DOI 10.31891/2307-5732-2024-337-3-65
УДК 004.056.5:004.7:621.395

РОМАНЕЦЬ ІГОР
Західноукраїнський національний університет
https://orcid.org/0000-0002-7061-6527
e-mail: i.romanets@wunu.edu.ua

АРХІТЕКТУРА ІНТЕЛЕКТУАЛІЗОВАНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВИКОРИСТАННЯ IP-ТЕЛЕФОНІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

У статті запропоновано архітектуру інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі. Розробка таких систем є актуальною через зростання кількості кібератак та внутрішніх загроз, що можуть призвести до серйозних порушень безпеки та конфіденційності корпоративних даних. Запропонована система використовує методи машинного навчання та аналізу даних для виявлення аномалій у поведінці користувачів, що дозволяє оперативно реагувати на потенційні загрози. Описано основні компоненти архітектури, такі як модулі збору та обробки даних, аналізу поведінки та прийняття рішень. Особлива увага приділяється питанням застосування штучного інтелекту та інтеграції системи з існуючими інфраструктурами та забезпечення її масштабованості та надійності. На основі досліджень розроблена розгорнута схема архітектури інтелектуалізованої системи.

Ключові слова: VoIP; Internet Protocol; телефонні лінії; голосовий зв'язок; аномальний трафік, штучний інтелект, машинне навчання.

ROMANETS IHOR
West Ukrainian National University

ARCHITECTURE OF AN INTELLIGENT SYSTEM FOR CONTROLLING ATYPICAL BEHAVIOR OF IP-TELEPHONY USERS IN A CORPORATE NETWORK

The article presents the architecture of an intelligent system for controlling atypical behavior of IP-telephony users in a corporate network. The development of such systems is relevant due to the growing number of cyberattacks and internal threats that can lead to serious breaches of security and confidentiality of corporate data. To analyze VoIP content, it is necessary to formalize the method of constructing a basic message in IP telephony. To do this, it is necessary to first convert the VoIP media message into a text representation and thus form a database of already text messages. The proposed system uses machine learning and data analysis methods to detect anomalies in user behavior, which allows for a prompt response to potential threats. The developed AISES-VoIP (Architecture of an Intelligent System for Ensuring the Security of VoIP) system, in comparison with existing solutions, has a powerful subsystem for analytics and reporting with the possibility of intelligent data analysis and the availability of means for adaptive integration into external specialized information systems and the possibility of integrating specialized software modules. The main components of the architecture are described, such as modules for data collection and processing, behavioral analysis, and decision making. Particular attention is paid to the application of artificial intelligence and integration of the system with existing infrastructures, as well as ensuring its scalability and reliability. On the basis of the research, a detailed architecture scheme of the intelligent system is developed. The implementation of natural language processing methods is a key element of the intellectualized system for analyzing atypical behavior of IR telephony users. This allows you to create a more effective system for detecting anomalous traffic and potentially dangerous communications.

Keywords: VoIP; Internet Protocol; telephone lines; voice communication; anomalous traffic, artificial intelligence, machine learning.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

В даний час зберігається тенденція до зростання кількості кібератак на комп'ютерні системи, а також внутрішніх загроз, що можуть призвести до серйозних порушень безпеки та конфіденційності корпоративних даних. Тому проблема виявлення мережевих аномалій перебуває в динамічній сфері досліджень, особливу увагу привертають системи контролю нетипової поведінки користувачів IP-телефонії в корпоративній мережі.

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 бажає спілкуватися більш ефективно.

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 такий зв'язок потрібно захищати, так як, завдяки Інтернету, він доступний для проникнення із любої точки світу.

Об'єкт дослідження – IP-телефонія у корпоративній мережі.

Предмет дослідження – процеси контролю нетипової поведінки користувачів.

Мета роботи – розробити архітектуру інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження:*

1. Розробити узагальнену структуру і визначити підсистеми, що будуть входити в архітектуру інтелектуалізованої системи.

2. Розробити схеми підсистем як складові компоненти архітектури інтелектуалізованої системи та визначити їх ролі в IP-телефонії корпоративної мережі.
3. Провести аналіз всіх підсистем інтелектуалізованої системи контролю.

