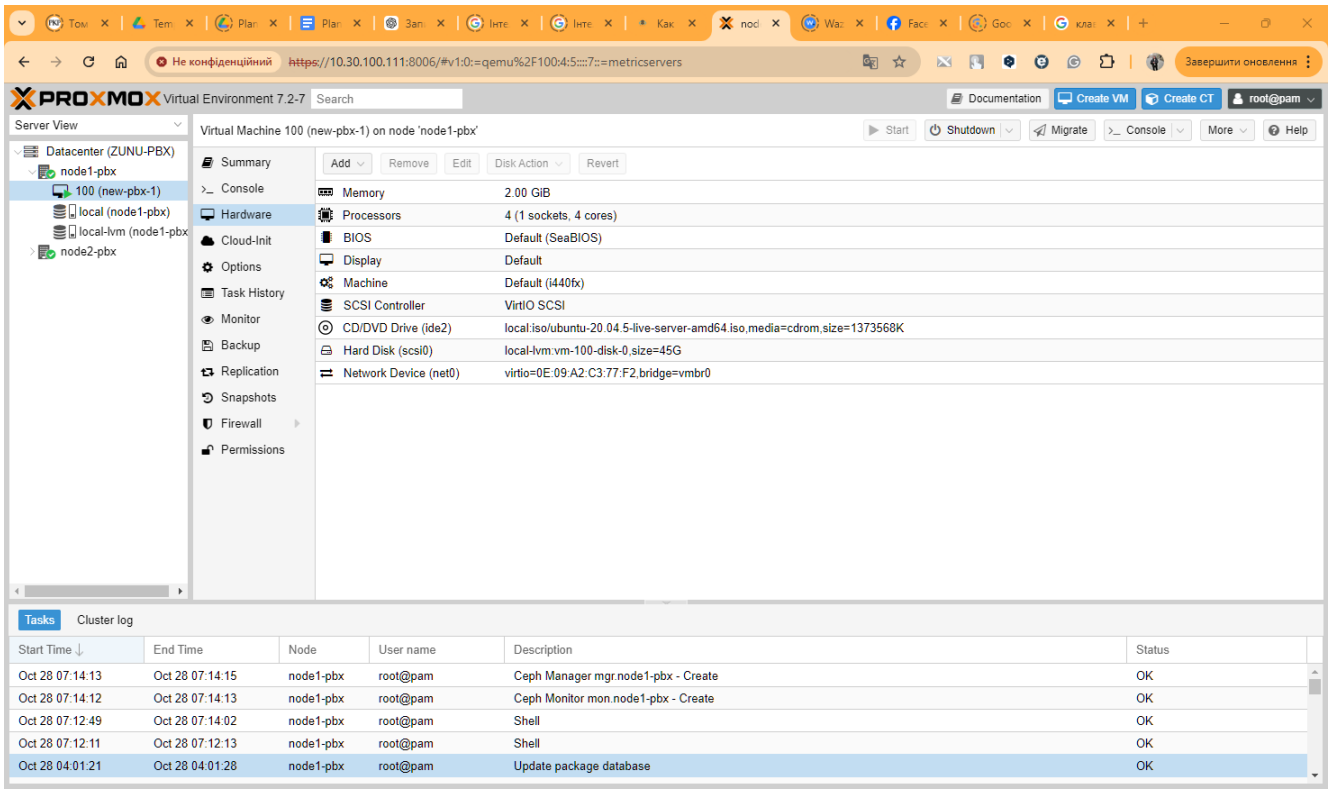


Рис. 4.16. Адміністративна панель Proxmox

Щоб створити взаємодію на рівні кластера між цими двома вузлами, необхідно встановити частоту синхронізації даних, яку називатимемо Delta T.

Delta T відноситься до різниці в часі між двома подіями, у цьому випадку синхронізації (або, як Proxmox називає «реплікації») даних між двома вузлами.

У реплікації даних між двома вузлами Delta T використовується для вказівки часу, що минув між останньою реплікацією даних і наступною. Іншими словами, Delta T вказує кількість часу, що минув між копіюванням даних з одного вузла на інший.

Значення Delta T можна змінювати за бажанням, але слід пам’ятати про апаратні характеристики хостів. Чим продуктивнішими є хости з апаратної точки зору, тим більше можливо буде встановити низьке значення Delta T і таким чином отримати дуже часті репліки.

На Delta T впливають такі фактори, як швидкість мережевого з’єднання між двома хостами, кількість даних, які потрібно синхронізувати, відстань між хостами та інші фактори. Таким чином, Delta T може змінюватися залежно від цих факторів.

Завдяки безперервній реплікації на рівні кластера між Node 1 і Node 2 поточні ресурси можна легко перенести з одного вузла на інший.

Жива міграція запущених віртуальних машин між вузлами, або «міграція на місці», дозволяє переміщувати віртуальний сервер з одного фізичного хоста на інший фізичний хост, не порушуючи роботу служб або програм на сервері.

Під час виконання міграції віртуальний сервер переміщується з першого хоста на другий через високошвидкісне мережеве з’єднання за підтримки Proxmox VE (віртуального середовища).

Під час процесу міграції віртуальні сервери продовжують нормально працювати без збоїв для кінцевих користувачів.

Поточна міграція ресурсів мінімізує час простою та покращує масштабованість системи, полегшуючи керування обчислювальними ресурсами та даними.

Це огляд базової конфігурації двовузлового кластера Proxmox VE.

Кластер Proxmox VE з двома вузлами також можна розширити або перетворити на багатовузловий кластер шляхом додавання додаткових вузлів, що гарантує гнучкість і масштабованість.

З точки зору бюджету, 2-вузловий кластер Proxmox VE дозволяє почати з базового рішення, яке можна розширити в майбутньому, постійно зберігаючи послуги.

Звернемо увагу ще на апаратне забезпечення розглядуваного кластера. Як показано на рисунку 4.17, сервер складається з двох процесорів Intel(R) Xeon(R) CPU E5405 2.00GHz по 4 ядра на кожен процесор 4 Гб оперативної памяті.

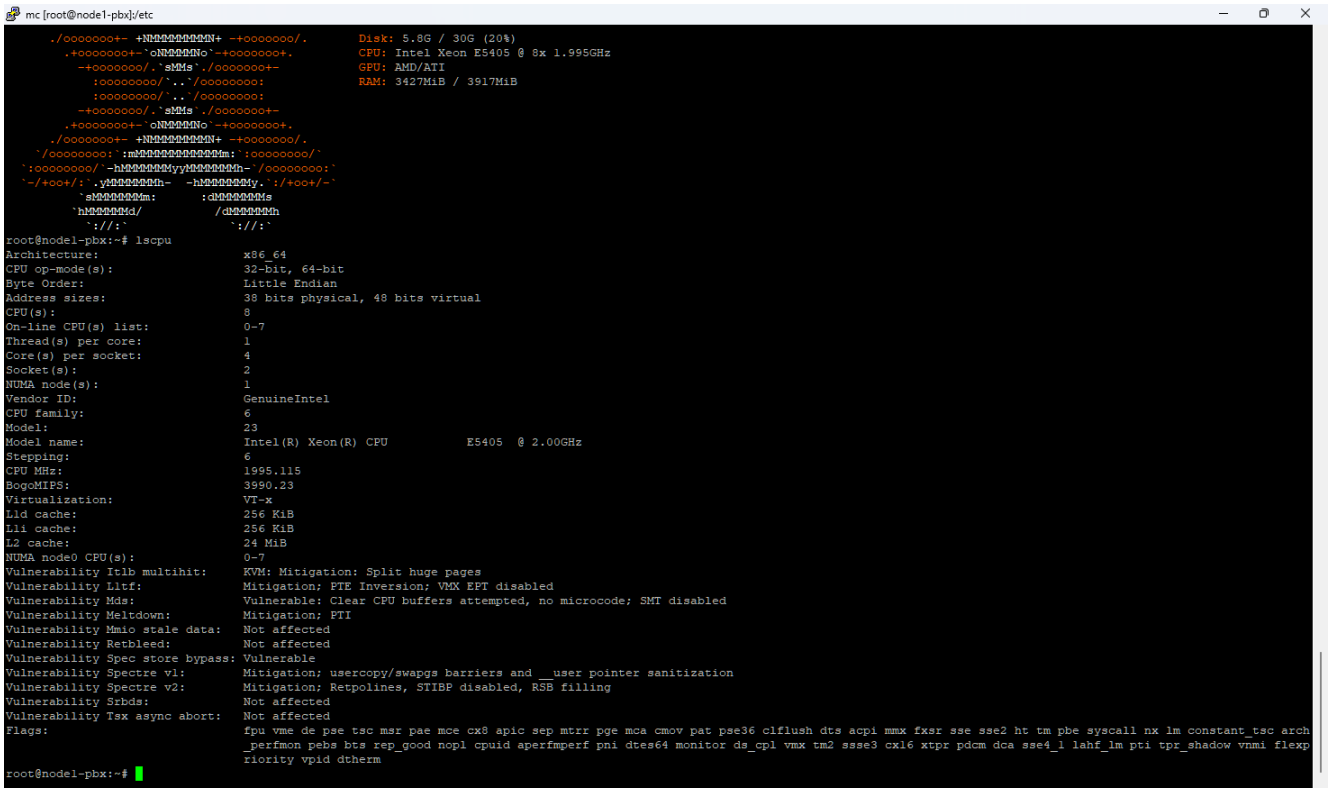


Рис. 4.17. Апаратна частина сервера Node 1 IP-телефонії

За допомогою команди ***htop*** можемо в режимі реального часу переглянути використання ресурсів та процеси, запущені на даний момент (рис. 4.18).

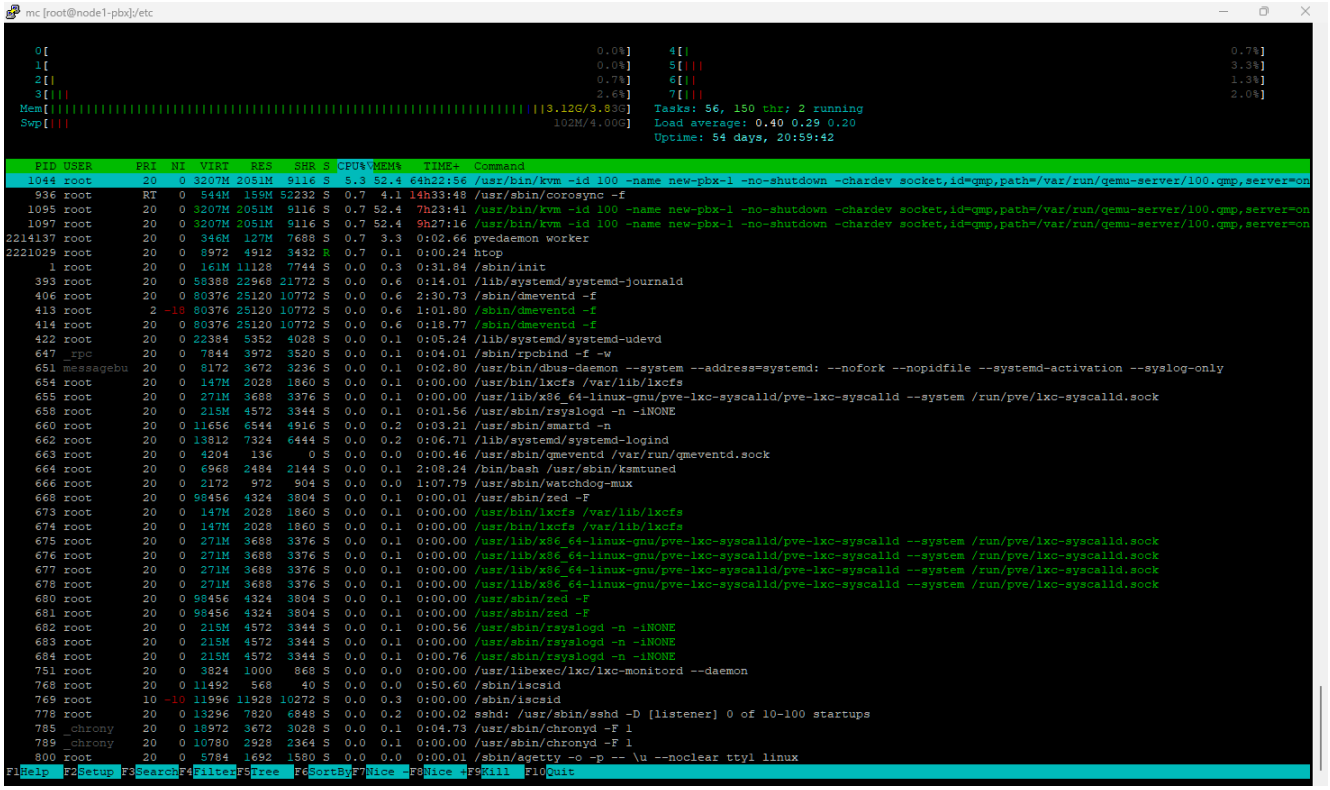


Рис. 4.18. Використання сервером Node 1 ресурсів у реальному часі

Трафік, виходячи із вище описаного кластеру, попадає напряму у комутатор D-Link DGS-3024.

DGS-3024, гігабітний комутатор рівня 2, призначений для підключення підрозділів, має 24 порти 10/100/1000BASE-T для підключення до мідної гігабітної мережі, а також 4 комбінованих SFP для гнучкого підключення до оптоволоконної магістралі. Потужний, цей комутатор забезпечує гігабітну швидкість для настільних комп'ютерів і серверів, надаючи при цьому всі необхідні функції, такі як транкінг портів, VLAN, черги пріоритетів і резервне живлення, щоб дозволити ефективно розгорнути комутаційну мережу без вузьких місць для легкої інтеграції з мережею (рис.4.19).

Це досить гнучкий комутатор в налаштуванні. Завдяки 24 портам 10/100/1000BASE-T з автоматичним визначенням у низькопрофільному корпусі, цей комутатор є економічно ефективним рішенням для гігабітних мереж. Всі порти підтримують автоматичний MDI/MDIX, що дозволяє підключатися до робочих станцій і серверів з будь-якого порту без необхідності змінювати звичну

виту пару на мережеві кабелі. На рисунку 4.20 подано опис підключених портів в реальному режимі.

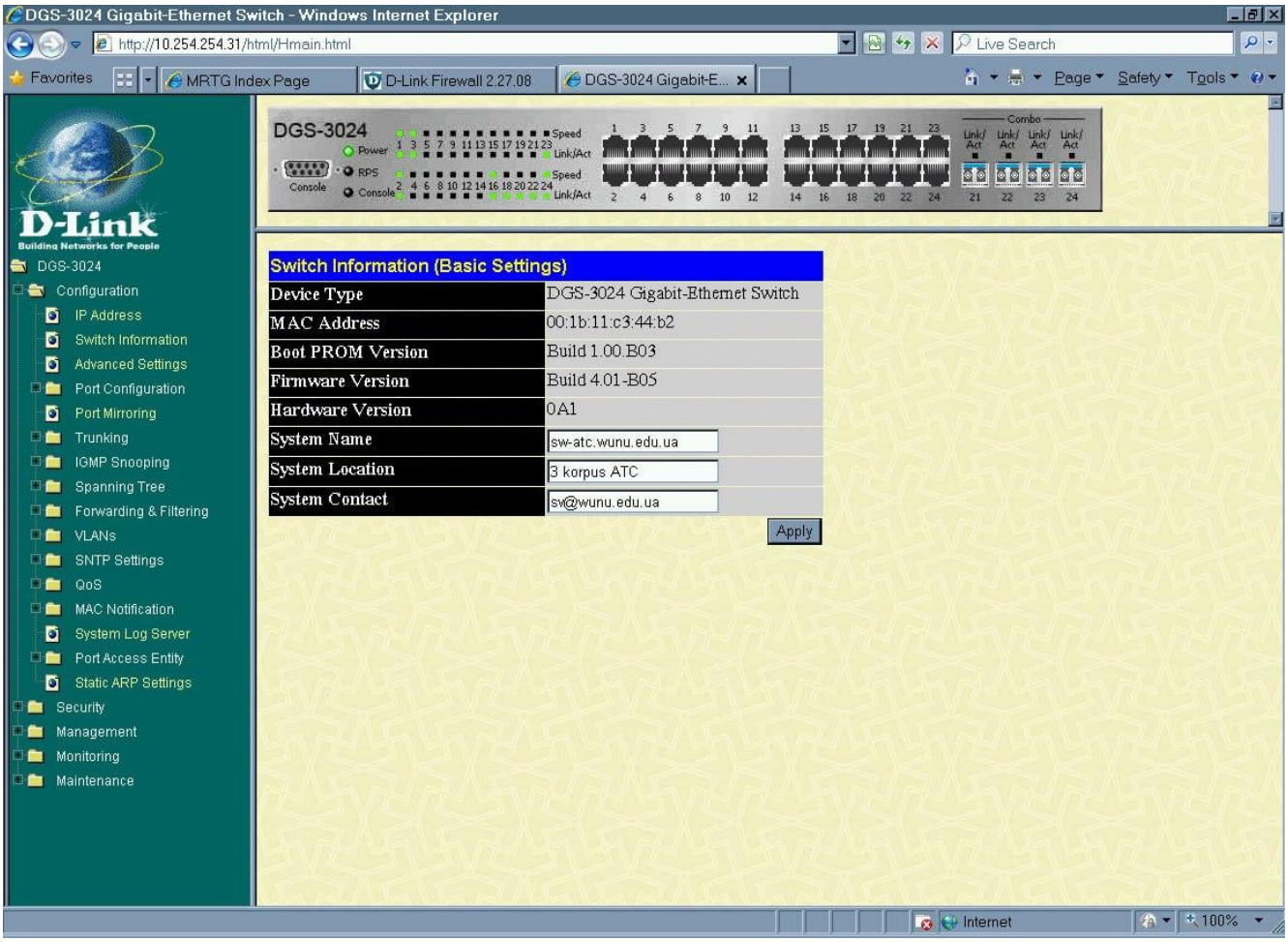


Рис. 4.19. Адміністративна панель комутатора DGS-3024

Розроблений як економічно ефективний керований комутатор для відомчих з'єднань, DGS-3024 надає всі базові функції безпеки і якості обслуговування (QoS), включаючи 802.1Q VLAN, GVRP, пріоритетні черги 802.1p, управління доступом 802.1x і захист від широкомовного шторму. Ці функції полегшують розгортання офісних додатків, таких як Інтернет-телефонія VoIP і потокове мультимедіа.

Комутатор DGS-3024 підтримує функцію агрегації каналів 802.3ad, що дозволяє об'єднати кілька портів у багатоканальне з'єднання для підвищення пропускної здатності для підключення до серверів або магістралі мережі. Для забезпечення надлишковості комутатор підтримує технологію 802.1 Spanning

Tree для створення резервних мостових шляхів і може бути підключений до зовнішнього джерела живлення для збільшення часу безвідмовної роботи мережі. У разі виходу з ладу вбудованого внутрішнього джерела живлення, резервний блок живлення автоматично забезпечить необхідну потужність для забезпечення безперервної роботи. На рисунку 4.21 зображено статистику прийому трафіка по першому порту, де підключений один із серверів IP-телефонії а на рисунку 4.22 - статистику передачі трафіка по першому порту, де підключений один із серверів IP-телефонії.

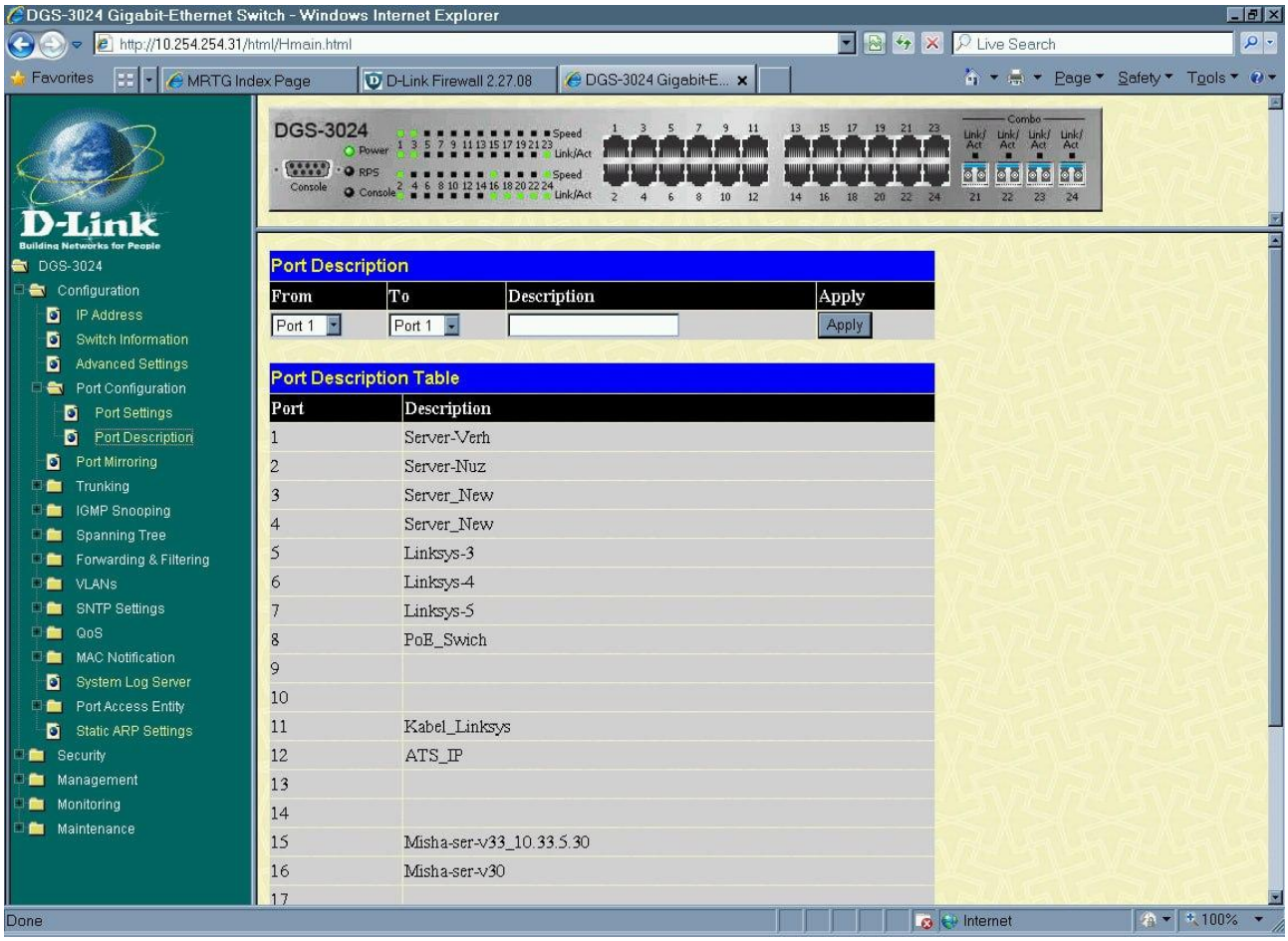


Рис. 4.20. Опис підключених портів

DGS-3024 відповідає сучасним різноманітним вимогам та, завдяки надійній підтримці стандартних протоколів мережевого управління (SNMP/RMON/BOOTP/ Telnet/Web) і дзеркалювання портів, може бути легко інтегрований з більшістю сторонніх продуктів для керування мережею.