Аналіз досліджень та публікацій

Дослідники підходили до цієї проблеми, використовуючи різні методи, такі як штучний інтелект, машинне навчання та моделювання автоматів. Наприклад, американськими дослідниками у статті представлено огляд області виявлення мережевих аномалій [1]. На основі наведених прикладів видно, що існує значна перевага у використанні широкого спектру методів обробки сигналів для вирішення проблеми виявлення аномалій. Більш тісна синергія між мережевими технологіями та методами обробки сигналів сприяє розробці більш ефективних інструментів для виявлення мережевих аномалій.

У 2019 році індійськими дослідниками у запропоновано три підходи на основі машинного навчання для виявлення аномалій у трафіку IP-мереж [2]. Розроблена стратегія багатовимірного гауссового 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

У 2020 році тайванськими вченими було представлено нову систему раннього виявлення шкідливого трафіку, а саме D-PACK, яка базується на вибірці трафіку, автопрофілюванні трафіку та неконтрольованій моделі DL (автокодер) [3]. Результати тестування показали, що D-PACK може виявляти зловмисний трафік з майже 100% точністю. Крім того, він скорочує тривалість попередньої обробки потоку порівняно з попередніми роботами.

Японські дослідники у 2023 році запропонували метод виявлення мережевих аномалій для великомасштабних глобальних IP-мереж за допомогою потужної системи Fast xFlow Proxy, яка може вимірювати IP-трафік з дрібнозернистою роздільною здатністю [4]. Метод базується на аналізі кореляційних значень з минулими часовими рядами, оскільки часові ряди окремих потоків мають тенденцію до періодичних коливань.

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.

Формулювання цілей статті

На основі аналізу вище наведених досліджень і з врахуванням запропонованих рішень [5-7] запропоновано узагальнену архітектуру інтелектуалізованої системи контролю нетипової поведінки користувачів IP-телефонії (рис. 1), серцевиною якої є чотири базові підсистеми:

- підсистема моніторингу трафіку
- підсистема аналізу
- підсистема прийняття рішень
- підсистема звітності та аналітики

Розглянемо детальніше кожну із підсистем.

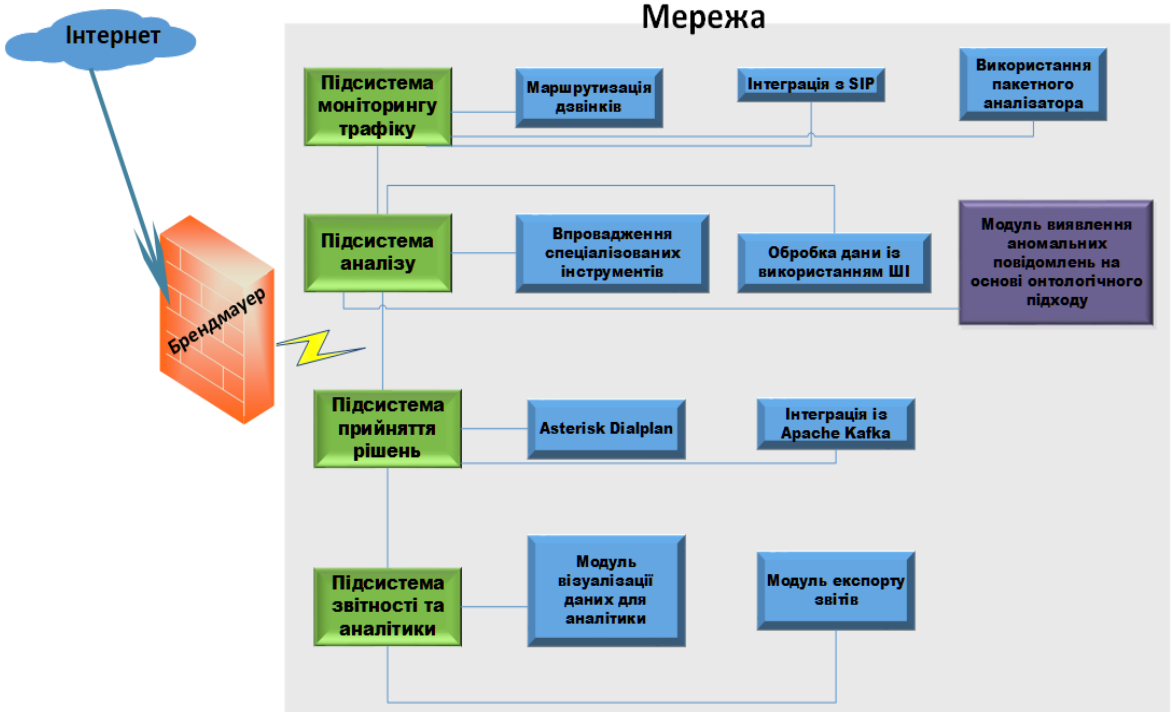

Рис. 1. Узагальнена архітектура інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережі

Підсистема моніторингу трафіка включає в себе IP-телефонію, що відповідає за маршрутизацію дзвінків та забезпечення основної функціональності 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 (ТфЗК), 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. Протокол ініціювання сеансу (SIP) з'явився як технологія, яка досить добре доповнює VoIP [9].