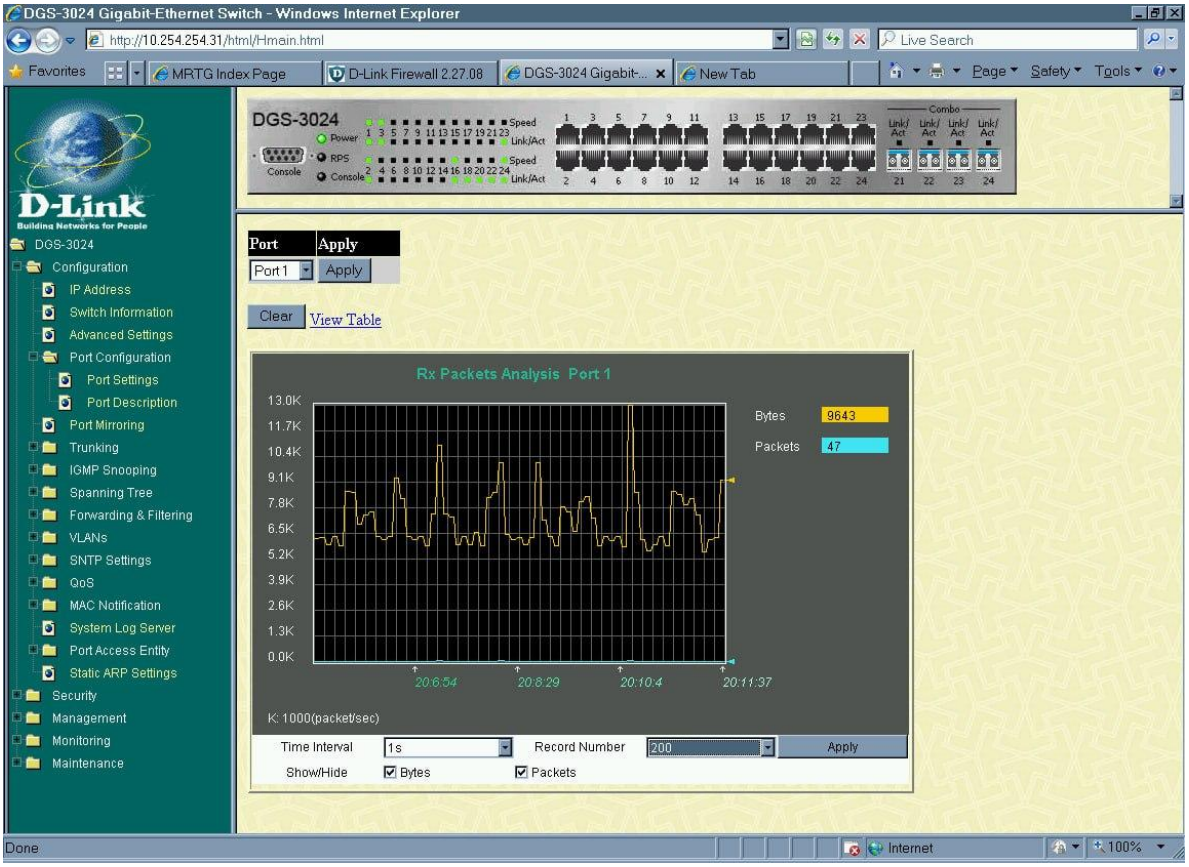


Рис.4.21. Статистику прийому трафіка по першому порту

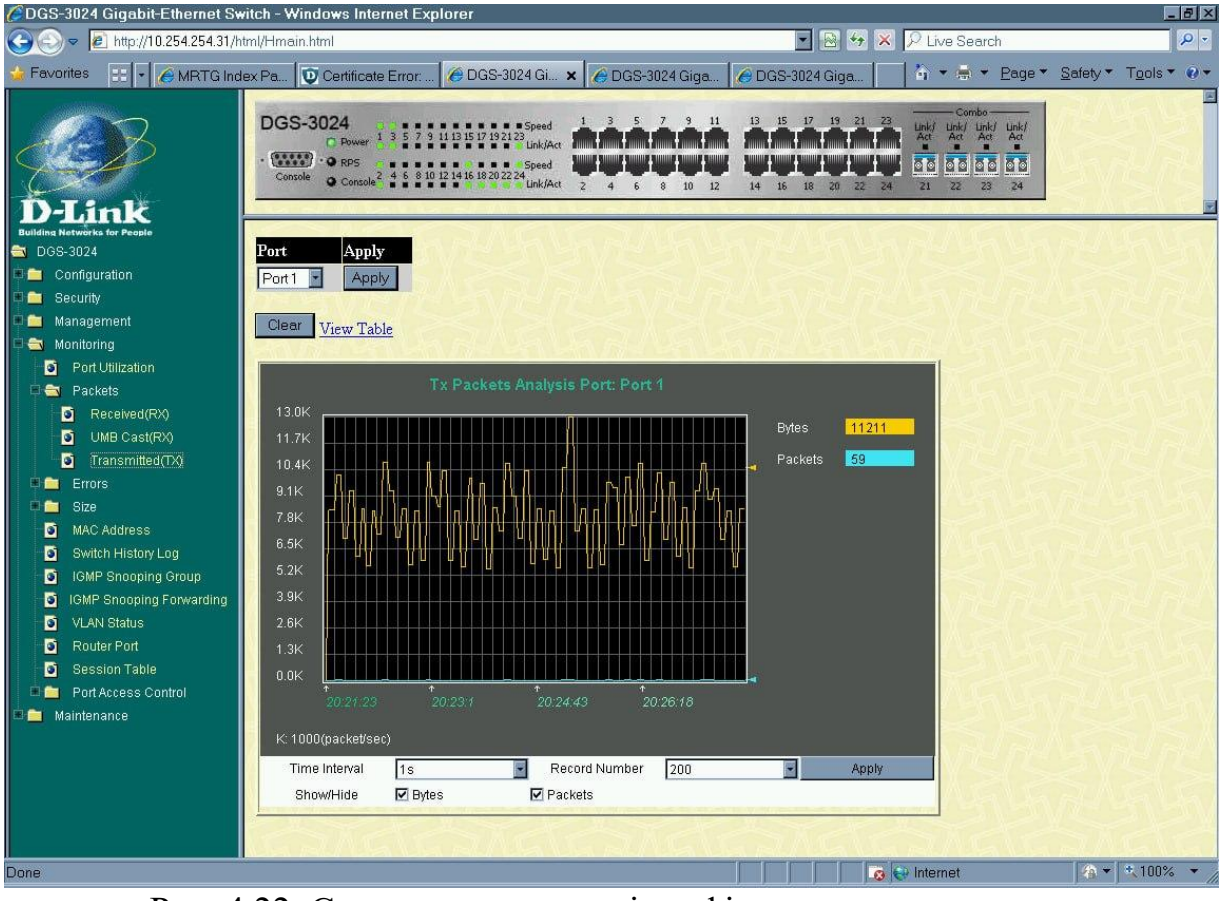


Рис. 4.22. Статистику передачі трафіка по першому порту

4.2 Розподіл доступу користувача до мережі IP-телефонії

Розглянемо застосування нечіткої логіки для захисту від термінації трафіку в IP-телефонії. Основною метою є розробка нечіткої системи, яка забезпечує розподіл доступу в режимі реального часу, враховуючи різні критерії.

Основні переваги нечітких систем порівняно з іншими полягають у наступному:

- здатність працювати з вхідними даними, які визначені нечітко, наприклад, зі значеннями, що постійно змінюються з часом (динамічні завдання);
- можливість нечітко формулювати критерії оцінки та порівняння;
- здатність проводити якісну оцінку як вхідних даних, так і результатів, оскільки система працює не лише з числовими значеннями, а й враховує їх ймовірність та її розподіл;
- можливість швидкого моделювання складних динамічних процесів чи систем та виконання їх порівняльного аналізу з заданою точністю.

У інженерних завданнях зазвичай застосовується механізм нечіткого висновку Мамдані [11-13]. Він базується на мінімаксній композиції нечітких множин. Цей механізм включає наступні кроки [12]:

1. Фазифікація: визначаються ступені істинності, тобто значення функцій належності для кожного правила-передумови.
2. Нечіткий висновок: спочатку знаходять мінімальний рівень "відсічення" для лівої частини кожного правила, після чого визначають "усічені" функції належності висновку.
3. Композиція або об'єднання отриманих "усічених" функцій, що виконується за допомогою максимальної композиції нечітких множин.
4. Дефазифікація або перетворення в чітке значення. Існує кілька методів дефазифікації, таких як метод середнього центру або центроїдний метод. Геометрично це означає знаходження центру ваги для кривої функції належності отриманого результату.

На вхід пропонованої нечіткої системи поступають критерії здійсненого дзвінка, які опрацьовуються підсистемою розподілу доступу на основі механізму нечіткого висновку Мамдані [12].

Моделювання нечіткої системи здійснено за допомогою Fuzzy Logic Toolbox середовища MATLAB. На вхід такої системи надходять значення рівня довіри клієнта по його IP-адресі (*IP-identification*), часу здійснення дзвінка клієнтом (*client-call-time*), часового поясу адресата дзвінка (*addr-call-time*) та якості зв'язку мережі клієнта (*connection-quality*).

Загальний вигляд запропонованої нечіткої системи подано на рисунку 4.23

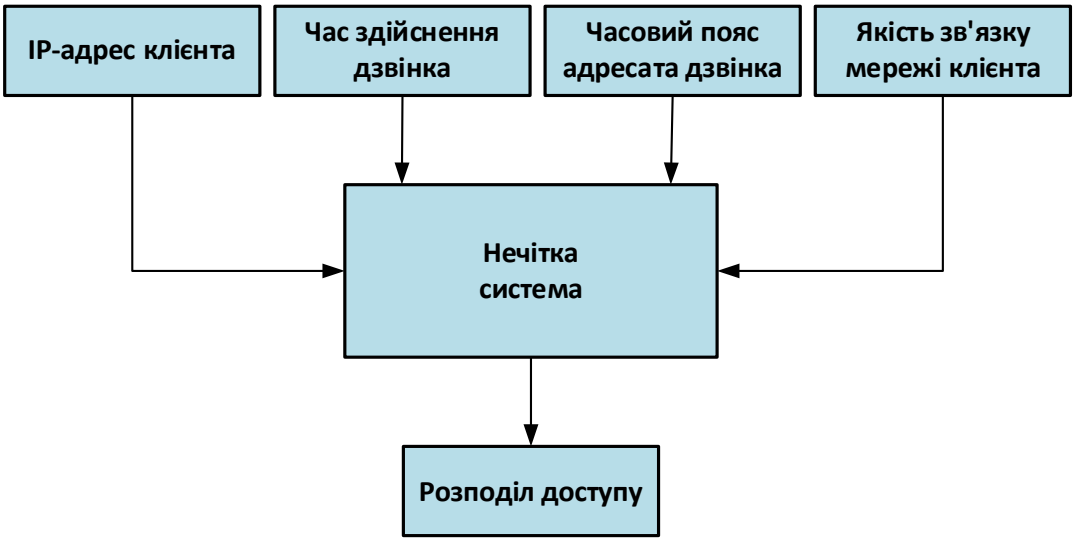


Рис. 4.23 Загальна схема нечіткої системи розподілу доступу в IP-телефонії

Кожна із вхідних змінних демонструє дані з певного діапазону. Над цими даними здійснюється фазифікація, тобто переведення кількісних значень у якісні.

Значення функцій належності вхідних змінних задається дзвоноподібною, а вихідної змінної – трапецевидною функцією [11].

Дзвоноподібна функція задається трьома числами (a, b, c), що відповідають абсцисам крайніх точок та центру кривої:

$$MF(x) = \frac{1}{1 + \left| \frac{x - c}{a} \right|^{2b}}. \quad (3.1)$$

Функції належності вхідної змінної *IP-identification* відображаються трьома множинами: *low*, *middle*, *high*, що відображають відповідно низький, середній та високий рівень довіри клієнта IP-телефонії. Цей показник легко можна сформувати зі статистичних даних IP-адреси клієнта, його присутності в IP-телефонії, здійснених атак чи наявності збоїв при здійсненні дзвінків та правах доступу, наданих йому адміністратором мережі. Для зручності вибрано інтервал задання значень цієї змінної [0, 1]. Функції належності змінної *IP-identification* подано на рисунку 4.24.

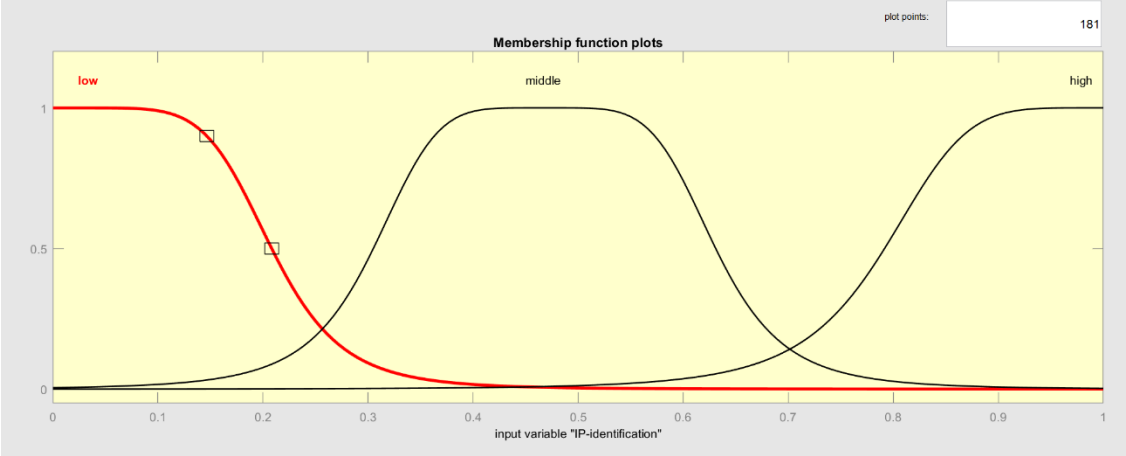


Рис. 4.24. Функції належності змінної *IP-identification*

Функції належності змінної *connection-quality*, що відображає якість зв'язку мережі, з якої здійснює запит до IP-телефонії на дзвінок клієнт, аналогічно поділені на три інтервали *low*, *middle*, *high*, що задані на відрізку [0, 1] (рисунок 4.25). Низька якість зв'язку може бути у мобільних мережах через різницю у покритті та якості надання послуг мобільними операторами. Середня якість зв'язку, як правило, можлива при застосуванні користувачем регіональної мережі Інтернет, а висока якість забезпечується використанням клієнтом локальної мережі.

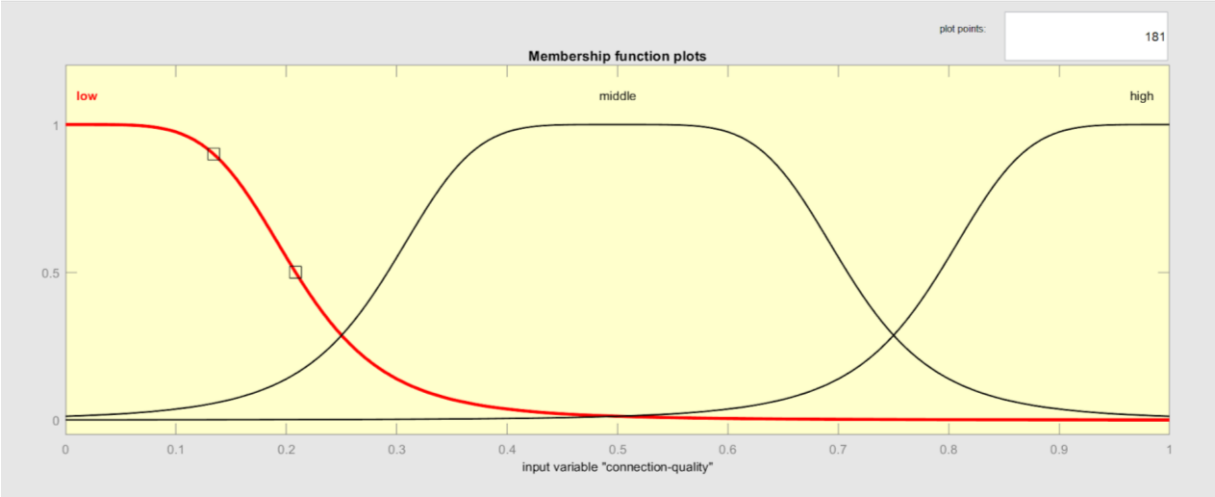


Рис. 4.25 Функції належності змінної *connection-quality*

Для задання функцій належності змінної *client-call-time*, що показує час здійснення дзвінка клієнтом в інтервалі [0, 24], пропонується на три діапазони *morning, work time, night* (рисунок 4.26).

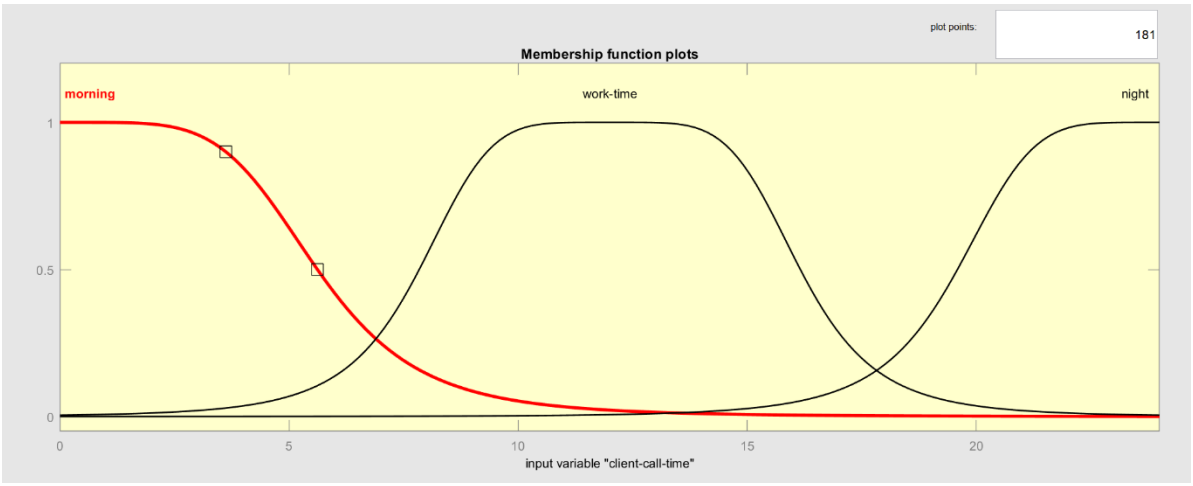
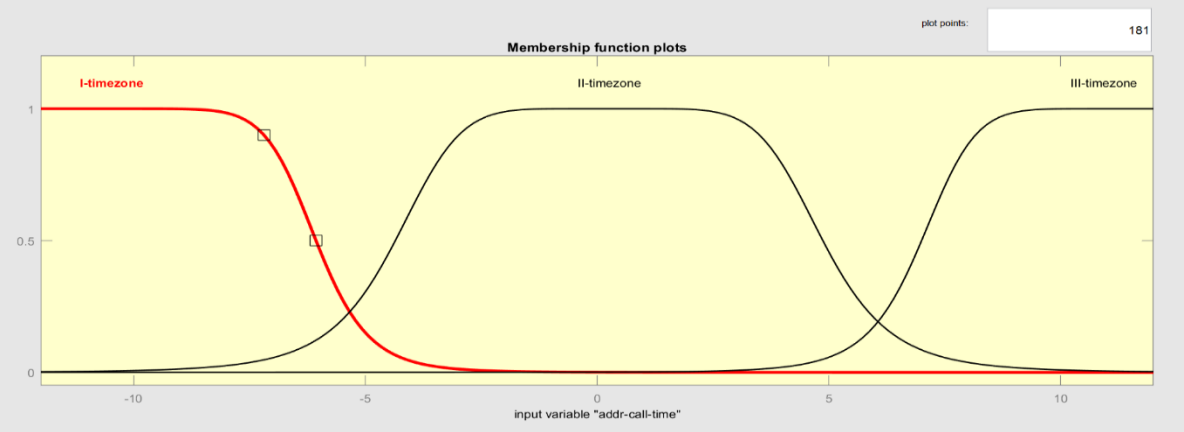


Рис. 4.26. Функції належності змінної *client-call-time*

Змінна *addr-call-time* відображає часові пояси світу, які поділені на три зони (*I-timezone*, *II-timezone*, *III-timezone*), які подані на інтервалі [-12, 12] та

враховуються при побудові бази правил відносно часу здійснення дзвінка клієнта (рисунок 4.27).

Рис. 4.27. Функції належності змінної *addr-call-time*



Трапецевидна функція задається четвіркою чисел (a, b, c, d), які позначають абсциси вершин трапеції, заданої функцією:

$$MF(x)=\begin{cases}\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ \dfrac{x-c}{d-c}, c\le x\le d\\ 0, \text{в інших випадках}\end{cases}. \quad (3.2)$$

Функції належності для вихідної змінної *access* позначаються двома трапецевидними інтервалами *deny*, *allow* для точного визначення центру ваги, що позначає нечіткий висновок системи (рисунок 4.28).

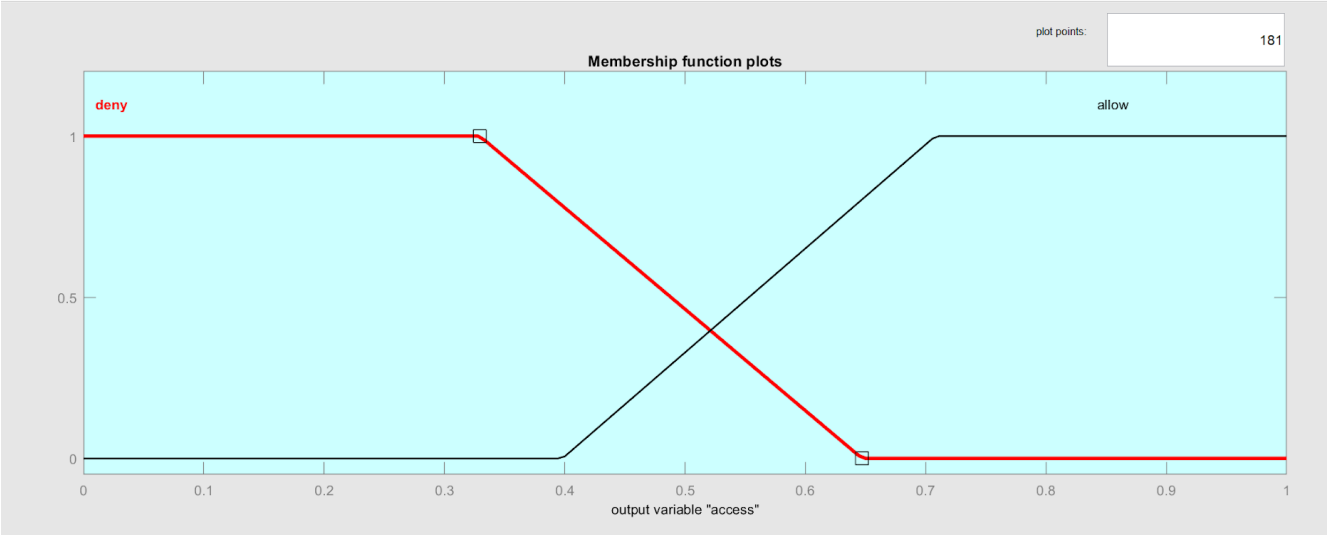


Рис. 4.28. Функції належності вихідної змінної *access*

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то» [12], усі вхідні змінні мають по три нечітких стани і ще один стан *none*, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий при функціонуванні системи IP-телефонії, тому кількість правил нечіткого висновку досліджуваної системи 4•4•4•4-1=255.

Нечіткий висновок підсистеми розподілу доступу, побудованого на основі заданих 255 правил з поточними значеннями вхідних та вихідної змінних, має вигляд, фрагмент якого представлений на рисунку 4.29.

На рисунку 4.29 зображено випадок, коли клієнт, рівень довіри якого низький, здійснює дзвінок у ранковий час в країну, яка має той самий часовий пояс, що і Україна, і якість зв’язку свідчить, що дзвінок здійснюється з локальної мережі. Висновок запропонованої нечіткої системи в даному випадку становить 0.48, що відповідає дозволу на здійснення даного дзвінка. Даний приклад підтверджує правильність роботи сформованої бази правил. Перевірка інших комбінацій значень вхідних змінних демонструє правильність роботи такої нечіткої системи.

Запропонована нечітка система може реалізовуватися як програмно, так і апаратно у вигляді нечіткого контролера для успішного захисту від термінації трафіку.

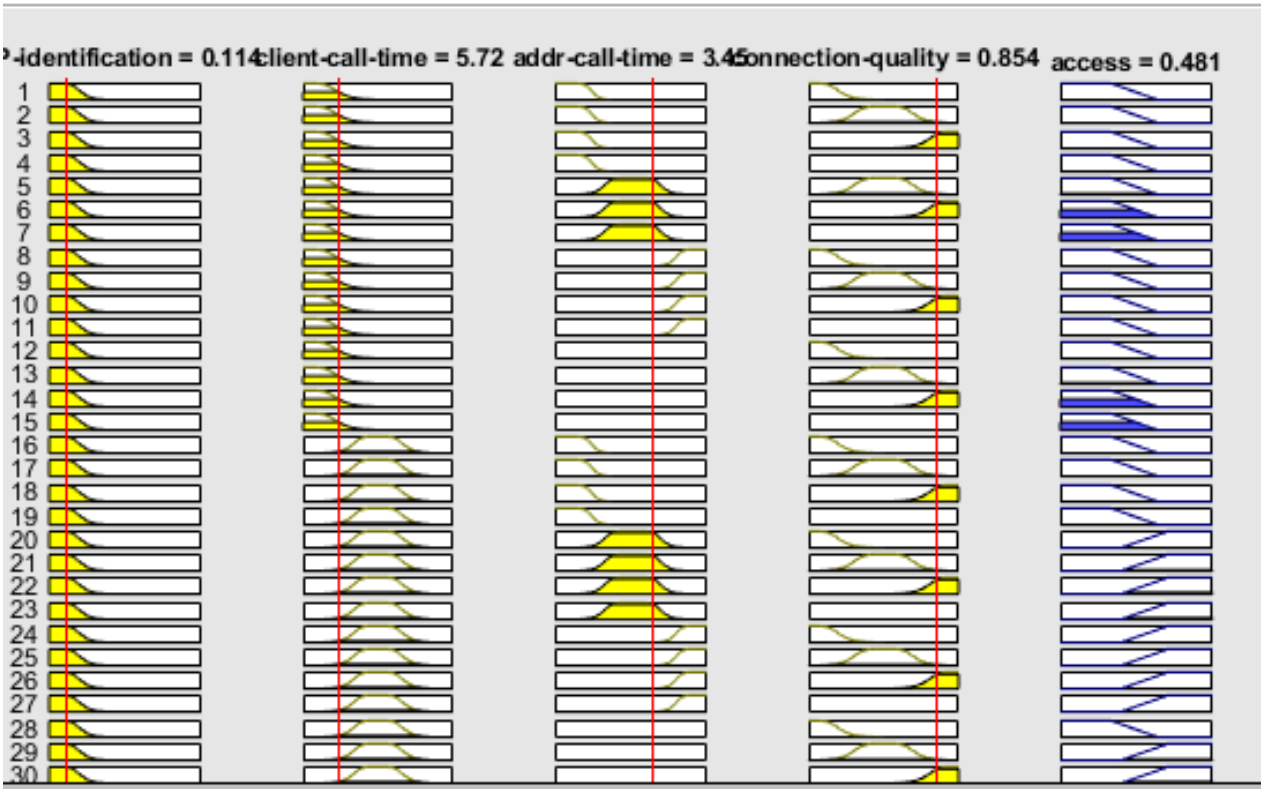


Рис. 4.29 Нечіткий висновок підсистеми розподілу доступу в IP-телефонії

Нечіткий контролер – це регулятор, який використовує принципи нечіткої логіки для керування складними системами. На відміну від традиційних контролерів, які працюють на основі точних математичних моделей, нечіткий контролер здатен працювати з невизначеними, неповними або нечіткими даними, імітуючи процес прийняття рішень, характерний для людини. Нечіткі контролери зазвичай застосовуються в задачах, де складно або неможливо побудувати точну математичну модель процесу.

Запропонована нечітка система для захисту термінації трафіку в IP-телефонії продемонструвала свою ефективність. Завдяки використанню механізму нечіткого висновку Мамдані, система здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних. Це дозволяє враховувати численні критерії, такі як IP-адреса клієнта, час здійснення дзвінка, часовий пояс і якість зв’язку, що сприяє підвищенню рівня безпеки та якості зв'язку.

4.3 Програмна реалізація методів автоматизованого наповнення онтології та виявлення аномальних повідомлень у IP-телефонії

4.3.1Автоматизоване наповнення онтології тематичних повідомлень в корпоративній системі VoIP

Для реалізації автоматизованого наповнення онтології тематичних повідомлень в корпоративній системі VoIP використано мову програмування Python та спеціалізовану бібліотеку Pandas для обробки та аналізу даних, що надає зручні й ефективні структури даних та інструменти для роботи з ними. Для збереження сформованих онтологічних структур використовується СУБД MySQL.

На рисунку 4.34 наведено інтерфейс аналізу ключових понять в окремих повідомленнях, які сформовані в процесі експлуатації засобів корпоративної IP-телефонії.

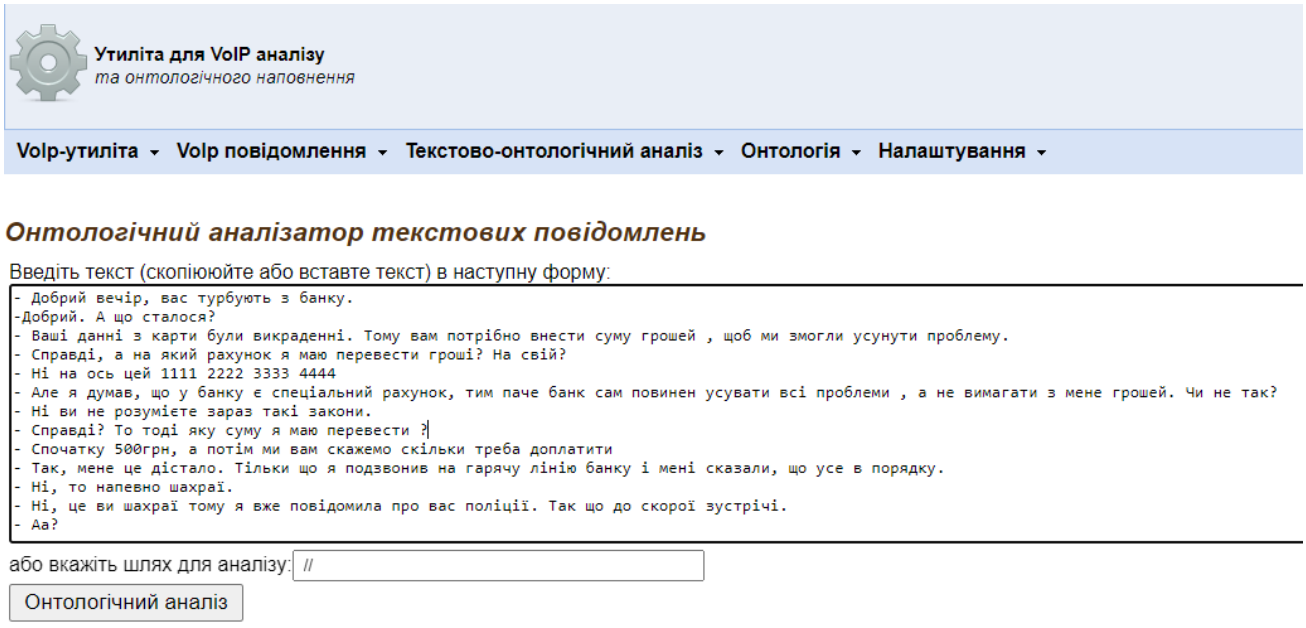


Рис. 4.34. Інтерфейс підсистеми аналізу ключових понять у VoIP повідомленнях

Після виконання процедури попереднього онтологічного аналізу, описаної вище і програмно реалізованої в системі, отримаємо результат, представлений на рисунку 4.35.

Сервіс дозволяє знайти ключові поняття в даному повідомленні, визначити необхідні коефіцієнти та, відповідно, дозволяє сформувати інформацію або для занесення в онтологічне представлення аналізованої області, або сформує схему для порівняння з формалізованими еталонними повідомленнями для виявлення аномальності такого повідомлення.

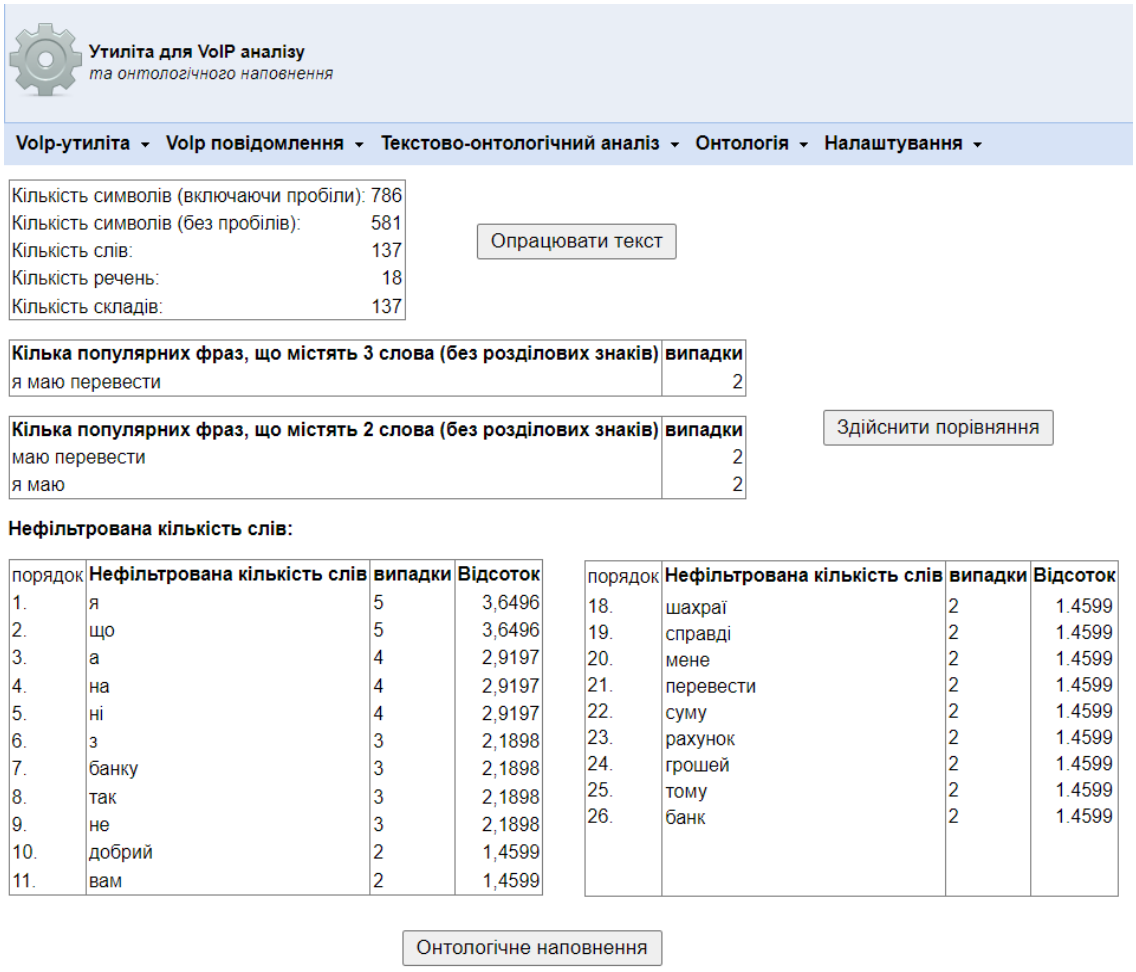


Рис. 4.35. Інтерфейс підсистеми аналізу ключових понять у VoIP повідомленнях та формування необхідних вагових коефіцієнтів для прийняття рішень

В процесі апробації запропонованих методів було здійснено інтеграцію даної інтелектуалізованої підсистеми в діючу корпоративну VoIP систему Західноукраїнського національного університету.

На рисунку 4.36 представлено сторінку, яка, окрім підсистеми аналізу ключових понять у VoIP, включає також модуль для перетворення голосових повідомлень в текстові представлення і адміністративний модуль, що використовується для прийняття рішень відносно користувачів системи та відповідне управління виявленими аномальними повідомленнями.

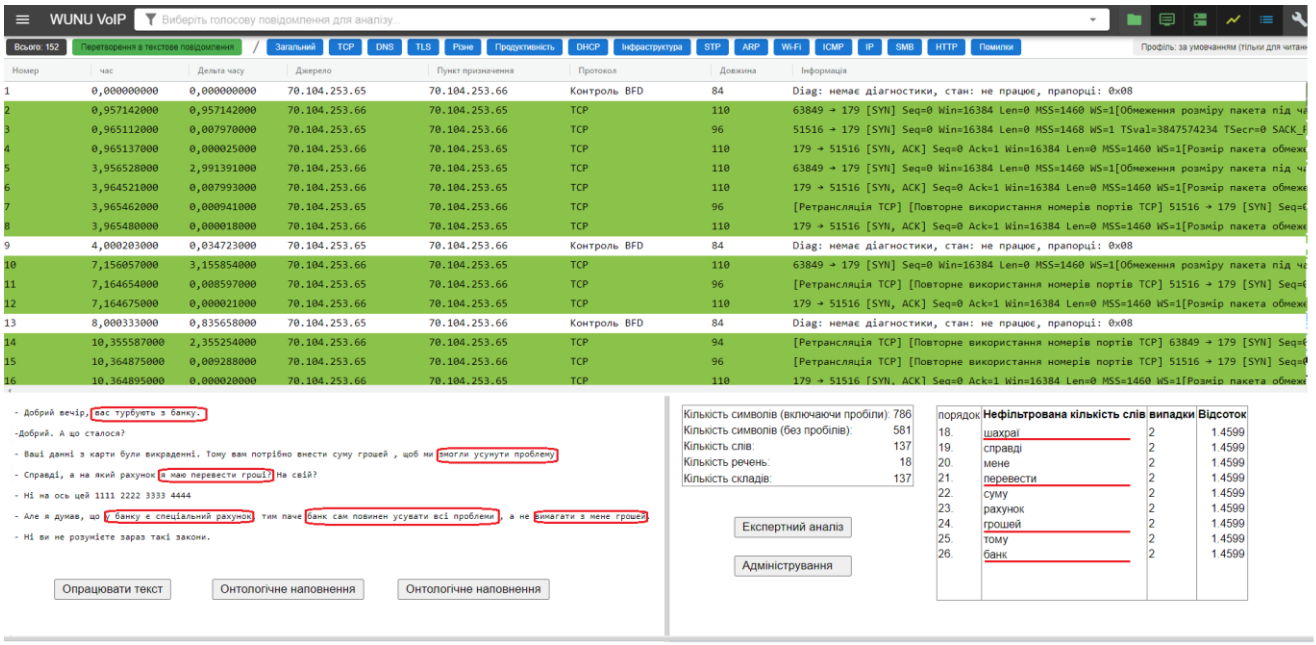


Рис. 4.36. Інтерфейс інтеграції підсистеми аналізу VoIP повідомлень в систему управління корпоративною IP-телефонією

Дана інтеграція може також використовуватися і для виявлення голосових повідомлень, які здійснюють користувачі при дзвінках на платні сервіси, що також є дуже актуальним питанням в системі практичного використання IP-телефонії.

4.3.2 Виявлення аномальних повідомлень у IP-телефонії

Зв'язок мережі із зовнішнім світом виконується за допомогою технології SIP-транк. Він встановлює, починає і завершує, сеанс в мережі, не бере участі в передачі голосу, а лише надає умови та способи для обміну інформацією, причому на основі інших протоколів.

Далі відбувається аутентифікація по IP-адресі. Автентифікація за IP-адресою – це метод контролю доступу на мережевому рівні, який задовольняє або відхиляє запит клієнта, ґрунтуючись виключно на його вихідній IP-адресі. Фільтр аутентифікації IP-адреси використовує значення, збережене в http. запит. Атрибут повідомлення clientaddr для визначення дозволу чи заборони доступу містить адресу віддаленого хоста з TCP-сокета, який використовується в з'єднанні між клієнтом і шлюзом API.