Послуга SIP-транкінг дозволяє використовувати існуюче обладнання АТС для переходу до телефонної мережі з підключенням до Інтернету. Також можна використовувати SIP-телефон як частину системи уніфікованих комунікацій. Крім того, можна синхронізувати всі канали зв'язку в режимі реального часу. SIP-транкінг працює як посередник між бізнес-телефонією та постачальником послуг інтернет-телефонії (ITSP) (рис. 2) [10].

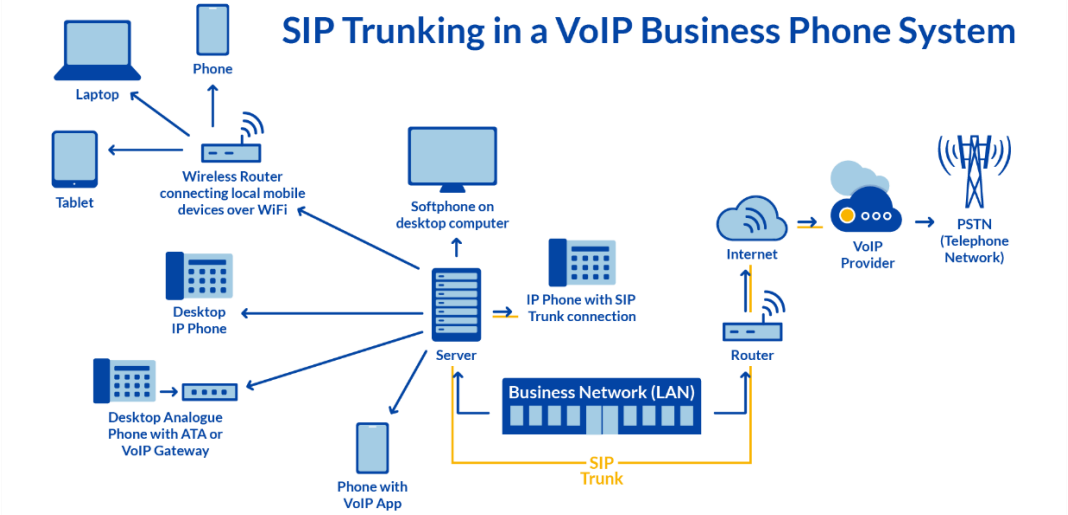

Рис. 2. SIP-транкінг в VoIP-телефонії [10]

При цьому, весь цей трафік потрібно постійно моніторити на предмет виявлення аномалій Для цього доцільно застосовувати аналізатор мережевих пакетів Wireshark (рис. 3). Він має відкритий вихідний код і представляє перехоплені дані пакетів в максимально детальному вигляді [11].