Як видно із рисунка 4.22, вхідний дзвінок приходить на сервер Asterisk, де він перевіряється, чи є така IP-адреса у базі даній і чи дозволити це з'єднання.

```
== Using SIP RTP CoS mark 5
  -- Called SIP/0352517585@komisiya_server
     > 0x7f941c0749d0 -- Strict RTP learning after remote address set to: 10.11.0.251:18636
  -- SIP/komisiya_server-0000172a answered SIP/ukrtel-00001729
  -- Executing [s@macro-otvet:1] NoOp("SIP/komisiya_server-0000172a", " ANSWERED call to 0352517585 ") in new stack
  -- Channel SIP/komisiya_server-0000172a joined 'simple_bridge' basic-bridge <5daea763-e46d-4fd8-9fde-f2e51df3f84b>
  -- Channel SIP/ukrtel-00001729 joined 'simple_bridge' basic-bridge <5daea763-e46d-4fd8-9fde-f2e51df3f84b>
     > Bridge 5daea763-e46d-4fd8-9fde-f2e51df3f84b: switching from simple_bridge technology to native_rtp
     > Locally RTP bridged 'SIP/ukrtel-00001729' and 'SIP/komisiya_server-0000172a' in stack
     > 0x7f94380a0c70 -- Strict RTP switching to RTP target address 195.5.0.213:42544 as source
```

Рис. 4.37. Приклад входу IP-адреси Укртелекому в мережу університету

На рисунку 4.38 більш детальніше розкрито весь процес аутентифікації входу IP-адреси 195.5.0.213 в мережу ЗУНУ, використовуючи протокол RTP. При вході в мережу ЗУНУ система використовує Secure Real-Time Transport Protocol (SRTP) – це розширення RTP, яке додає шифрування, аутентифікацію та захист від повторного відтворення. Це означає, що всі дані, які передаються через SRTP, захищені від підслуховування і підробки, що критично важливо для конфіденційних комунікацій.

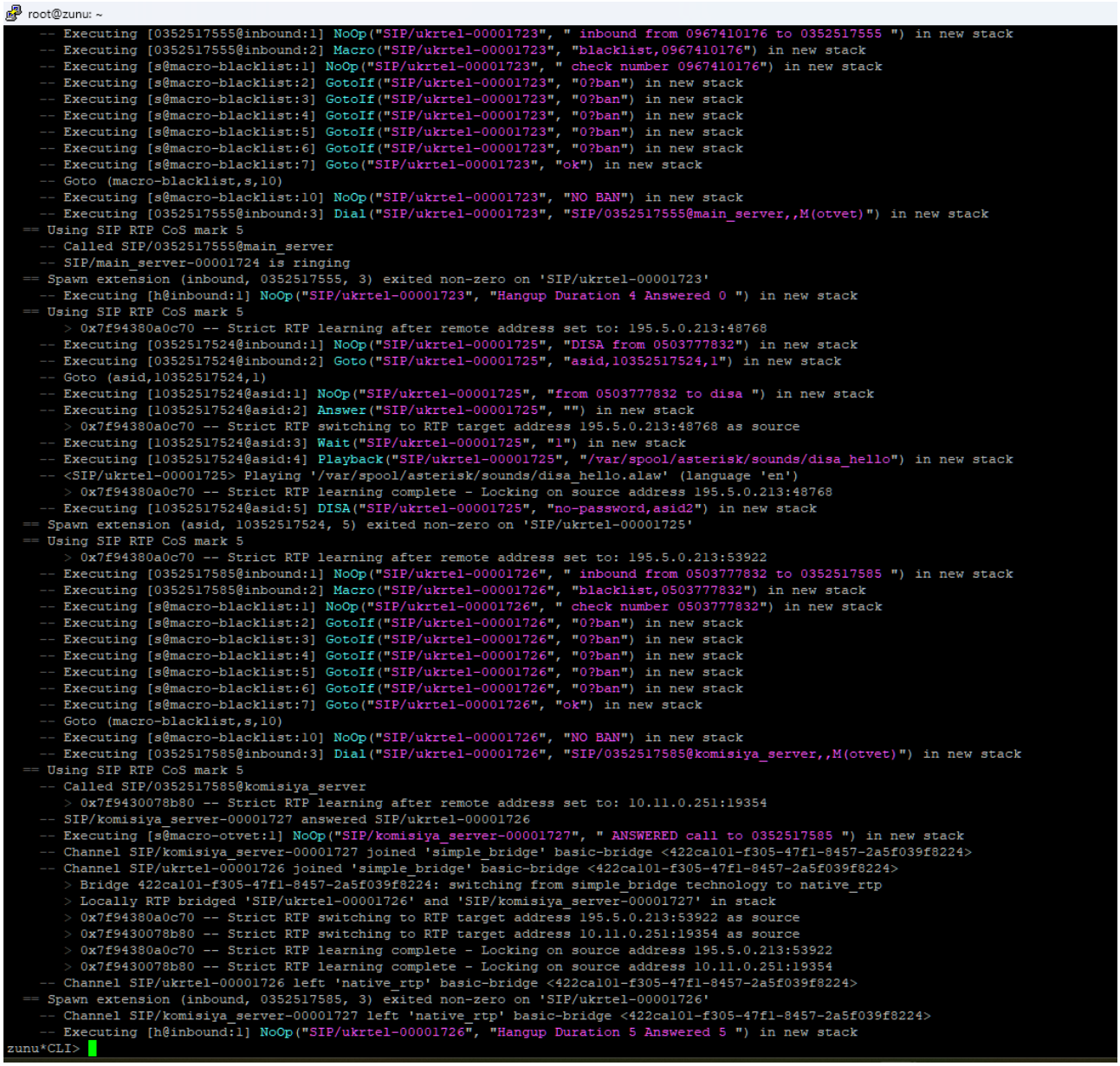


Рис. 4.38. Процес аутентифікації входу IP-адреси

Відмінності між RTP та SRTP полягають у тому, що SRTP пропонує додатковий рівень безпеки для мультимедійних даних. У той час, як RTP забезпечує доставку даних у реальному часі, SRTP захищає ці дані за допомогою шифрування та аутентифікації.

TLS – це криптографічний протокол, який забезпечує наскрізну безпеку даних, що надсилаються між програмами через Інтернет. Слід зазначити, що TLS не захищає дані в кінцевих системах. Він просто забезпечує безпечну доставку даних через Інтернет, уникаючи можливого прослуховування та/або зміни вмісту. TLS використовує комбінацію симетричної та асиметричної

криптографії, оскільки це забезпечує хороший компроміс між продуктивністю та безпекою під час безпечної передачі даних.

Найчастіше зловмисники при спробі проникнення на сервер IP-телефонії використовують стандартні логіни, що прописані у Dialplan, та пробують метод підбору паролів Bruteforce [4]. Для того, щоб виявити зловмисника, необхідно спостерігати за *log.file* на сервері Asterisk [5]. Так як записів у файлі може бути досить багато, то доцільно автоматизувати цей процес за допомогою програми Fail2ban [7].

Запропонований метод можна описати сукупністю наступних кроків:

Встановлюємо Fail2ban на сервер, виконуємо наступні команди:

sudo apt-get update

sudo apt-get install fail2ban

Для того, щоб встановлена програма працювала належним чином необхідно внести деякі правки у файл конфігурації (за замовчуванням це */etc/fail2ban/jail.conf*).

Тепер потрібно виконувати редагування тільки */etc/fail2ban/jail.local*. Він буде підключений системою автоматично та має вищий пріоритет при виконанні.

Відкриваємо файл *jail.local* для редагування:

sudo vi /etc/fail2ban/jail.local

При цьому потрібно звернути увагу на секцію [DEFAULT].

В ній знаходяться основні правила, що задані за замовчуванням для *Fail2ban*.

ignoreip – значення цього параметру вказують, які IP-адреси блокуватися не будуть. Якщо потрібно, щоб *Fail2ban* ігнорував при перевірці декілька IP-адрес, то їх необхідно вказати в параметрі *ignoreip* через пробіл.

bantime – даний параметр означає час в секундах, протягом якого підозріла IP-адреса буде заблокована (за замовчуванням це 10 хв.).

findtime – визначає проміжок часу в секундах, протягом якого програма буде визначати наявність підозрілої активності.

maxretry – допустиме число невдалих спроб отримання доступу до сервера. При перевищенні вказаного значення IP-адреса блокується.

На рисунку 4.39 показано зміни у файлі, а саме змінені параметри *ignoreip=127.0.0.1/8*, що означає дозвіл на пропускання всіх IP-адрес із локальної мережі; *bantime=600*, тобто блокування користувача буде тільки 10 хв.; *findtime=600*, система буде визначати підозрілу активність 10 хв.; *maxretry=5*, кількість невдалих спроб доступу до сервера.

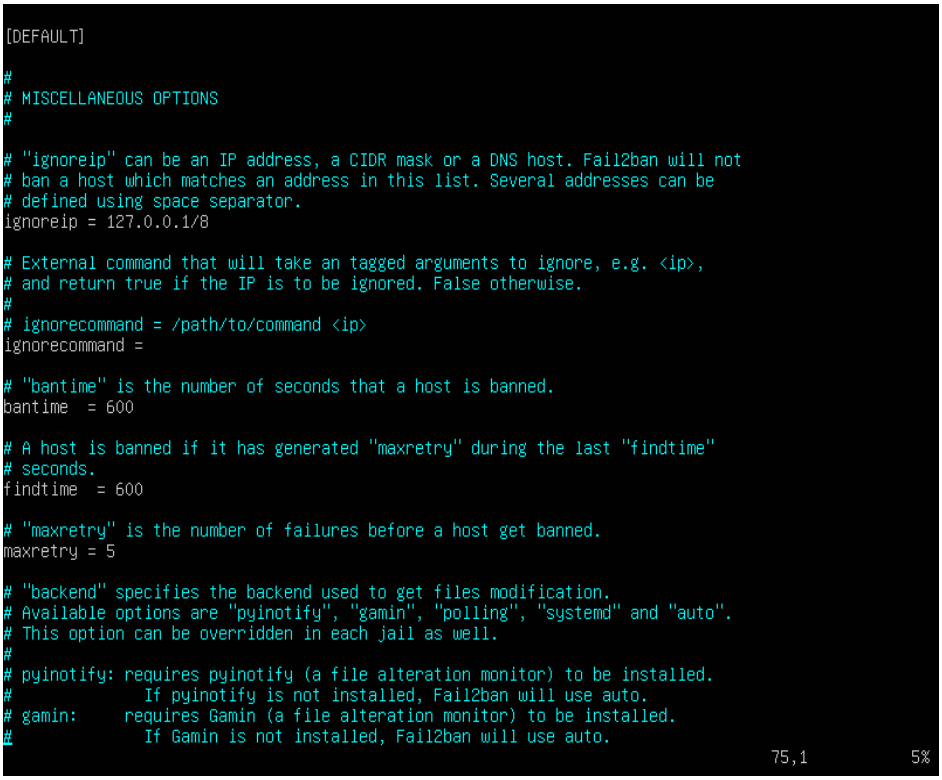


Рис.4.39. Вигляд файлу jail.local після редагування

Після редагування jail.local обов’язково потрібно перезапустити Fail2ban командами

sudo service fail2ban restart

tail /var/log/fail2ban.log

Тепер перейдемо до налаштування Fail2ban в Asterisk.

Відкриваємо конфігураційний файл Asterisk, який відповідає за логування подій в /var/log/asterisk/messages:

sudo vi /etc/asterisk/logger.conf

Додаємо *security* в *messages*:

messages =>notice,warning,error,security

Перезапустимо систему логування asterisk:

sudo asterisk –rvv

logger reload

quit

На рисунку 4.40 показано виконання команд перезапуску Asterisk. Додаємо файл налаштувань Asterisk в директорію с конфігурацією Fail2Ban, тим самим активувавши спостереження його логів:

sudo vi /etc/fail2ban/jail.d/asterisk.conf

Рис. 4.40. Вигляд консолі після перезапуску logger

На рисунку 4.41 показано виконання команди *bantime*, де вона блокує зловмисника на 24 год.

[asterisk]

enabled = true

bantime = 86400,

де 86400 в секундах = 24 години, тобто зловмисник буде заблокований на добу.

Перезапустимо fail2ban для завантаження нового файлу налаштувань:

sudo fail2ban-client reload

Перевіримо:

sudo fail2ban-client status asterisk

```
                                ; background.
;forceblackbackground = yes     ; Force the background of the terminal to be
                                ; black, in order for terminal colors to show
                                ; up properly.
;defaultlanguage = en           ; Default language
documentation_language = en_US  ; Set the language you want documentation
                                ; displayed in. Value is in the same format as
                                ; locale names.
;hideconnect = yes              ; Hide messages displayed when a remote console
                                ; connects and disconnects.
;lockconfdir = no               ; Protect the directory containing the
                                ; configuration files (/etc/asterisk) with a
                                ; lock.
;stdexten = gosub               ; How to invoke the extensions.conf stdexten.
                                ; macro - Invoke the stdexten using a macro as
                                ;         done by legacy Asterisk versions.
                                ; gosub - Invoke the stdexten using a gosub as
                                ;         documented in extensions.conf.sample.
                                ; Default gosub.
;live_dangerously = no          ; Enable the execution of 'dangerous' dialplan
                                ; functions from external sources (AMI,
                                ; etc.) These functions (such as SHELL) are
                                ; considered dangerous because they can allow
                                ; privilege escalation.
                                ; Default no

; Changing the following lines may compromise your security.
;[files]
;astctlpermissions = 0660
;astctlowner = root
;astctlgroup = apache
;astctl = asterisk.ctl

[asterisk]
enabled = true
bantime = 86400
                                                              101,1         Знизу
```

Рис. 4.41. Вигляд зміненого файлу asterisk.conf

```
|  |- Total failed:     0
|  `- File list:        /var/log/asterisk/messages
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
irom@VoIP:~$ sudo fail2ban-client status asterisk
Status for the jail: asterisk
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/asterisk/messages
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
irom@VoIP:~$ sudo fail2ban-client status asterisk
Status for the jail: asterisk
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/asterisk/messages
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
irom@VoIP:~$ sudo fail2ban-client status asterisk
Status for the jail: asterisk
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/asterisk/messages
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
irom@VoIP:~$
```

Рис. 4.42. Вигляд консолі після перевірки статусу

На рисунку. 4.42 показано виконання команди, яка виводить на консоль, де вказано, що *Currently banned=0*, *Total banned=0* та *Banned IP list* – пустий.

В результаті *Fail2Ban* буде блокувати IP-адреси, з яких невірно вводяться паролі до акаунтів Asterisk.

Як описано вище, спостерігаємо автоматизацію по запобіганню проникнення за рахунок відсікання IP-адрес, які ведуть себе підозріло і система блокує їх.

Fail2Ban є ефективним інструментом для захисту IP-телефонії, зокрема для виявлення і блокування аномальних повідомлень та підозрілої активності, яка може свідчити про спроби підбору паролів, фрод або інші атаки на VoIP-системи.

Dialplan є одним з ключових елементів для захисту IP-телефонії. Його належна конфігурація може значно підвищити безпеку VoIP-системи, захищаючи її від зловмисних дій, таких як несанкціоновані виклики, атаки типу DoS тощо.

Розглянемо як Dialplan захищає IP-телефонію.

Встановлюємо правила для викликів, дозволяючи лише певні напрямки. На рисунку 4.43 зображено правило для заборони користувачам дзвонити із внутрішніх телефонів університету на зовнішні телефони університету.

Обмежуємо доступ до особливих типів викликів, наприклад за кордон, як показано на рисунку 4.44.

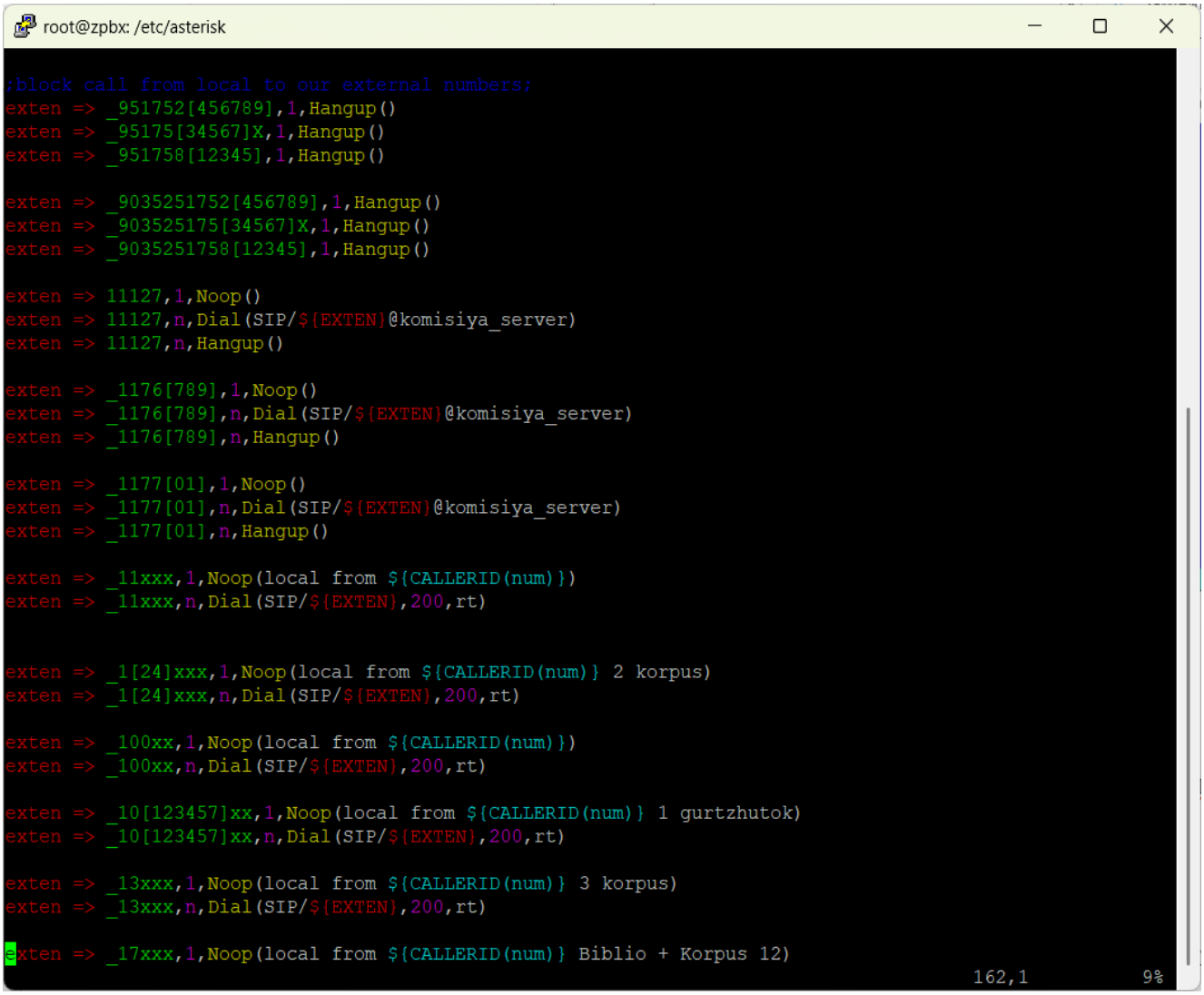


Рис. 4.43. Заборона здійснення дзвінків на міські номери університету

Однією із корисних функцій Dialplan є детекція аномальних дій, якщо необхідно налаштувати моніторинг і правила для виявлення підозрілих дзвінків або спроб несанкціонованого доступу. Наведемо приклад Dialplan в Asterisk для детекції аномальних дій, таких як виявлення підозрілої кількості викликів протягом короткого періоду часу.

Як видно з рисунку 4.45, якщо на один номер буде 10 викликів за часовий інтервал 60 секунд, то система сприймає цей виклик як аномальний, але запустить на перевірку іншу функцію перевірки номера за певний інтервал часу. Якщо виклик не перевищує ліміт, продовжується обробка дзвінка. Якщо виявлено аномальні дії, то номер, з якого телефонували, блокується.

Також існує функція визначення лімітів на кількість викликів за певний проміжок часу, щоб запобігти атакам типу DoS.

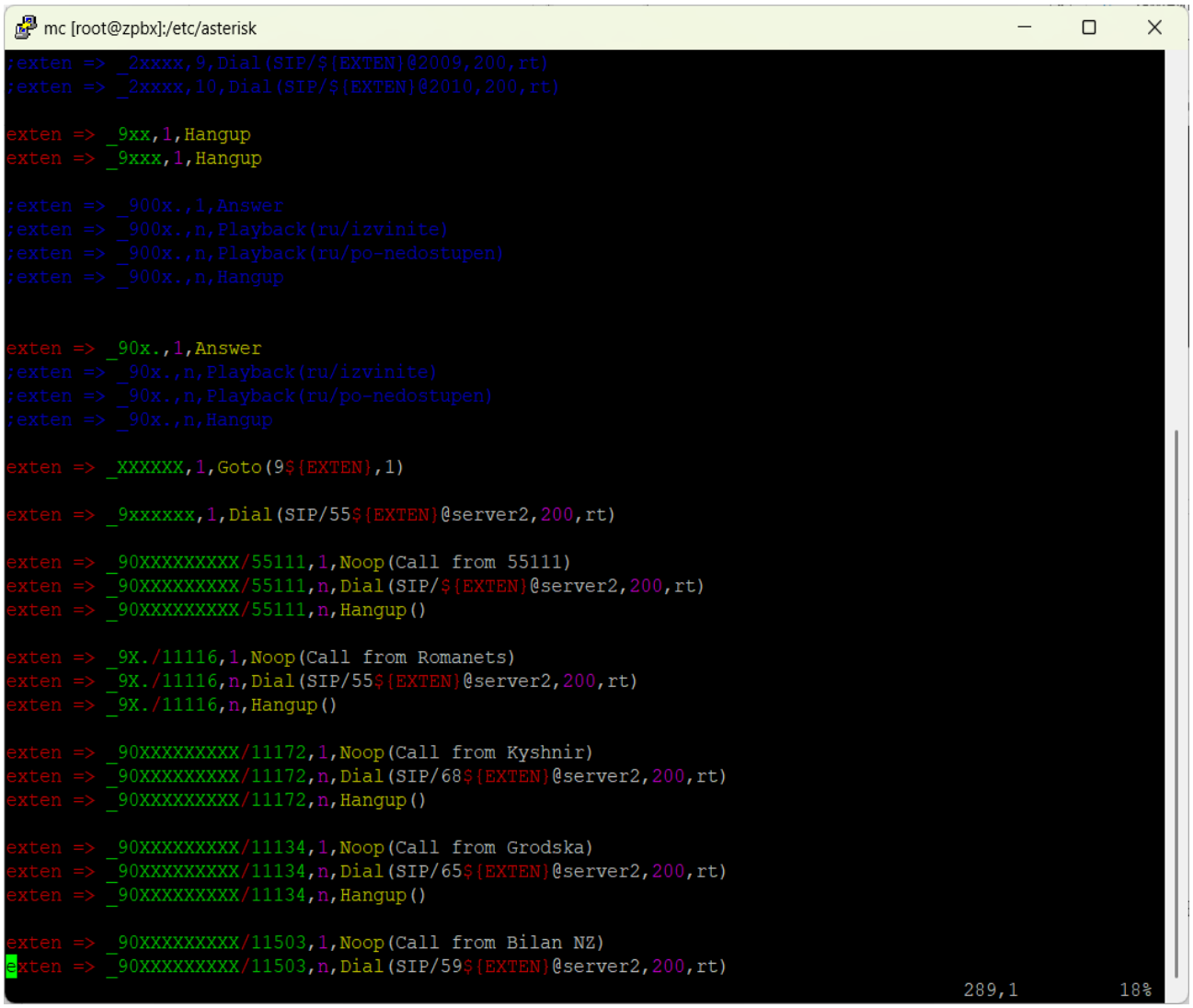


Рис. 4.44. Заборона здійснення дзвінків за кордон

```
[main-context]
; Налаштування обмеження кількості викликів на певний номер
exten => _X.,1,NoOp(Перевірка кількості викликів для аномальної активності)
 same => n,Set(CALL_LIMIT=10) ; Максимальна кількість викликів
 same => n,Set(TIME_PERIOD=60) ; Часовий інтервал в секундах (1 хвилина)

; Використання функції для перевірки кількості викликів на цей номер за останній інтервал
 same => n,Set(CALL_COUNT=${ODBC_CALL_COUNT(${EXTEN},${TIME_PERIOD})})
 same => n,GotoIf($[${CALL_COUNT} >= ${CALL_LIMIT}]?block-call,1)

; Якщо виклики не перевищують ліміт, продовжуємо обробку
 same => n,Dial(SIP/${EXTEN})

; Обробка аномальних викликів
exten => block-call,1,NoOp(Аномальна активність виявлена: Блокування виклику)
 same => n,Playback(sorry-cannot-complete-call) ; Відтворення повідомлення
 same => n,Hangup() ; Завершення виклику
```

Рис. 4.45 Програмний код детекції аномальних дій

У Dialplan є функція обробки невірних викликів, яка визначає обробку для викликів, що не відповідають встановленим правилам. Наприклад, перенаправляє підозрілі виклики на голосову пошту або автоматично відхиляє їх. Також забезпечує маршрутизацію помилок для коректного управління невідомими чи потенційно шкідливими запитами.

Конфігурація Dialplan є важливою частиною комплексного підходу до виявлення аномалій та захисту IP-телефонії, тому варто враховувати її як одну з ключових ланок безпеки.

4.4 Оцінка ефективності інтелектуалізованої системи виявлення аномальних повідомлень

З метою оцінювання ефективності розробленого методу виявлення аномальних повідомлень у трафіку IP-телефонії було проведено серію експериментів, що базуються на аналізі VoIP-повідомлень у режимі реального

часу. Запропонований підхід передбачає групування тематично схожих SIP-повідомлень з використанням структурованої онтології домену IP-телефонії, яка автоматично оновлюється в процесі аналізу трафіку.

Для оцінки продуктивності системи було змодельовано ситуацію, в якій порівнюється швидкість обробки повідомлень оператором вручну та системою автоматичного виявлення. При аналізі вибірки з 10 повідомлень система витратила 539 секунд на їхню обробку та верифікацію, тоді як оператору знадобилося 1560 секунд для виконання аналогічного завдання (рисунок 4.46.). Таким чином, було досягнуто скорочення часу обробки в 2,89 рази.

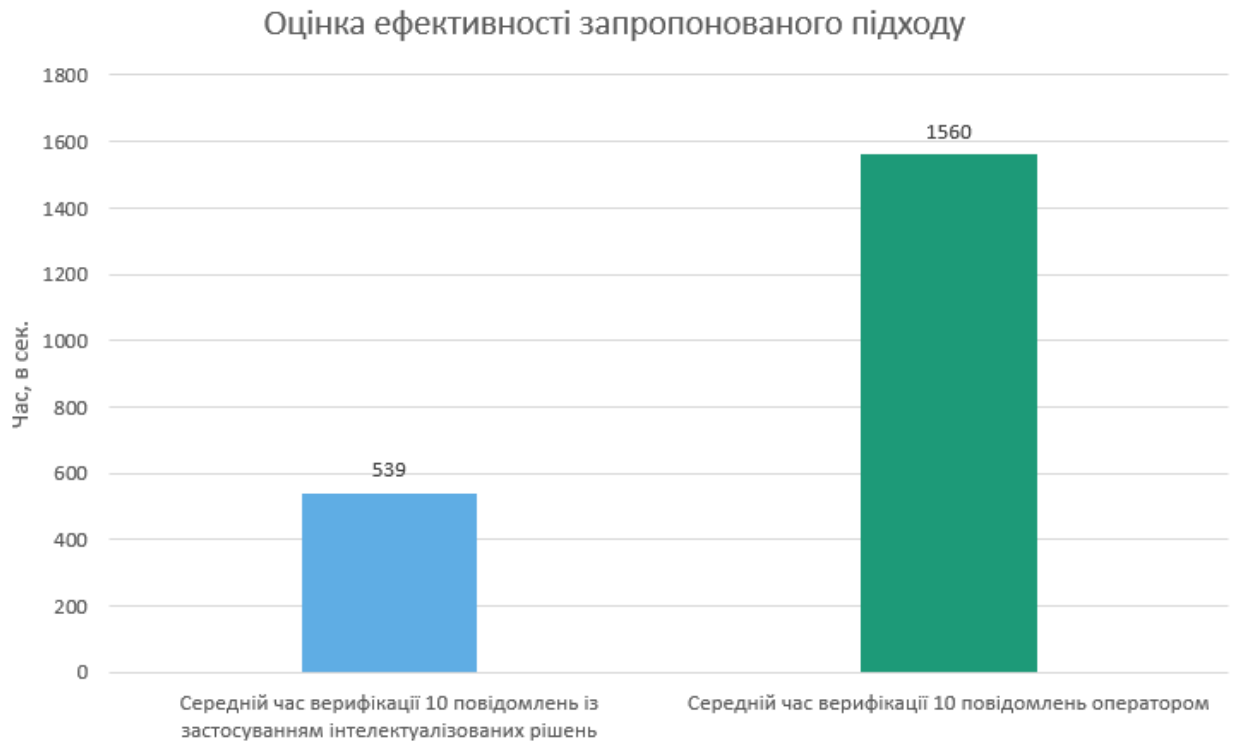


Рис. 4.46. Результат: скорочення часу опрацювання повідомлень в середньому в 2.89 раз

Подальше масштабування експерименту продемонструвало зростання ефективності автоматизованої системи зі збільшенням обсягу даних. Зокрема, при обробці 50 повідомлень система витратила 1185 секунд, у той час як оператор — 6720 секунд. Аналогічна тенденція спостерігалася при обробці 100 повідомлень: автоматизована система завершила процес за 1730 секунд, тоді як

вручну оператору для цього було потрібно 14356 секунд. Отже, із зростанням кількості повідомлень різниця в часі між ручною та автоматизованою обробкою суттєво зростає, що свідчить про хорошу масштабованість запропонованого рішення.

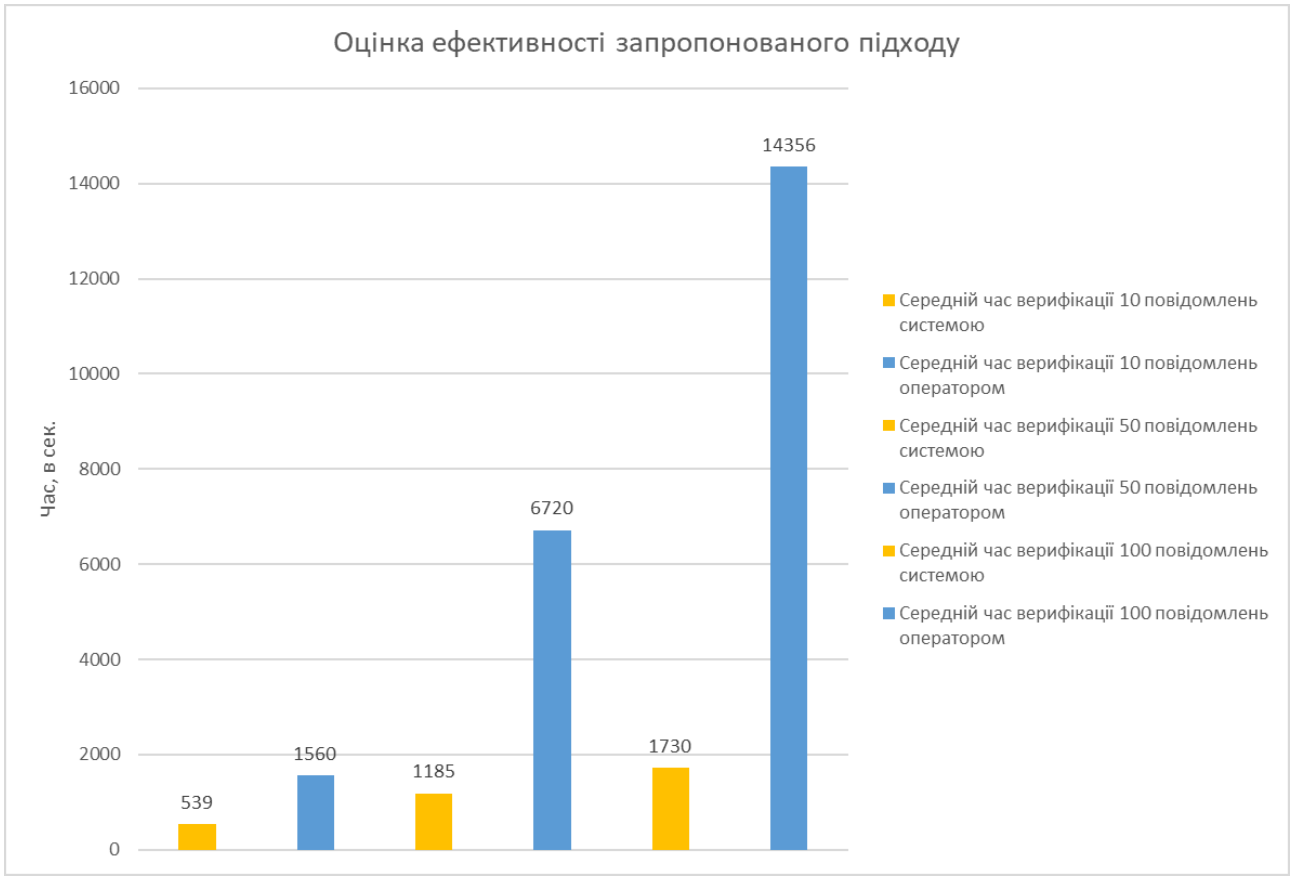


Рис. 4.47. Результат: скорочення часу опрацювання повідомлень в середньому від 2.89 до 8.3 рази

Проведені експериментальні дослідження підтвердили ефективність методу виявлення аномальних VoIP-повідомлень, заснованого на групуванні та онтологічному аналізі трафіку IP-телефонії. Результати показали суттєве зниження часу обробки повідомлень у порівнянні з ручною роботою оператора, при цьому ефективність системи зростає зі збільшенням обсягів даних.

Ключовим чинником, що забезпечує приріст продуктивності, є механізм автоматичного поповнення онтології, який дає змогу враховувати нові шаблони та семантичні характеристики аномальних повідомлень у корпоративній мережі. Таким чином, розроблена система демонструє високий потенціал до

впровадження в інфраструктуру IP-телефонії для забезпечення оперативного виявлення аномалій, підвищення надійності комунікацій та зниження навантаження на персонал.

У подальших дослідженнях передбачається удосконалення методів семантичного аналізу SIP-повідомлень, а також інтеграція з системами реагування на інциденти інформаційної безпеки.

Запропонований метод виявлення аномальних повідомлень у трафіку IP-телефонії був інтегрований до прототипу діючої корпоративної системи з метою оцінки його ефективності в умовах реального використання. Імплементація здійснювалася як додатковий модуль до підсистеми контролю трафіку, що дозволило не лише зберегти існуючу архітектуру мережевої інфраструктури, але й забезпечити її розширення без значних витрат ресурсів або порушення стабільності основних сервісів.

Оцінка ефективності інтеграції базувалася на низці ключових критеріїв: зниження часу обробки повідомлень, рівень точності виявлення аномалій, зменшення навантаження на персонал, а також адаптивність системи до змін у структурі трафіку. Практичні результати продемонстрували, що після впровадження методу в діючу систему середній час реагування на інциденти, пов’язані з аномальними SIP-повідомленнями, скоротився майже втричі. Це зумовлено тим, що основні сценарії виявлення виконуються автоматично, а система самостійно класифікує повідомлення за ступенем потенційної загрози, використовуючи побудовану онтологічну модель знань.

Крім того, система показала високу гнучкість у роботі з нетиповими повідомленнями завдяки механізму автоматичного поповнення бази знань на основі нових шаблонів. Це забезпечує адаптивність до динамічних змін у мережевому середовищі та нових типів атак без необхідності вручну оновлювати правила або конфігурації.

Важливо відзначити, що завдяки модульному характеру розробленого рішення його можливо масштабувати для використання в системах різного рівня, від локальних корпоративних офісів до міжрегіональних вузлів операторів

зв’язку. Таким чином, впровадження методу може здійснюватися поетапно, з мінімальним втручанням у поточні процеси функціонування інфраструктури IP-телефонії.

Загалом результати впровадження підтверджують, що запропонований метод є не лише теоретично обґрунтованим, але й практично застосовним. Його використання дозволяє значно підвищити рівень кібербезпеки в IP-телефонних системах за рахунок своєчасного виявлення аномалій, зменшення кількості хибнопозитивних спрацьовувань та зниження витрат часу на ручний аналіз мережевого трафіку.

На основі аналізу узагальненої структури інтелектуалізованої комп’ютерної системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі ICSDMM-VoIP (Intelligent Computer System for Detection of Malicious Messages), розглянутої в підрозділі 3.1, виконано порівняльну оцінку основних показників, які впливають на ефективність контролю нетипової поведінки користувачів IP-телефонії (таблиця4.1).

Таблиця 4.1

Порівняння систем контролю нетипової поведінки користувачів IP-телефонії

Техніко-економічні характеристики	Системи				
	Wireshark	Suricata	Snort	Asterisk	ICSDMM -VoIP
Аналітика та звітність	+/–	–	+/-	+/-	+
Багатопотокова обробка даних	+/–	+	–	+	+
Адаптивна інтеграція	+/–	–	+	+	+
Масштабованість	–	–	–	+	+
Інтелектуальний аналіз даних	–	–	–	–	+
Вартість	Freeware	Freeware	Shareware	Freeware	Freeware

Висновки до розділу 4

Реалізація запропонованих методів та засобів захисту IP-телефонії дозволяє значно знизити ризики атак, таких як підбір паролів, фрод, DoS/DDoS-атаки, перехоплення даних та інші види загроз. Використання сучасних рішень забезпечує ефективний захист як від зовнішніх, так і внутрішніх загроз.

Впровадження шифрування голосових даних (SRTP) та захисту сигналізації (TLS) забезпечує високий рівень конфіденційності та зменшує ризик перехоплення розмов зловмисниками. Шифрування є обов'язковою складовою сучасних систем захисту IP-телефонії.

Налаштування та використання інструменту Fail2Ban для автоматичного виявлення і блокування підозрілих IP-адрес дозволяє оперативно реагувати на спроби вторгнень та атаки на сервер IP-телефонії. Це рішення забезпечує динамічний захист у реальному часі без потреби в ручному втручанні.

Застосування сучасних систем моніторингу, таких як Wazuh і Grafana, дає змогу аналізувати трафік, контролювати доступ та оперативно виявляти аномалії. Це сприяє кращому управлінню безпекою та швидшому виявленню інцидентів.

Запропоновані засоби виявлення аномальної активності (наприклад, Fail2Ban) і системи захисту від фроду дозволяють мінімізувати ризики фінансових втрат, пов'язаних із несанкціонованими дзвінками та іншими формами шахрайства.

Ефективна реалізація запропонованих методів показує комплексний підхід, а Dialplan можна адаптувати залежно від специфіки системи IP-телефонії та необхідних заходів безпеки.

Проведено експериментальні дослідження запропонованих підходів, імплементовано програмну підсистему виявлення аномальних повідомлень на основі онтологічного підходу в діючу корпоративну IP-телефонію.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну задачу створення інтелектуалізованої комп'ютерної системи своєчасного виявлення зловмисних VoIP-повідомлень в корпоративній мережі з метою підвищення ефективності захисту IP-телефонії, що базується на онтологічній моделі її функціонування та методах інтелектуального аналізу даних.

Основні наукові та практичні результати дослідження дозволяють сформулювати наступні висновки:

1. Проведено аналіз сучасних методів та засобів захисту IP-телефонії у корпоративних мережах. Проведено систематизацію загроз, притаманних IP-телефонії, зокрема атак типу spoofing, sniffing, DoS/DDoS, маніпулювання сигналізаційним трафіком (SIP), термінацію VoIP-трафіку. Встановлено, що традиційні засоби безпеки, такі як брандмауери та VPN, є недостатньо ефективними проти складних, багаторівневих атак у VoIP-середовищі. Доведено доцільність застосування методів інтелектуального аналізу даних для підвищення ефективності захисту VoIP-інфраструктури.

2. Запропоновано онтологію опису VoIP-повідомлень у межах функціонування системи IP-телефонії. В межах онтологічного моделювання здійснено формалізацію ключових понять предметної області, які репрезентовано у вигляді окремих концептів. Кожному концепту присвоєно чітке визначення, атрибутивний склад та типові екземпляри, що забезпечує однозначність інтерпретації інформації як людиною, так і програмними агентами. Розроблена онтологія є гнучкою основою для подальшого розширення та адаптації під конкретні прикладні задачі, зокрема для виявлення аномалій у трафіку, забезпечення семантичного аналізу повідомлень, генерації сигнатур для систем захисту від VoIP-атак, а також інтеграції з інструментами інтелектуального аналізу даних у сфері мережевої безпеки. Її використання дозволяє підвищити рівень інтероперабельності, автоматизації та формалізації у процесах контролю, аудиту та реагування на події в IP-телефонії.

3. Запропоновано метод автоматизованого наповнення онтології тематичних повідомлень у корпоративній системі IP-телефонії, що є суттєвим внеском у підвищення ефективності побудови онтологічних баз знань для аналізу комунікаційного трафіку. Основою методу є формалізоване представлення VoIP-повідомлень у вигляді деревовидних структур, які моделюють логічну та ієрархічну організацію повідомлень із розподілом на рівні заголовків, полів, параметрів і вкладених елементів. Такий підхід дозволяє здійснювати семантичний аналіз та структуризацію повідомлень із врахуванням протоколів SIP, SDP, RTP та інших, що використовуються в IP-телефонії. Додатково, операції аналізу та взаємодії між структурними компонентами повідомлень описано за допомогою алгебри кортежів, яка забезпечує формальну основу для їх порівняння, об'єднання, фільтрації та трансформації у відповідні концепти онтології. Це дозволяє автоматизувати процес ідентифікації нових сутностей і зв'язків, які мають бути внесені до онтологічної моделі, що в свою чергу дає можливість зменшити час наповнення онтологічної бази знань.

4. Розроблено метод виявлення аномалій у трафіку IP-телефонії, заснований на групуванні VoIP-повідомлень з використанням онтологічного підходу та контекстно-частотного аналізу, що дозволяє значно підвищити точність і швидкість виявлення нестандартної або шкідливої активності у корпоративних мережах зв'язку. Метод базується на інтеграції знання-орієнтованої моделі, у якій повідомлення описані за допомогою спеціалізованої онтології, що відображає типи повідомлень, їхні структури, допустимі послідовності взаємодії та семантичні зв'язки між учасниками сесії зв'язку. Така онтологічна база дозволяє порівнювати вхідні повідомлення з відомими шаблонами «нормальної» поведінки. Розроблений метод забезпечив підвищення ефективності виявлення аномальних повідомлень, у середньому 5, 6 разів, порівняно з традиційними підходами. Це досягнуто за рахунок глибшого урахування контексту комунікаційних подій, семантики повідомлень та гнучкого онтологічного представлення знань про мережеві взаємодії.