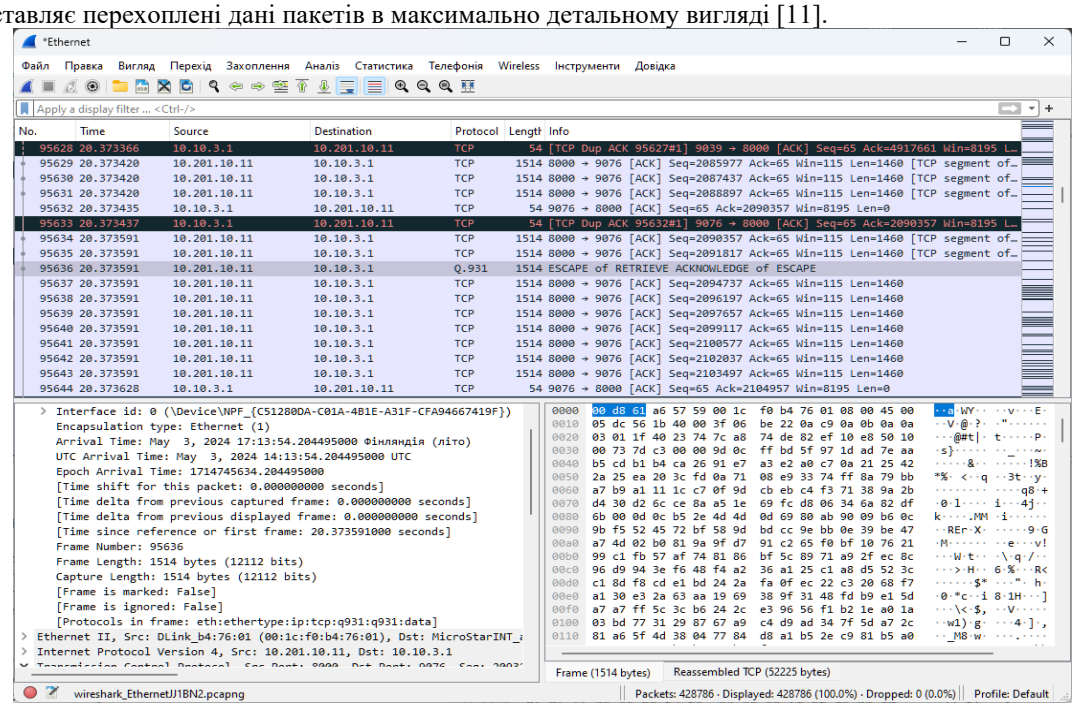

Рис. 3. Перегляд вмісту перехоплених пакетів Wireshark

Однією із функцій Wireshark є захоплення даних пакетів з мережевого інтерфейсу у реальному часі. Ці дані зберігаються і далі експортуються у різні формати файлів з можливим переглядом їх вмісту.

Після перехоплення та перегляду пакетів проводять аналіз на предмет виявлення індикаторів нетипової або підозрілої активності.

Підсистема аналізу впроваджує спеціалізовані інструменти такі як Snort або Suricata. Розглянемо більш детальніше їх роботу.

Коли мова заходить про системи виявлення мережевих вторгнень Network Intrusion Detection System (NIDS), використовують спеціалізовані інструменти Suricata та Snort у складі. Ці інструменти з відкритим вихідним кодом пропонують розширені функції для моніторингу та захисту мереж від потенційних загроз.

NIDS використовує різні методи для виявлення та попередження про потенційні загрози. Наприклад, сигнатура Signature-based Detection (SIDS) виявляє загрози до зловмисної активності, тоді як Anomaly-based Detection (AIDS) виявляє відхилення від нормальної поведінки мережі, які можуть свідчити про атаку [12].

Suricata може використовуватися як система запобігання вторгненням (IPS) та механізм моніторингу мережевої безпеки, Вона аналізує мережевий трафік, на основі заздалегідь визначених правил для виявлення зловмисної активності та сповіщення адміністраторів про потенційні загрози (рис. 4). Suricata відрізняється від інших систем своєю багатопотоковою архітектурою, яка дозволяє їй ефективно обробляти кілька завдань одночасно.

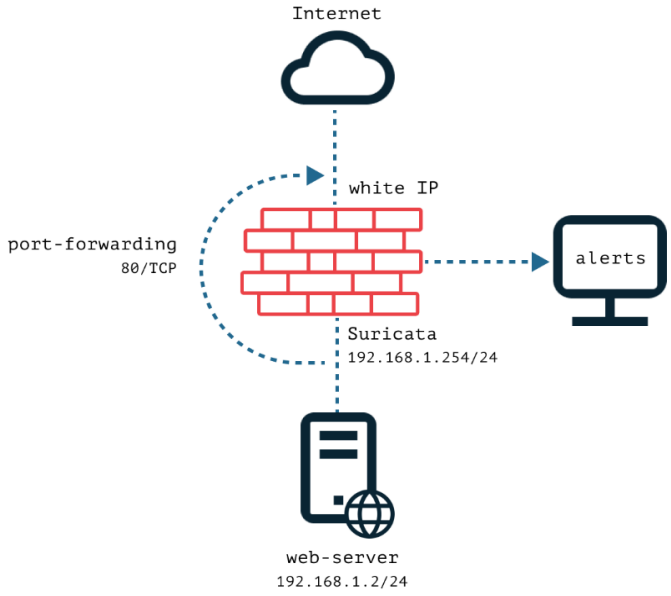

Рис. 4. Мережева схема на базі Suricata [13]

Snort – популярна система виявлення мережевих вторгнень з відкритим вихідним кодом на основі правил та аналізі протоколів. Вона відстежує мережевий трафік і застосовує попередньо визначені правила для виявлення зловмисної активності, генеруючи сповіщення для адміністраторів для вжиття відповідних заходів. Така адаптивність дозволяє Snort відмінно працювати в різних середовищах, забезпечуючи індивідуальний захист від широкого спектру загроз.