5. Розроблено підсистему для захисту від термінації трафіку в IP-телефонії на основі використання нечіткої логіки. Підсистема здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних. Це дозволяє враховувати численні критерії, такі як IP-адреса клієнта, час здійснення дзвінка, часовий пояс і якість зв’язку, що сприяє підвищенню рівня безпеки та якості зв'язку.

6. Розроблено архітектуру, структурно-функціональні схеми та узагальнений алгоритм функціонування інтелектуалізованої системи виявлення аномалій у трафіку IP-телефонії, яка об’єднує окремі підсистеми в єдиний цілісний інформаційно-аналітичний контур. Система охоплює всі етапи обробки VoIP-трафіку — від первинного збору даних до прийняття рішень щодо наявності аномальних або потенційно загрозливих повідомлень. Завдяки такій архітектурі забезпечено модульність, гнучкість і масштабованість розробленого рішення, а також можливість інтеграції з зовнішніми системами інформаційної безпеки, SIEM-платформами та системами моніторингу.

Проведено експериментальні дослідження запропонованих методів і засобів для виявлення аномалій у трафіку IP-телефонії, що дозволило кількісно оцінити їх ефективність та практичну придатність. З метою перевірки працездатності розроблених методів імплементовано програмну підсистему виявлення аномальних VoIP-повідомлень, яка інтегрована в університетську корпоративну систему IP-телефонії. Програмна підсистема реалізує компоненти онтологічного аналізу повідомлень, модуль контекстно-частотної обробки, інтерфейси інтеграції з потоковими джерелами SIP/SDP/RTP-трафіку, а також механізми прийняття рішень щодо ідентифікації аномальних подій. Це дозволило здійснювати обробку повідомлень у режимі, наближеному до реального часу, що критично важливо для виявлення атак типу DoS, SIP flooding, spoofing, несанкціонованого доступу та інших загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Voice over IP. [Online]. Available: https://en.wikipedia.org/wiki/ Voice_over_IP
2. OECD (2014), "International Traffic Termination", OECD Digital Economy Papers, No. 238, OECD Publishing. DOI:10.1787/5jz2m5mnlvkc-en
3. “What is a DDoS attack?” https://www.digitalattackmap.com /understanding-ddos/
4. K. Apostol, Brute-force Attack, SaluPress, 2012.
5. Asterisk [Online]. Available: https://uk.wikipedia.org/wiki/Asterisk.
6. “What is a VoIP phone, and how does it work?” Hosted VoIP Services Provider - Start Free Today | On SIP. [Онлайн]. Доступно: https://www.onsip.com/voip-resources/voip-fundamentals/how-do-voip-phones-work
7. J. Van Meggelen, L. Madsen, and J. Smith, Asterisk: The Future of Telephony, Second Edition, O’Reilly Media Inc., 2007.
8. Fail2ban, [Online]. Available: https://www.fail2ban.org
9. Dialplan, [Online]. Available: https://wiki.asterisk.org/wiki/display/ AST/Dialplan
10. D. Sisalem at al., SIP Security, John Wiley & Sons, Ltd., 2009.
11. Installation of Debian, [Online]. Available: http://www.asteriskguru.com /tutorials/asterisk_installation_compilation_debian.html
12. Todd J.B. Blayone, Olena Mykhailenko, Svetlana Usca, Ihor Romanets, Exploring technology attitudes and personal–cultural orientations as student readiness factors for digitalised work. *Higher Education, Skills and Work-based Learning* 17 June 2021; 11 (3): 649–671. DOI:10.1108/HESWBL-03-2020-0041
13. M.S. Abadeh, J. Habibi, C. Lucas, “Intrusion detection using a fuzzy genetics-based learning algorithm,” Journal of Network and Computer Applications, no. 30, pp. 414-428, 2007.
14. T.J. Ross, Fuzzy Logic with Engineering Applications, McGraw-Hill Inc., USA, 1995.

15. L. Dubchak, N. Vasylkiv, V. Kochan, A. Lyapandra, “Fuzzy data processing method,” Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2013), September 12-14, 2013, Berlin, Germany, Vol. 1, pp. 373-375.
16. S. Shtovba, Introduction to the Theory of Fuzzy Sets and Fuzzy Logic, [Online]. Available: http://matlab.exponenta.ru/fuzzylogic/book1/
17. V.S. Mikhaylenko, V.V. Nikolsky, “Use of Fuzzy Adaptive Control System for Computer Monitoring of Boiler Network,” Automation, Electrotechnical Complexes and Systems, [Online]. Available: http://aaecs.org/mihailenko-vs-nikolskii-vv-ispolzovanie-nechetkoi-adaptivnoi-sistemi-upravleniya-dlya-kompyuternogo-monitoringa-setyu-kotelnih-ustanovok.html
18. L.A. Zadeh, “Fuzzy logic – a personal perspective,” Fuzzy Sets and Systems, vol. 281, pp. 4-20, 2015
19. M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, I. Romanets, “High performance adaptive system for cyberattacks detection,” Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2017), September 21-23, 2017, Bucharest, Romania, Vol. 2, pp. 853-858.
20. Balyk, M. Karpinski, A. Naglik, G. Shangytbayeva, and I. Romanets, “Using graphic network simulator 3 for DDoS attacks simulation,” International Journal of Computing, vol. 16, issue 4, pp. 219-225, 2017.
21. M. Komar, V. Golovko, A. Sachenko, and S. Bezobrazov, “Development of neural network immune detectors for computer attacks recognition and classification,” Proceedings of the IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2013), September 12-14, 2013, Berlin, Germany, Vol. 2, pp. 665-668.
22. V. Golovko, M. Komar, & A. Sachenko, “Principles of neural network artificial immune system design to detect attacks on computers,” Proceeding of the 2010 IEEE International Conference on Modern Problems of Radio Engineering,

Telecommunications and Computer Science (TCSET'2010), February 2010, pp. 237-237.

23. Sergii Lysenko, Oleg Savenko, Kira Bobrovnikova, Andrii Kryshchuk. Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks, International Conference on Computer Networks, Springer CN 2018: Computer Networks pp 385-401.
24. Криміналістика і судова експертиза: міжвідом. наук. -метод. зб. / Київський НДІ судових експертиз; Куцо Г. В., Юлов С. О. Дослідження телекомунікаційного обладнання термінації VoIP трафіку (рефайлінгу), побудованого на базі модемів HUAWEI. Київ, 2017- С. 344-352. Вип. 62. – 1072 с
25. I. Romanets, A. Sachenko and L. Dubchak, "Method of Protection Against Traffic Termination in VoIP," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-5, doi: 10.1109/ECAI.2018.8678992.
26. Nazih, Waleed, Khaled Alnowaiser, Esraa Eldesouky, and Osama Youssef Atallah. 2023. "Detecting SPIT Attacks in VoIP Networks Using Convolutional Autoencoders: A Deep Learning Approach" Applied Sciences 13, no. 12: 6974. https://doi.org/10.3390/app13126974 L. Tuanhua, "Interactive Behavior Analysis Based on Social Network," 2021 International Conference of Social Computing and Digital Economy (ICSCDE), 2021, pp. 188-191.
27. Pascual, S.; Bonafonte, A.; Serra, J. SEGAN: Speech Enhancement Generative Adversarial Network. In Proceedings of the 18th Annual Conference of the International Speech Communication Association (INTERSPEECH 2017), Stockholm, Sweden, 20–24 August 2017; pp. 3642–3646.
28. Hernes, M., Nguyen, N.T., Maleszka, M., Bytniewski, A. The automatic summarization of text documents in the cognitive integrated management information system (2015) Proceedings of the 2015 Federated Conference on Computer Science and Information Systems, FedCSIS 2015, art. No 8, pp. 1387-1396.

29. Dyvak, M., Papa, O., Melnyk, A., Pukas, A., Porplytsya, N., Rot, A. Interval model of the efficiency of the functioning of information web resources for services on ecological expertise (2020) Mathematics, 8 (12), art. no. 2116, pp. 1-12.
30. Glorot, X.; Bengio, Y. Understanding the difficulty of training deep feedback on neural networks. In Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics, JMLR Workshop and Conference Proceedings, Sardinia, Italy, 13–15 May 2010; pp. 249–256
31. Alvares, C.; Dinesh, D.; Alvi, S.; Gautam, T.; Hasib, M.; Raza, A. Dataset of attacks on a live enterprise VoIP network for machine learning based intrusion detection and prevention systems. Comput. Netw. 2021, 197, 108283
32. Cauteruccio, D.; Oliveira, R. Detection of Abnormal SIP Signaling Patterns: A Deep Learning Comparison. Computers 2022, 11, 27.
33. Ruff, L.; Kauffmann, J.R.; Vandermeulen, R.A.; Montavon, G.; Samek, W.; Kloft, M.; Dietterich, T.G.; Müller, K.R. A unifying review of deep and shallow anomaly detection. Proc. IEEE 2021, 109, 756–795.
34. Mohamed, Amira A., Amira Eltokhy, and Abdelhalim A. Zekry. 2023. "Enhanced Multiple Speakers' Separation and Identification for VOIP Applications Using Deep Learning" Applied Sciences 13, no. 7: 4261. DOI: 10.3390/app13074261
35. Kafke, John, and Thiago Viana. 2022. "Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems" Network 2, no. 4: 545-567. doi.org/10.3390/network2040032
36. Ormazabal, G.; Sarvesh, N.; Eilon, Y.; Henning, S. Secure sip: A scalable prevention mechanism for dos attacks on sip-based VoIP systems. In Proceedings of the International Conference on Principles, Systems and Applications of IP Telecommunications, Berlin/Heidelberg, Germany, 1–2 July 2008; pp. 107–132.
37. Cauteruccio, F.; Cinelli, L.; Corradini, E.; Terracina, G.; Ursino, D.; Virgili, L.; Savaglio, C.; Liotta, A.; Fortino, G. A framework for anomaly detection and

classification in Multiple IoT scenarios. Future Gener. Comput. Syst. 2021, 114, 322–335.

38. R. Pasichnyk and A. Sachenko, "Semantic WEB-Search Developing by Problem-Oriented Ontology Means," 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, Germany, 2007, pp. 445-448, doi: 10.1109/IDAACS.2007.4488457.
39. Mykola Dyvak, Andriy Melnyk, Artur Rot, Marcin Hernes, Andriy Pukas, "Ontology of mathematical modeling based on interval data," Complexity, vol. 2022, Article ID 8062969, 24 pages, 2022.
40. Tas, I.M.; Unsalver, B.G.; Baktir, S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism. IEEE Access 2020, 8, 112574–112584.
41. A. Kovbasistyi, A. Melnyk, M. Dyvak, V. Brych, and I. Spivak, "Method for detection of non-relevant and wrong information based on content analysis of web resources," 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2017, pp. 154-156.
42. Пасічник Н. Р. Метод формування онтологічного наповнення на основі аналізу зашумленої слабо структурованої інформації спеціалізованих Веб-сайтів / Н. Р. Пасічник, М.П. Дивак // Індуктивне моделювання складних систем. Збірник наукових праць. – Київ : Міжнар.наук.-навч.центр інформ. технологій та систем НАН та МОН України, 2012. – Вип. №4. – С.158-168.
43. Пасічник Н. Р. Метод формування онтологічного контенту на основі аналізу інформації спеціалізованих Веб-сайтів / Н. Р. Пасічник// Вісник Хмельницького національного університету : Технічні науки, 2012. – Вип. №5. – С. 241-244.
44. Korel, Lukáš, Uladzislau Yorsh, Alexander S. Behr, Norbert Kockmann, and Martin Holeňa. 2023. "Text-to-Ontology Mapping via Natural Language Processing with Application to Search for Relevant Ontologies in Catalysis" *Computers* 12, no. 1: 14. doi.org/10.3390/computers12010014

45. Memariani, A.; Glauer, M.; Neuhaus, F.; Mossakowski, T.; Hatings, J. Automated and Explainable Ontology Extension Based on Deep Learning: A Case Study in the Chemical Domain. In Proceedings of the 3rd International Workshop on Data Meets Applied Ontologies, Hersonissos, Greece, 29 May–2 June 2021: pp. 1–16.
46. Thottan, Marina & ji, Chuanyi. (2003). Anomaly Detection in IP Networks. Signal Processing, IEEE Transactions on. 51. 2191 - 2204. https://doi.org/10.1109/TSP.2003.814797
47. Chakraborty, Niloy & Nair, Roshan & Kasula, Chaithanya Pramodh & Vankayala, Sravanthi. (2019). IP Network Anomaly Detection using Machine Learning. https://doi.org/10.1109/I2CT45611.2019.9033545
48. R. -H. Hwang, M. -C. Peng, C. -W. Huang, P. -C. Lin and V. -L. Nguyen, "An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection," in IEEE Access, vol. 8, pp. 30387-30399, 2020. https://doi.org/10.1109/ACCESS.2020.2973023
49. Kamamura, Shohei & Takei, Yuki & Nishiguchi, Masato & Hayashi, Yuhei & Fujiwara, Takayuki. (2023). Network Anomaly Detection Through IP Traffic Analysis with Variable Granularity. IEEE Access. PP. 1-1. doi.org/10.1109/ACCESS.2023.3334212.
50. Романець, І. (2024). Захист від термінації трафіку в IP-мережі на основі нечіткої логіки. Measuring And Computing Devices In Technological Processes, (1), 186–193. doi.org/10.31891/2219-9365-2024-77-23
51. Doan A. (2023). What Is VoIP? The Newbie’s Guide to Voice over IP. URL: https://www.nextiva.com/blog/what-is-voip.html.
52. The Plum Group, Inc. (2023). What is VoIP and How Does it Work? URL: https://www.plumvoice.com/resources/blog/what-is-voip-how-it-works/
53. Manna J. (2024). What Is SIP Trunking? How It Works, Benefits, & How To Get It. URL: https://www.nextiva.com/blog/what-is-sip-trunking.html.
54. Sharpe R., Warnicke E., Lamping U. (2021). Wireshark User’s Guide. URL: https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs.

55. DeVito A. (2024). Suricata vs Snort: A Comprehensive Review. URL: https://www.stationx.net/suricata-vs-snort/.
56. Snort and Suricata. (2023). URL: https://habr.com/companies/selectel /articles/744478/
57. Müller S. (2024). Powering Network Analytics with Machine Learning & A. Rohde & Schwarz, URL: https://www.ipoque.com/blog/powering-network-analytics-with-ml-ai.
58. K. Anand, J. Kumar and K. Anand, "Anomaly detection in online social network: A survey," *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, 2017, pp. 456-459, doi: 10.1109/ICICCT.2017.7975239.
59. Романець, І. (2024). Онтологічний підхід в системі забезпечення безпеки використання IP-телефонії . *Оптико-електронні інформаційно-енергетичні технології*. 47, 1 (Чер 2024), 240–252. doi.org/10.31649/1681-7893-2024-47-1-240-252.
60. Asterisk Documentation. (2020). URL: https://docs.asterisk.org/ Fundamentals/Asterisk-Architecture/.
61. Asterisk Documentation. (2020). URL: https://docs.asterisk.org /Fundamentals /Asterisk-Architecture/Asterisk-Architecture-The-Big-Picture/
62. Meggelen, J. V., Madsen, L., & Smith, J. (n.d.). (2017). Asterisk™: The Future of Telephony. O'Reilly. URL: http://cdn.oreilly.com/ books/9780596510480.pdf
63. What is Apache Kafka? (2022). Kafka. URL: https://kafka.apache.org/intro
64. What is Apache Flink? (2024). Apache Software Foundation. URL: https://flink.apache.org/what-is-flink/flink-architecture/
65. Manage Test Results. (2023). Grafana Labs Documentation. URL: https://grafana.com/docs/grafana-cloud/testing/k6/analyze-results/manage-test-results/
66. Diro, A.; Chilamkurti, N.; Nguyen, V.-D.; Heyne, W. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. *Sensors* 2021, *21*, 8320. doi.org/10.3390/s21248320

67. Aircall. “What is a softphone? Benefits and why to use one”. Aircall. [Онлайн]. Доступно: https://aircall.io/blog/call-center/softphone/
68. Contributors to Wikimedia projects. “Real-time transport protocol - Wikipedia.” Wikipedia, the free encyclopedia. [Онлайн]. Доступно: https://en.wikipedia.org/wiki/Real-time_Transport_Protocol
69. Contributors to Wikimedia projects. “H.323 gatekeeper - Wikipedia”. Wikipedia, the free encyclopedia. [Онлайн]. Доступно: https://en.wikipedia.org/wiki/H.323_Gatekeeper
70. Cisco Small Business Pro SPA2102, SPA3102, SPA8000, PAP2T, WRP400. [Онлайн]. Доступно: https://downloads.linksys.com/downloads /userguide/ATA_AG_v3_200809_AdminGuide.pdf
71. “What is a switch vs a router?” Cisco. [Онлайн]. Доступно: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html
72. Balyk, A., Karpinski, M., Naglik, A., Shangytbayeva, G., & Romanets, I. (2017). Using Graphic Network Simulator 3 For DDoS Attacks Simulation. International Journal of Computing, 16(4), 219-225 DOI: 10.47839/ijc.16.4.910
73. [Онлайн]. Доступно: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/
74. Contributors to Wikimedia projects. “Media gateway control protocol - Wikipedia.” Wikipedia, the free encyclopedia. [Онлайн]. Доступно: https://en.wikipedia.org/wiki/Media_Gateway_Control_Protocol
75. “Conferencing systems overview”. Small business tech tips | Tech Donut. [Онлайн]. Доступно: https://www.techdonut.co.uk/communications/ conferencing-systems/conferencing-systems-overview
76. “Call routing & call forwarding - business phone systems.” PA Communications. [Онлайн]. Доступно: https://pacomms.co.uk/call-routing/
77. “Tutorial: Voice digitization principles.” Telecommunications Tutorials. [Онлайн]. Доступно: https://www.telecommunications-tutorials.com/tutorial-voice-digitization-principles.htm

78. [Онлайн]. Доступно: https://www.quora.com/What-are-data-packets-and-why-is-it-divided
79. “IP transit vs transport - full span solutions.” Full Span Solutions. [Онлайн]. Доступно: https://www.fullspansolutions.com/ip-transit-vs-transport/
80. Поляков М. О. Шифрування трафіку в IP-телефонії. :Наукові праці Четвертої міжнар. наук.-практ. конф.«Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 1–2 лютого 2022 р. (Київ, Україна).–К.: НУХТ, 2022.–222 с. У працях конференції наведено доповіді за напрямами:• світові тенденції в розробленні інформаційних систем і. р. 151.
81. “Encrypted Network Traffic - LiveAction”. LiveAction. [Онлайн]. Доступно: https://www.liveaction.com/glossary/encrypted-network-traffic/
82. С. Устенко та Т. Остапович, “Аналіз та використання технологій VoIP-телефонії в банківських системах”, *Моделювання та інформ. системи в економіці*, т. 95, с. 181–194, 2018.
83. I. V. Kasovs′ka, O. D. Shapovalenko та I. M. Lutsenko, “Network monitoring software for improving the effectiveness of network protection”, *Modern inf. secur.*, т. 45, № 1, 2021. doi.org/10.31673/2409-7292.2021.014757
84. H. Larijani and K. Radhakrishnan, "Voice Quality in VoIP Networks Based on Random Neural Networks," 2010 Ninth International Conference on Networks, Menuires, France, 2010, pp. 89-92, doi: 10.1109/ICN.2010.23
85. D. Pereira, R. Oliveira, and H. S. Kim, "Abnormal Signaling SIP Dialogs Detection based on Deep Learning," *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, Helsinki, Finland, 2021, pp. 1-6, doi: 10.1109/VTC2021-Spring51267.2021.9448664.
86. A. Melnyk, R. Shevchuk, I. Romanets, I. Yakymenko, S. Voznyak and V. Luchyk, "A Method of Detecting Anomalies in IP Phone Traffic based on Ontology of Voip Messages," 2024 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2024, pp. 485-489, doi: 10.1109/ACIT62333.2024.10712505

87. Silva, Rick, MySQL Crash Course: A Hands-on Introduction to Database Development. No Starch Press, 2023
88. І. Романець, “Архітектура інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі”, *Вісник Хмельницького національного університету. Серія: Технічні науки*, vol. 337, no. 3(2), pp. 425–436, May 2024, DOI: 10.31891/2307-5732-2024-337-3-65.
89. Markowsky, G., Sachenko, A., Voznyak, S., Spilchuk, V., Romanyak, R., Turchenko, V. and Romanets, I. 2014. The Ternopil Educational Communication Center: A Nato Project To Integrate Regional Information Technology Resources. *International Journal of Computing*. 7, 1 (Aug. 2014), 185-190. DOI:10.47839/ijc.7.1.503
90. M. Dyvak, A. Pukas, A. Melnyk, I. Voytyuk, S. Valchyshyn, and I. Romanets, "Software Architecture for Modeling the Interval Static and Dynamic Objects," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 2021, pp. 572-575, DOI: 10.1109/ ACIT52158.2021.9548577.
91. M. Dyvak, A. Melnyk, L. Dostalek, V. Ostroverkhov, L. Honchar, and I. Romanets, "Repository of Interval Models of Dynamics of Concentrations of Harmful Emissions of Motor Transport," 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 89-94, DOI: 10.1109/ACIT54803.2022.9913123.
92. O. Kochan, O. Osolinskyi, A. Sachenko, V. Kochan, and I. Romanets, "Simulator of Microcontroller's Power Consumption," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 787-792, DOI: 10.1109/IDAACS58523.2023.10348884.
93. A. Sartiukova, O. Markiv, V. Vysotska, I. Shakleina, N. Sokulska, and I. Romanets, "Remote Voice Control of Computer Based on Convolutional Neural Network," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications

(IDAACS), Dortmund, Germany, 2023, pp. 1058–1064, DOI: 10.1109/IDAACS58523. 2023.10348808.

94. Komar, M., Sachenko, A., Bezobrazov, S., Golovko, V. (2017). Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques. In: Ginige, A., *et al.* Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2016. Communications in Computer and Information Science, vol 783. Springer, Cham. DOI: 10.1007/978-3-319-69965-3_3
95. Golovko, V., Kroshchanka, A., Rubanau, U., Jankowski, S. (2014). A Learning Technique for Deep Belief Neural Networks. In: Golovko, V., Imada, A. (eds) Neural Networks and Artificial Intelligence. ICNNAI 2014. Communications in Computer and Information Science, vol 440. Springer, Cham. DOI:10.1007/978-3-319-08201-1_13
96. Komar, M., Golovko, V., Sachenko, A., Bezobrazov, S.: Development of neural network immune detectors for computer attacks recognition and classification. In: Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2013), Berlin, Germany, vol. 2, pp. 665–668 (2013) DOI: 10.1109/IDAACS.2013.6663008
97. Dyvak, Mykola, Melnyk, Andriy, Rot, Artur, Hernes, Marcin, Pukas, Andriy, Ontology of Mathematical Modeling Based on Interval Data, *Complexity*, 2022, 8062969, 19 pages, 2022. DOI:10.1155/2022/8062969
98. A. Melnyk, I. Shcherbiak, R. Shevchuk, A. Shevchuk, O. Huhul and Y. Franko, "Software Architecture for Mathematical Modelling Based on Interval and Ontology Approach," *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*, Ruzomberok, Slovakia, 2022, pp. 101-105, DOI: 10.1109/ACIT54803.2022.9913108.
99. A. Melnyk, O. Huhul, R. Shevchuk, I. Shcherbiak, Y. Martsenyuk and A. Kovbasistyi, "Intelligent System of Analyzing the Structure of Web-resources," *2021 11th International Conference on Advanced Computer*

Information Technologies (ACIT), Deggendorf, Germany, 2021, pp. 560-563, doi: 10.1109/ACIT52158.2021.9548432.

100. S. Vladov *et al*., "Fuzzy Logic Application in Helicopter Turboshaft Engines Automatic Control Systems," *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv, Ukraine, 2024, pp. 253-256, doi: 10.1109/TCSET64720.2024.10755839.
101. A. Sachenko, O. Osolinskyi, P. Bykovyy, M. Dobrowolski and V. Kochan, "Development of the Flexible Traffic Control System Using the LabView and ThingSpeak," *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2020, pp. 326-330, doi: 10.1109/DESSERT50317.2020.9125036.
102. A. Melnyk, R. Shevchuk, M. Mudrak, O. Huhul, Y. Martsenyuk and I. Shcherbiak, "The Method of Identifying Irrelevant Information in Service-Oriented Corporate Systems," *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, Wrocław, Poland, 2023, pp. 539-542, doi: 10.1109/ACIT58437.2023.10275454.
103. Komar, M., Kochan, V., Dubchak, L., Sachenko, A., Golovko, V., Bezobrazov, S., Romanets, I. “High performance adaptive system for cyber attacks detection”, 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, Bucharest, Romania, 2, art. no. 8095208, pp. 853-858. DOI: 10.1109/IDAACS.2017.8095208.
104. P.C. K. Hung and M. V. Martin, "Security Issues in VOIP Applications," *2006 Canadian Conference on Electrical and Computer Engineering*, Ottawa, ON, Canada, 2006, pp. 2361-2364, doi: 10.1109/CCECE.2006.277789.
105. E. Coulibaly and L. Hao Liu, "Security of Voip networks," *2010 2nd International Conference on Computer Engineering and Technology*, Chengdu, China, 2010, pp. V3-104-V3-108, doi: 10.1109/ICCET.2010.5485790.

106. C. Zhang, Y. Yan, S. Jiang and Z. Chen, "Efficient Detection of QIM-Based VoIP Steganography Using Adjacent Frame Integration and Multi-Codeword Priority Attention," in *IEEE Signal Processing Letters*, vol. 32, pp. 2534-2538, 2025, doi: 10.1109/LSP.2025.3580496.
107. N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," in *IEEE Access*, vol. 10, pp. 36429-36463, 2022, doi: 10.1109/ACCESS.2022.3151903.
108. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A. (2018). Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks. In: Gaj, P., Sawicki, M., Suchacka, G., Kwiecień, A. (eds) Computer Networks. CN 2018. Communications in Computer and Information Science, vol 860. Springer, Cham. DOI: 10.1007/978-3-319-92459-5_31.
109. D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko and A. Kashtalian, "Method for Detecting Steganographic Changes in Images Using Machine Learning," *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2023, pp. 1-6, doi: 10.1109/DESSERT61349.2023.10416453.
110. S. Lysenko, K. Bobrovnikova, R. Shchuka and O. Savenko, "A Cyberattacks Detection Technique Based on Evolutionary Algorithms," *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2020, pp. 127-132, doi: 10.1109/DESSERT50317. 2020.9125016.
111. L. Dubchak, A. Sachenko, C. Wolff, N. Vasylkiv and Z. Bernas, "Classification of Wind Turbine Defects based on the SqueezeNet Neural Network," *2024 IEEE 19th International Conference on Computer Science and Information Technologies (CSIT)*, Lviv, Ukraine, 2024, pp. 1-4, doi: 10.1109/CSIT65290.2024.10982610.
112. B. V. D. Krishna, P. Yogendrasai, S. Rajeev and S. M. Rajagopal, "Voice Over Internet Protocol: Custom SIP Server with QoS Optimization for Real-Time

Communication," *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India, 2025, pp. 566-571, doi: 10.1109/IDCIOT64235.2025.10914779.

.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. A. Melnyk, R. Shevchuk, I. Romanets, I. Yakymenko, S. Voznyak, and V. Luchyk, "A Method of Detecting Anomalies in IP Phone Traffic based on Ontology of Voip Messages," *2024 14th International Conference on Advanced Computer Information Technologies (ACIT)*, Ceske Budejovice, Czech Republic, 2024, pp. 485-489, DOI: 10.1109/ACIT62333.2024.10712505.
2. Balyk, A., Karpinski, M., Naglik, A., Shangytbayeva, G., & Romanets, I. (2017). Using Graphic Network Simulator 3 For DDoS Attacks Simulation. International Journal of Computing, 16(4), 219-225 DOI: 10.47839/ijc.16.4.910
3. Todd J.B. Blayone, Olena Mykhailenko, Svetlana Usca, Anda Abuze, Ihor Romanets, Mykhailo Oleksiiv; Exploring technology attitudes and personal–cultural orientations as student readiness factors for digitalised work. *Higher Education, Skills and Work-based Learning* 17 June 2021; 11 (3): 649–671. DOI:10.1108/HESWBL-03-2020-0041
4. Романець І. Захист від термінації трафіку в IP-мережі на основі нечіткої логіки: Науковий журнал “Вимірювальна та обчислювальна техніка в технологічних процесах”(1), Хмельницький національний університет, Хмельницький, 2024 с. 186-193, DOI: 10.31891/2219-9365-2024-77-23.
5. І. Романець, «Онтологічний підхід в системі забезпечення безпеки використання IP-телефонії», *Опт-ел. інф-енерг. техн.*, вип. 47, вип. 1, с. 240–252, Чер. 2024. DOI: 10.31649/1681-7893-2024-47-1-240-252.
6. І. Романець, “Архітектура інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі”, *Вісник Хмельницького національного університету. Серія: Технічні науки*, vol. 337, no. 3(2), pp. 425–436, May 2024, DOI: 10.31891/2307-5732-2024-337-3-65.
7. Markowsky, G., Sachenko, A., Voznyak, S., Spilchuk, V., Romanyak, R., Turchenko, V. and Romanets, I. 2014. The Ternopil Educational Communication Center: A Nato Project To Integrate Regional Information

Technology Resources. *International Journal of Computing*. 7, 1 (Aug. 2014), 185-190. DOI:10.47839/ijc.7.1.503.

Список наукових праць, які додатково відображають наукові результати та засвідчують апробацію матеріалів дисертації:

8. I. Romanets, A. Sachenko and L. Dubchak, "Method of Protection Against Traffic Termination in VoIP," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-5, DOI: 10.1109/ECAI.2018.8678992.
9. Komar, M., Kochan, V., Dubchak, L., Sachenko, A., Golovko, V., Bezobrazov, S., Romanets, I. “High performance adaptive system for cyber attacks detection”, 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, Bucharest, Romania, 2, art. no. 8095208, pp. 853-858. DOI: 10.1109/IDAACS.2017.8095208.
10. M. Dyvak, A. Pukas, A. Melnyk, I. Voytyuk, S. Valchyshyn, and I. Romanets, "Software Architecture for Modeling the Interval Static and Dynamic Objects," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 2021, pp. 572-575, DOI: 10.1109/ ACIT52158.2021.9548577.
11. M. Dyvak, A. Melnyk, L. Dostalek, V. Ostroverkhov, L. Honchar, and I. Romanets, "Repository of Interval Models of Dynamics of Concentrations of Harmful Emissions of Motor Transport," 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 89-94, DOI: 10.1109/ACIT54803.2022.9913123.
12. O. Kochan, O. Osolinskyi, A. Sachenko, V. Kochan, and I. Romanets, "Simulator of Microcontroller's Power Consumption," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 787-792, DOI: 10.1109/IDAACS58523.2023.10348884.

13. V. Tymchyshyn, B. Tymchyshyn, A. Melnyk, V. Manzhula, V. Faifura, and I. Romanets, "The System Architecture of the Software for Modeling Harmful Emissions in Soil," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 58-62, DOI: 10.1109/ACIT58437.2023.10275416.
14. A. Sartiukova, O. Markiv, V. Vysotska, I. Shakleina, N. Sokulska, and I. Romanets, "Remote Voice Control of Computer Based on Convolutional Neural Network," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1058–1064, DOI: 10.1109/IDAACS58523. 2023.10348808.

Апробація результатів дисертації:

1. IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications – IDAACS (м. Бухарест, Румунія, 2017 р.);
2. 10th International Conference on Electronics, Computers and Artificial Intelligence – ECAI (м. Яси, Румунія, 2018 р.);
3. 11th International Conference on Advanced Computer Information Technologies – ACIT (м. Деггендорф, Німеччина, 2021 р.);
4. 12th International Conference on Advanced Computer Information Technologies – ACIT (м. Руженберок, Словаччина, 2022 р.);
5. IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications – IDAACS (м. Дортмунд, Німеччина, 2023 р.);
6. 13th International Conference on Advanced Computer Information Technologies – ACIT (м. Вроцлав, Польща, 2023 р.);
7. 14th International Conference on Advanced Computer Information Technologies – ACIT (м. Чеське Будейовіце, Чехія, 2024 р.).

Додаток Б

SQL код створеня бази даних

```
CREATE DATABASE VOIP ;
CREATE TABLE Users (
ID      int(10) NOT NULL AUTO_INCREMENT,
username varchar(255),
password int(255),
role    varchar(100),
PRIMARY KEY (ID));

CREATE TABLE Sessions (
Code      int(10) NOT NULL AUTO_INCREMENT,
user_id   int(10) NOT NULL,
token     varchar(255),
ip_address varchar(255),
created_at date,
expires_at int(10),
PRIMARY KEY (Code));

CREATE TABLE Calls (
 ID                  int(10) NOT NULL,
 user_id             int(10) NOT NULL,
 ProductCode         int(10) NOT NULL,
 `source_number integer` int(10),
 status              int(10),
 PRIMARY KEY (ID,
 ProductCode));

CREATE TABLE Ontology (
ID       int(10) NOT NULL AUTO_INCREMENT,
Id_cont  int(10) NOT NULL,
reportsTo int(10) NOT NULL,
Describe  varchar(255),
Main     varchar(255),
Resource  varchar(255),
Vlalidate varchar(100),
PRIMARY KEY (ID));
```

```
ALTER TABLE Ontology ADD CONSTRAINT FKOntology804552 FOREIGN
  KEY (reportsTo) REFERENCES Ontology (ID);

CREATE TABLE Message (
  ID           int(10) NOT NULL AUTO_INCREMENT,
  user_id      int(10) NOT NULL,
  Context      varchar(255),
  Theme        varchar(255),
  Kaywords     varchar(255),
  Phone        varchar(255),
  Address1     varchar(255),
  OntologyId   varchar(255),
  Status       varchar(255),
  Code         int(10),
  `Count words` varchar(255),
  Limit        numeric(19, 0),
  PRIMARY KEY (ID));

CREATE TABLE Logs (
  ID          int(10) NOT NULL AUTO_INCREMENT,
  user_id     int(10) NOT NULL,
  event_type  int(10),
  description varchar(255),
  created_at  int(10),
  Status      int(10),
  Comments    varchar(255),
  PRIMARY KEY (ID));

CREATE TABLE Conennt (
  Code        int(10) NOT NULL AUTO_INCREMENT,
  Id_ontology int(10),
  user_id     int(10),
  Concept1    varchar(255),
  Concept2    varchar(255),
  State       varchar(255),
  Describe    varchar(255),
  Parent      int(10),
  Theme       varchar(200),
  PRIMARY KEY (Code));
```

```
CREATE TABLE Configurations (
  ID         int(10) NOT NULL AUTO_INCREMENT,
  message_id int(10) NOT NULL,
  `key`      varchar(255),
  value      numeric(19, 2),
PRIMARY KEY (ID));
```

Додаток В

Лістинг модуля автоматичної обробки записів у режимі реального часу та перетворення голосу в текст в системі IP телефонії

```
import os
import datetime
import json
import speech_recognition as sr
from pydub import AudioSegment

# === Налаштування ===
AUDIO_DIR = "sip_audio"              # Каталог з аудіо файлами
LOG_FILE = "voip_transcripts.jsonl"  # Файл логів результатів розпізнавання
LANGUAGE = 'uk-UA'                   # Мова розпізнавання

# === Функція: Конвертація MP3 в WAV (якщо потрібно) ===
def convert_mp3_to_wav(mp3_path):
    wav_path = mp3_path.replace('.mp3', '.wav')
    if not os.path.exists(wav_path):
        audio = AudioSegment.from_mp3(mp3_path)
        audio.export(wav_path, format="wav")
    return wav_path

# === Функція: Розпізнавання мовлення з аудіофайлу ===
def recognize_speech(audio_path):
    recognizer = sr.Recognizer()
    with sr.AudioFile(audio_path) as source:
        audio = recognizer.record(source)
    try:
        text = recognizer.recognize_google(audio, language=LANGUAGE)
        return text
    except sr.UnknownValueError:
        return "[UNRECOGNIZED]"
    except sr.RequestError as e:
        return f"[ERROR: {e}]"

# === Функція: Обробка одного файлу SIP аудіо ===
def process_voip_audio_file(file_path):
    filename = os.path.basename(file_path)
    call_id = os.path.splitext(filename)[0]
    timestamp = datetime.datetime.now().isoformat()

    if file_path.endswith('.mp3'):
        file_path = convert_mp3_to_wav(file_path)

    print(f"[INFO] Обробка файлу: {file_path}")
    recognized_text = recognize_speech(file_path)

    log_entry = {
        "call_id": call_id,
        "timestamp": timestamp,
```

```
        "file": filename,
        "recognized_text": recognized_text
    }

    # Запис у лог-файл
    with open(LOG_FILE, 'a', encoding='utf-8') as f:
        f.write(json.dumps(log_entry, ensure_ascii=False) + "\n")

    print(f"[LOGGED] {call_id} → {recognized_text[:50]}...")
    return log_entry

# === Основна функція ===
def main():
    print("[START] Запуск VoIP Speech-to-Text системи...")
    files = [f for f in os.listdir(AUDIO_DIR) if f.endswith(('.wav', '.mp3'))]

    for file in files:
        full_path = os.path.join(AUDIO_DIR, file)
        process_voip_audio_file(full_path)

    print("[DONE] Усі файли оброблено.")

# === Точка входу ===
if __name__ == "__main__":
    main()

    # Після обробки всіх аудіофайлів — статистика і пошук
    generate_word_frequency_statistics()
    search_transcripts_by_keywords(["аварія", "терміново", "скарга"])
from collections import Counter
import re

def generate_word_frequency_statistics(log_file=LOG_FILE, top_n=20):
    word_counter = Counter()

    with open(log_file, 'r', encoding='utf-8') as f:
        for line in f:
            entry = json.loads(line)
            text = entry.get("recognized_text", "").lower()
            words = re.findall(r'\b\w+\b', text)
            word_counter.update(words)

    print(f"\n Найчастіші слова (топ-{top_n}):\n")
    for word, freq in word_counter.most_common(top_n):
        print(f"{word:>15} → {freq}")

    return word_counter
def search_transcripts_by_keywords(keywords, log_file=LOG_FILE):
    matches = []

    with open(log_file, 'r', encoding='utf-8') as f:
        for line in f:
            entry = json.loads(line)
```

```
            text = entry.get("recognized_text", "").lower()

            if any(kw.lower() in text for kw in keywords):
                matches.append(entry)

    print(f"\n🔍 Знайдено {len(matches)} збігів за ключовими словами: {keywords}\n")
    for entry in matches:
        print(f"[{entry['timestamp']}] {entry['call_id']}: {entry['recognized_text'][:100]}")

    return matches
import json
import random
from datetime import datetime, timedelta

# Шлях до файлу для запису
LOG_FILE = "voip_transcripts.jsonl"

# Базові шаблони фраз, які часто зустрічаються в IP-телефонії
base_phrases = [
    "Доброго дня, ви телефонуєте до служби підтримки.",
    "Це термінове повідомлення про аварію в мережі.",
    "Будь ласка, залишайтеся на лінії.",
    "Ваша заявка прийнята і обробляється.",
    "Ми передамо ваш запит до технічного відділу.",
    "На жаль, ми не змогли вас з'єднати з оператором.",
    "Цей дзвінок може бути записаний для покращення якості обслуговування.",
    "Дзвінок стосується скарги на якість зв'язку.",
    "Ваш баланс наближається до нуля.",
    "Вітаємо в системі корпоративного обслуговування.",
    "Зараз всі оператори зайняті.",
    "Повідомлення отримано, обробка триває.",
    "Повідомлення: спроба несанкціонованого доступу.",
    "Спробуйте перезапустити обладнання.",
    "Ми оновлюємо систему, дякуємо за розуміння."
]

def generate_fake_logs(file_path, num_entries=300):
    with open(file_path, 'w', encoding='utf-8') as f:
        base_time = datetime.now() - timedelta(days=5)

        for i in range(num_entries):
            timestamp = (base_time + timedelta(minutes=i * 5)).isoformat()
            call_id = f"call_{i+1:04d}"
            file_name = f"{call_id}.wav"
            recognized_text = random.choice(base_phrases)
            # Додати варіативність: іноді об'єднуються 2-3 фрази
            if random.random() > 0.7:
                recognized_text += " " + random.choice(base_phrases)
            if random.random() > 0.9:
                recognized_text += " " + random.choice(base_phrases)

            log_entry = {
                "call_id": call_id,
```

```
                "timestamp": timestamp,
                "file": file_name,
                "recognized_text": recognized_text
            }

            f.write(json.dumps(log_entry, ensure_ascii=False) + "\n")

    print(f"[DONE] Згенеровано {num_entries} логів у {file_path}")

# Запуск генерації
generate_fake_logs(LOG_FILE)


import pyshark

# Вказуємо інтерфейс мережі (наприклад, 'eth0' або 'Wi-Fi')
INTERFACE = 'eth0'

# Фільтр лише для RTP або SIP
CAPTURE_FILTER = 'udp port 5060 or udp portrange 10000-20000'

def capture_voip_packets():
    print("[INFO] Запуск перехоплення VoIP...")
    capture = pyshark.LiveCapture(interface=INTERFACE, bpf_filter=CAPTURE_FILTER)

    for packet in capture.sniff_continuously():
        try:
            if 'sip' in packet:
                print(f"[SIP] {packet.sip.Request_Line}")
            elif 'rtp' in packet:
                print(f"[RTP] From {packet.ip.src} to {packet.ip.dst} - Payload Length: {packet.length}")
        except AttributeError:
            continue

# Запуск
if __name__ == "__main__":
    capture_voip_packets()
import os
import time
import json
import speech_recognition as sr
from datetime import datetime

# === Налаштування ===
MONITOR_DIR = "/var/spool/asterisk/monitor"       # Asterisk записує сюди
PROCESSED_DIR = "/var/spool/asterisk/processed"   # Оброблені сюди
LOG_FILE = "/var/log/voip_transcripts.jsonl"      # Логи результатів

# Створити каталог для оброблених файлів, якщо не існує
os.makedirs(PROCESSED_DIR, exist_ok=True)

def recognize_wav_file(file_path):
```

```
    recognizer = sr.Recognizer()
    with sr.AudioFile(file_path) as source:
        audio = recognizer.record(source)
    try:
        return recognizer.recognize_google(audio, language='uk-UA')
    except sr.UnknownValueError:
        return "[UNRECOGNIZED]"
    except sr.RequestError as e:
        return f"[ERROR] {e}"

def process_new_files():
    processed = set()

    print("[MONITORING] Починаємо моніторинг SIP-записів...")

    while True:
        for filename in os.listdir(MONITOR_DIR):
            if filename.endswith(".wav") and filename not in processed:
                full_path = os.path.join(MONITOR_DIR, filename)
                print(f"[PROCESSING] {filename}")

                transcript = recognize_wav_file(full_path)
                timestamp = datetime.now().isoformat()

                entry = {
                    "filename": filename,
                    "timestamp": timestamp,
                    "transcript": transcript
                }

                with open(LOG_FILE, 'a', encoding='utf-8') as log_file:
                    log_file.write(json.dumps(entry, ensure_ascii=False) + '\n')

                # Перемістити файл до архіву
                os.rename(full_path, os.path.join(PROCESSED_DIR, filename))
                processed.add(filename)

                print(f"[SAVED] {filename} → Лог оновлено")

        time.sleep(5)  # Перевірка кожні 5 секунд

if __name__ == "__main__":
    process_new_files()
```

Додаток Г

Текст програмного коду нечіткого висновку системи

```
[System]
Name='VoIP'
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=1
NumRules=255
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='IP-identification'
Range=[0 1]
NumMFs=3
MF1='low':'gbellmf',[0.2083 3.125 0]
MF2='middle':'gbellmf',[0.162952380952381 2.5 0.468]
MF3='high':'gbellmf',[0.2083 2.5 1]

[Input2]
Name='client-call-time'
Range=[0 24]
NumMFs=3
MF1='morning':'gbellmf',[5.61904761904762 2.5 -1.11e-16]
MF2='work-time':'gbellmf',[4.15873015873016 2.5 12]
MF3='night':'gbellmf',[4.41269841269841 2.5 24]

[Input3]
Name='addr-call-time'
Range=[-12 12]
NumMFs=3
MF1='I-timezone':'gbellmf',[5.93650793650794 5.25 -12]
MF2='II-timezone':'gbellmf',[4.61 3.13 0.258730158730162]
MF3='III-timezone':'gbellmf',[5 4.16717299520821 12]

[Input4]
Name='connection-quality'
Range=[0 1]
NumMFs=3
MF1='low':'gbellmf',[0.2083 2.5 -1.388e-17]
MF2='middle':'gbellmf',[0.2083 2.5 0.5]
MF3='high':'gbellmf',[0.2083 2.5 1]

[Output1]
Name='access'
Range=[0 1]
NumMFs=2
MF1='deny':'trapmf',[-0.359 -0.0258 0.329365079365079 0.647]
MF2='allow':'trapmf',[0.398148148148148 0.708 1.04 1.38]

[Rules]
1 1 1 1, 1 (1) : 1
1 1 1 2, 1 (1) : 1
1 1 1 3, 1 (1) : 1
```

```
1 1 1 0, 1 (1) : 1
1 1 2 2, 1 (1) : 1
1 1 2 3, 1 (1) : 1
1 1 2 0, 1 (1) : 1
1 1 3 1, 1 (1) : 1
1 1 3 2, 1 (1) : 1
1 1 3 3, 1 (1) : 1
1 1 3 0, 1 (1) : 1
1 1 0 1, 1 (1) : 1
1 1 0 2, 1 (1) : 1
1 1 0 3, 1 (1) : 1
1 1 0 0, 1 (1) : 1
1 2 1 1, 1 (1) : 1
1 2 1 2, 1 (1) : 1
1 2 1 3, 1 (1) : 1
1 2 1 0, 1 (1) : 1
1 2 2 1, 2 (1) : 1
1 2 2 2, 2 (1) : 1
1 2 2 3, 2 (1) : 1
1 2 2 0, 2 (1) : 1
1 2 3 1, 2 (1) : 1
1 2 3 2, 2 (1) : 1
1 2 3 3, 2 (1) : 1
1 2 3 0, 2 (1) : 1
1 2 0 1, 1 (1) : 1
1 2 0 2, 2 (1) : 1
1 2 0 3, 2 (1) : 1
1 2 0 0, 1 (1) : 1
1 3 1 1, 1 (1) : 1
1 3 1 2, 1 (1) : 1
1 3 1 3, 1 (1) : 1
1 3 1 0, 1 (1) : 1
1 3 2 1, 1 (1) : 1
1 3 2 2, 2 (1) : 1
1 3 2 3, 2 (1) : 1
1 3 2 0, 1 (1) : 1
1 3 3 1, 1 (1) : 1
1 3 3 2, 1 (1) : 1
1 3 3 3, 1 (1) : 1
1 3 3 0, 1 (1) : 1
1 3 0 1, 1 (1) : 1
1 3 0 2, 1 (1) : 1
1 3 0 3, 1 (1) : 1
1 3 0 0, 1 (1) : 1
1 0 1 1, 1 (1) : 1
1 0 1 2, 1 (1) : 1
1 0 1 3, 1 (1) : 1
1 0 1 0, 1 (1) : 1
1 0 2 1, 1 (1) : 1
1 0 2 2, 2 (1) : 1
1 0 2 3, 2 (1) : 1
1 0 2 0, 1 (1) : 1
1 0 3 1, 1 (1) : 1
1 0 3 2, 1 (1) : 1
1 0 3 3, 1 (1) : 1
1 0 3 0, 1 (1) : 1
1 0 0 1, 1 (1) : 1
1 0 0 2, 1 (1) : 1
1 0 0 3, 1 (1) : 1
1 0 0 0, 1 (1) : 1
2 1 1 1, 1 (1) : 1
2 1 1 2, 1 (1) : 1
2 1 1 3, 1 (1) : 1
```

```
2 1 1 0, 1 (1) : 1
2 1 2 1, 1 (1) : 1
2 1 2 2, 2 (1) : 1
2 1 2 3, 2 (1) : 1
2 1 2 0, 1 (1) : 1
2 1 3 1, 2 (1) : 1
2 1 3 2, 2 (1) : 1
2 1 3 3, 2 (1) : 1
2 1 3 0, 2 (1) : 1
2 1 0 1, 1 (1) : 1
2 1 0 2, 1 (1) : 1
2 1 0 3, 1 (1) : 1
2 1 0 0, 1 (1) : 1
2 2 1 1, 2 (1) : 1
2 2 1 2, 2 (1) : 1
2 2 1 3, 2 (1) : 1
2 2 1 0, 2 (1) : 1
2 2 2 1, 2 (1) : 1
2 2 2 2, 2 (1) : 1
2 2 2 3, 2 (1) : 1
2 2 2 0, 2 (1) : 1
2 2 3 1, 2 (1) : 1
2 2 3 2, 2 (1) : 1
2 2 3 3, 2 (1) : 1
2 2 3 0, 2 (1) : 1
2 2 0 1, 1 (1) : 1
2 2 0 2, 1 (1) : 1
2 2 0 3, 2 (1) : 1
2 2 0 0, 1 (1) : 1
2 3 1 1, 1 (1) : 1
2 3 1 2, 1 (1) : 1
2 3 1 3, 1 (1) : 1
2 3 1 0, 1 (1) : 1
2 3 2 1, 1 (1) : 1
2 3 2 2, 1 (1) : 1
2 3 2 3, 1 (1) : 1
2 3 2 0, 1 (1) : 1
2 3 3 1, 1 (1) : 1
2 3 3 2, 1 (1) : 1
2 3 3 3, 1 (1) : 1
2 3 3 0, 1 (1) : 1
2 3 0 1, 1 (1) : 1
2 3 0 2, 1 (1) : 1
2 3 0 3, 1 (1) : 1
2 3 0 0, 1 (1) : 1
2 0 1 1, 1 (1) : 1
2 0 1 2, 1 (1) : 1
2 0 1 3, 1 (1) : 1
2 0 1 0, 1 (1) : 1
2 0 2 1, 1 (1) : 1
2 0 2 2, 2 (1) : 1
2 0 2 3, 2 (1) : 1
2 0 2 0, 1 (1) : 1
2 0 3 1, 1 (1) : 1
2 0 3 2, 1 (1) : 1
2 0 3 3, 1 (1) : 1
2 0 3 0, 1 (1) : 1
2 0 0 1, 1 (1) : 1
2 0 0 2, 1 (1) : 1
2 0 0 3, 1 (1) : 1
2 0 0 0, 1 (1) : 1
3 1 1 1, 1 (1) : 1
3 1 1 2, 1 (1) : 1
```

```
3 1 1 3, 1 (1) : 1
3 1 2 1, 1 (1) : 1
3 1 2 2, 1 (1) : 1
3 1 2 3, 2 (1) : 1
3 1 2 0, 1 (1) : 1
3 1 3 1, 1 (1) : 1
3 1 3 2, 2 (1) : 1
3 1 3 3, 2 (1) : 1
3 1 3 0, 1 (1) : 1
3 1 0 1, 1 (1) : 1
3 1 0 2, 1 (1) : 1
3 1 0 3, 1 (1) : 1
3 1 0 0, 1 (1) : 1
3 2 1 1, 2 (1) : 1
3 2 1 2, 2 (1) : 1
3 2 1 3, 2 (1) : 1
3 2 1 0, 1 (1) : 1
3 2 2 1, 2 (1) : 1
3 2 2 2, 2 (1) : 1
3 2 2 3, 2 (1) : 1
3 2 2 0, 2 (1) : 1
3 2 3 1, 1 (1) : 1
3 2 3 2, 2 (1) : 1
3 2 3 3, 2 (1) : 1
3 2 0 1, 1 (1) : 1
3 2 0 2, 2 (1) : 1
3 2 0 3, 2 (1) : 1
3 2 0 0, 2 (1) : 1
3 3 1 1, 2 (1) : 1
3 3 1 2, 2 (1) : 1
3 3 1 3, 2 (1) : 1
3 3 1 0, 1 (1) : 1
3 3 2 1, 1 (1) : 1
3 3 2 2, 2 (1) : 1
3 3 2 3, 2 (1) : 1
3 3 2 0, 1 (1) : 1
3 3 3 1, 1 (1) : 1
3 3 3 2, 1 (1) : 1
3 3 3 3, 1 (1) : 1
3 3 3 0, 1 (1) : 1
3 3 0 1, 1 (1) : 1
3 3 0 2, 1 (1) : 1
3 3 0 3, 1 (1) : 1
3 3 0 0, 1 (1) : 1
3 0 1 1, 1 (1) : 1
3 0 1 2, 1 (1) : 1
3 0 1 3, 1 (1) : 1
3 0 1 0, 1 (1) : 1
3 0 2 1, 2 (1) : 1
3 0 2 2, 2 (1) : 1
3 0 2 3, 2 (1) : 1
3 0 2 3, 2 (1) : 1
3 0 2 0, 1 (1) : 1
3 0 3 1, 1 (1) : 1
3 0 3 2, 2 (1) : 1
3 0 3 3, 2 (1) : 1
3 0 3 0, 1 (1) : 1
3 0 0 1, 1 (1) : 1
3 0 0 2, 2 (1) : 1
3 0 0 3, 2 (1) : 1
3 0 0 0, 1 (1) : 1
0 1 1 1, 1 (1) : 1
0 1 1 2, 1 (1) : 1
```

```
0 1 1 3, 1 (1) : 1
0 1 1 0, 1 (1) : 1
0 1 2 1, 1 (1) : 1
0 1 2 2, 2 (1) : 1
0 1 2 3, 2 (1) : 1
0 1 2 0, 1 (1) : 1
0 1 3 1, 1 (1) : 1
0 1 3 2, 1 (1) : 1
0 1 3 3, 1 (1) : 1
0 1 3 0, 1 (1) : 1
0 1 0 1, 1 (1) : 1
0 1 0 2, 1 (1) : 1
0 1 0 3, 1 (1) : 1
0 1 0 0, 1 (1) : 1
0 2 1 1, 2 (1) : 1
0 2 1 2, 2 (1) : 1
0 2 1 3, 2 (1) : 1
0 2 1 0, 2 (1) : 1
0 2 2 1, 2 (1) : 1
0 2 2 2, 2 (1) : 1
0 2 2 3, 2 (1) : 1
0 2 2 0, 2 (1) : 1
0 2 3 1, 1 (1) : 1
0 2 3 2, 1 (1) : 1
0 2 3 3, 2 (1) : 1
0 2 3 0, 1 (1) : 1
0 2 0 1, 1 (1) : 1
0 2 0 2, 2 (1) : 1
0 2 0 3, 2 (1) : 1
0 2 0 0, 1 (1) : 1
0 3 1 1, 1 (1) : 1
0 3 1 2, 1 (1) : 1
0 3 1 3, 1 (1) : 1
0 3 1 0, 1 (1) : 1
0 3 2 1, 1 (1) : 1
0 3 2 2, 1 (1) : 1
0 3 2 3, 1 (1) : 1
0 3 2 0, 1 (1) : 1
0 3 3 1, 2 (1) : 1
0 3 3 2, 2 (1) : 1
0 3 3 3, 2 (1) : 1
0 3 3 0, 1 (1) : 1
0 3 0 1, 1 (1) : 1
0 3 0 2, 1 (1) : 1
0 3 0 3, 1 (1) : 1
0 3 0 0, 1 (1) : 1
0 0 1 1, 1 (1) : 1
0 0 1 2, 1 (1) : 1
0 0 1 3, 1 (1) : 1
0 0 1 0, 1 (1) : 1
0 0 2 1, 1 (1) : 1
0 0 2 2, 2 (1) : 1
0 0 2 3, 2 (1) : 1
0 0 2 0, 1 (1) : 1
0 0 3 1, 1 (1) : 1
0 0 3 2, 1 (1) : 1
0 0 3 3, 1 (1) : 1
0 0 3 0, 1 (1) : 1
0 0 0 1, 1 (1) : 1
0 0 0 2, 1 (1) : 1
0 0 0 3, 1 (1) : 1
1 1 1 1, 1 (1) : 1
1 1 1 2, 1 (1) : 1
```

Додаток Д

Акт впровадження ПП «Колумбус»

КОЛУМБУС
провайдер телекомунікацій

46020 м. Тернопіль
вул. Київська, 2
тел. (0352) 51-18-71
e-mail: office@columbus.in.ua

ЄДРПОУ 21150086
р/р UA 7138 0805 0000 0000 2600 5582 758
в АТ Райффайзен Банк Аваль,
МФО 380805

АКТ
про впровадження результатів дисертаційної роботи Романця Ігоря Євгеновича на тему «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти»

Даний акт складений в тому, що результати дисертаційної роботи Романця І.Є. «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» апробовано та впроваджено у IP-телефонії ПП «КОЛУМБУС», зокрема:

1. Онтологічна модель функціонування IP-телефонії формується на основі структурованого представлення концептів, сутностей, зв'язків у сфері технології VoIP, що на відміну від відомих дозволяє отримати формалізовану та семантично насичену структуру для розуміння та представлення знань про протоколи, компоненти та їх взаємодію.
2. Метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень. Запропонований метод дозволяє згрупувати повідомлення відповідно до класифікованої структури ключових понять. Таке групування доцільно використовувати для виявлення аномальних повідомлень в спеціалізованій корпоративній мережі з розгорнутою системою IP-телефонії.

Впровадження запропонованих методів аналізу мовлення та відповідної обробки природної мови, які дозволяє створювати більш точні та ефективні системи виявлення аномального трафіку та потенційно небезпечних комунікацій в системі VoIP.

Цей акт не є підставою для фінансових взаєморозрахунків.

Директор ПП «Колумбус» _____ **Зазуля Н.Г.**

Додаток Е

Акт впровадження компанії «Infineon»

АКТ

про впровадження результатів дисертаційної роботи
Романця Ігоря Євгеновича
«Інтелектуалізована комп'ютерна система виявлення аномальних повідомлень IP-телефонії в корпоративній мережі »

Ознайомлення з результатами дисертаційної роботи здобувача Західноукраїнського національного університету Романця І.Є. підвередило їх актуальність, а також наукову цінність і практичну значимість. Зокрема, з точки зору практичного використання є найбільш цікавими наступні результати:

1. Метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень. Запропонований метод дозволяє згрупувати повідомлення відповідно до класифікованої структури ключових понять. Таке групування доцільно використовувати для виявлення аномальних повідомлень в спеціалізованій корпоративній мережі з розгорнутою системою IP-телефонії.
2. Система забезпечення розподілу доступу в режимі реального часу на основі нечіткої логіки. Завдяки використанню механізму нечіткого висновку Мамдані, система здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних. Це дозволяє враховувати численні критерії, такі як IP-адреса клієнта, час здійснення дзвінка, часовий пояс і якість зв'язку, що сприяє підвищенню рівня безпеки та якості зв'язку.
3. Система виявлення та запобігання потенційних атак.

Запропоновані рішення не обмежуються системами IP телефонії, а можуть бути використані для інших систем передачі голосового трафіка через IP, наприклад в безпровідних системах. Результати роботи будуть використані при розробці нових версій програмного забезпечення для лінійки продуктів компанії Infineon's AIROC™ Wi-Fi 6/6E.

Цей акт не є підставою для фінансових взаєморозрахунків.

Консультант Infineon Technologies.
Senior Principal Engineer — Кремінь В.Т.

Додаток Ж

Акт про впровадження в Тернопільській обласній військовій адміністрації

ТЕРНОПІЛЬСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ТЕРНОПІЛЬСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
УПРАВЛІННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

вул. М. Грушевського, 8, м. Тернопіль, 46021, тел.: (0352) 51-70-11
E-mail: digital@te.gov.ua, Web: digital.te.gov.ua Код згідно з ЄДРПОУ 44253982

від_____20___року № _____ На № _____ від_____20_____року

АКТ
про впровадження результатів дисертаційної роботи
Романця Ігоря Євгеновича
«Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі»

Результати дисертаційної роботи здобувача Західноукраїнського національного університету Романця І. Є. викликають зацікавлення та можуть бути використані управління цифрової трансформації обласної військової адміністрації, а саме:

1. Метод виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень
2. Система забезпечення розподілу доступу в режимі реального часу на основі нечіткої логіки. Запропонована система продемонструвала свою ефективність. Завдяки використанню механізму нечіткого висновку Мамдані, система здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних. Це дозволяє враховувати численні критерії, такі як IP-адреса клієнта, час здійснення дзвінка, часовий пояс і якість зв'язку, що сприяє підвищенню рівня безпеки та якості зв'язку.

Наукові та практичні результати дослідження можуть знайти подальше практичне застосування у процесі захисту IP-телефонії від несанкціонованого доступу.

Цей акт не є підставою для фінансових взаєморозрахунків.

Начальник управління **Сергій ВЕРБОВИЙ**

Додаток З

Акт про впровадження в освітній процес

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
Західноукраїнського
національного університету
к.е.н., доцент Віктор ОСТРОВЕРХОВ

_____

_____ 202 р.

АКТ

про впровадження в освітній процес Західноукраїнського національного університету результатів дисертаційної роботи
Романця Ігоря Євгеновича
«Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії у корпоративній мережі»

Даний акт складений про те, що результати дисертаційної роботи Романця Ігоря Євгеновича на тему: «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії у корпоративній мережі» використані в освітньому процесі факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету для студентів спеціальності 123 «Комп'ютерна інженерія».

При викладанні дисципліни «Комп'ютерні системи» та «Комп'ютерні мережі» розглядається комп'ютерна система IP-телефонії у корпоративній мережі. При викладанні дисципліни «Програмно-апаратні засоби захисту інформації» розглядається архітектуру системи захисту IP-телефонії в корпоративній мережі, яка відрізняється від відомих наявністю блоків і процедур виявлення аномальних повідомлень.

Декан факультету комп'ютерних інформаційних технологій, к.т.н., доцент — Ігор ЯКИМЕНКО

Завідувач кафедри комп'ютерної інженерії, к.т.н., доцент — Леся ДУБЧАК

Додаток К

Акт впровадження в науково-дослідній роботі

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Західноукраїнського національного
університету
д.т.н., проф. Микола ДИВАК
_____
«___» _____ 202 р.

МІНІСТЕРСТВО ОСВІТИ ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ * 33680120 *

АКТ

про використання результатів дисертаційної роботи
Романця Ігоря Євгеновича
«Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі»

Комісія у складі: голови – декана факультету комп'ютерних інформаційних технологій, к.т.н., доц. Якименка І.З. та членів: начальника науково-дослідної частини, д.е.н., проф. Семанюк В.З., відповідального виконавця, д.т.н., проф. Пукаса А.В., начальника планово-фінансового відділу Кушніра О.Р. склали цей акт про те, що дослідження та результати дисертаційної роботи Романця І.Є. використані під час виконання науково-дослідних робіт на кафедрі комп'ютерних наук факультету комп'ютерних інформаційних технологій згідно з пріоритетним напрямом «Комп'ютерні системи та компоненти» з безпосередньою участю автора, а саме: НДР "Математичне та комп'ютерне моделювання об'єктів з розподіленими параметрами на основі поєднання онтологічного та інтервального аналізу" (2022-2024 рр., № держреєстрації 0122U001497, виконавець). Автор запропонував та обґрунтував метод виявлення аномалій в трафіку IP-телефонії, який, на відміну від існуючих, ґрунтується на поєднані методів групування VoIP повідомлень та контекстно-частотного аналізу, що у сукупності дозволило підвищити ефективність виявлення зловмисних повідомлень.

Голова комісії:
декан факультету комп'ютерних
інформаційних технологій,
к.т.н., доц. Ігор ЯКИМЕНКО

відповідальний виконавець
НДР, д. т. н., проф. Андрій ПУКАС

Члени комісії:
начальник науково-дослідної
частини, д. е. н., проф. Віта СЕМАНЮК

Начальник
планово-фінансового відділу Олексій КУШНІР