Порівнюючи Suricata і Snort, важливо вивчити ключові характеристики, якими повинні володіти IDS, щоб визначити їхню ефективність і придатність для різних середовищ. Розглянемо основні характеристики обох інструментів, підкресливши їх схожість та відмінності (табл. 1).

Виявлення на основі правил є основною функцією як Suricata, так і Snort, що використовує заздалегідь визначені правила для виявлення зловмисної активності в мережевому трафіку. Перевага Snort полягає в широкому наборі правил, які можна налаштувати відповідно до конкретних потреб безпеки. Suricata також пропонує надійний набір правил з додатковою перевагою - Suricata-Update, інструментом для більш ефективного управління та оновлення наборів правил.

Таблиця 1

Порівняння функціональних можливостей Suricata і Snort [12]

SURICATA	SNORT
Багатопотокова архітектура дозволяє ефективно обробляти кілька завдань одночасно	Однопотокова архітектура
Suricata-Update для управління та оновлення наборів правил	Ширша сумісність із пристроями, операційними системами та сторонніми інструментами завдяки довшій присутності на ринку
Розширені можливості виявлення та запобігання вторгненням	Зосередженість на виявленні на основі правил та аналізі протоколів
Підвищена продуктивність у середовищах з високим трафіком	Краща продуктивність в умовах обмежених ресурсів
Підтримує вбудований і пасивний режими	Підтримує вбудований і пасивний режими

Зараз у високому темпі наростає обробка та аналіз даних з використанням машинного навчання та штучного інтелекту (ШІ). IP-мережі є методологічною основою для штучного інтелекту через величезний обсяг даних, які IP-мережі реєструють щосекунди. По-перше, резервуар трафіку мережі забезпечує достатню кількість даних для роботи будь-якого складного алгоритму. По-друге, прогрес у захопленні та обробці трафіку в режимі реального часу за допомогою таких інструментів, як IP-зонди, забезпечує повноту даних і відсутність затримок у часі. Це гарантує точність і релевантність аналітичних результатів. По-третє, різноманітність сучасних потоків трафіку з точки зору користувачів, додатків і послуг несе в собі безмежну інформаційну цінність, яка при розумному використанні може дати неоціненну інформацію для операційних поліпшень і зростання бізнесу.

Глибока перевірка пакетів (англ. Deep packet inspection DPI) нового покоління для аналітики мережевого трафіку:

- зіставлення шаблонів, яке сканує корисне навантаження пакетів;
- розширений поведінковий, статистичний і евристичний аналіз, який оцінює рух пакетів, такі як частота і затримки

Використовуючи ці методології, DPI:

- ідентифікує протоколи, типи додатків і сервісів;
- обчислює критично важливу інформацію щодо використання та продуктивності мережі;
- встановлює стан безпеки мережі, виявляючи зловмисний, аномальний і підозрілий трафік.

Сьогодні до 95% усіх потоків трафіку є зашифрованими [14]. Такі додатки, як WhatsApp і Telegram, використовують шифрування. Також все частіше використовуються методи анонімізації та маскування, такі як VPN і TOR. Це створює серйозні проблеми з видимістю для традиційних інструментів DPI. Наприклад, новітні методи шифрування, включаючи TLS 1.3, ESNI і QUIC, поступово приховують інформацію про рукостискання, а деякі навіть приховують дані заголовків пакетів, що робить неможливим для традиційних інструментів DPI ідентифікувати основні потоки трафіку.

Для усунення цього обмеження доцільно застосувати аналітику зашифрованого трафіку, яка розширила межі перевірки трафіку на основі DPI шляхом об'єднання [14]: Алгоритмів ML (наприклад, k-найближчих сусідів (k-NN) і навчання на основі дерева рішень); Алгоритмів DL (наприклад, згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та мережі з довгою короткочасною пам'яттю (LSTM)); Аналізу даних високої розмірності; Вдосконалених методів кешування. Маючи понад 1000 функцій, включаючи статистичні, часові ряди та функції на рівні пакетів, ці методи дозволяють виявляти основні додатки в реальному часі.

Виклад основного матеріалу

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 (рис. 5).

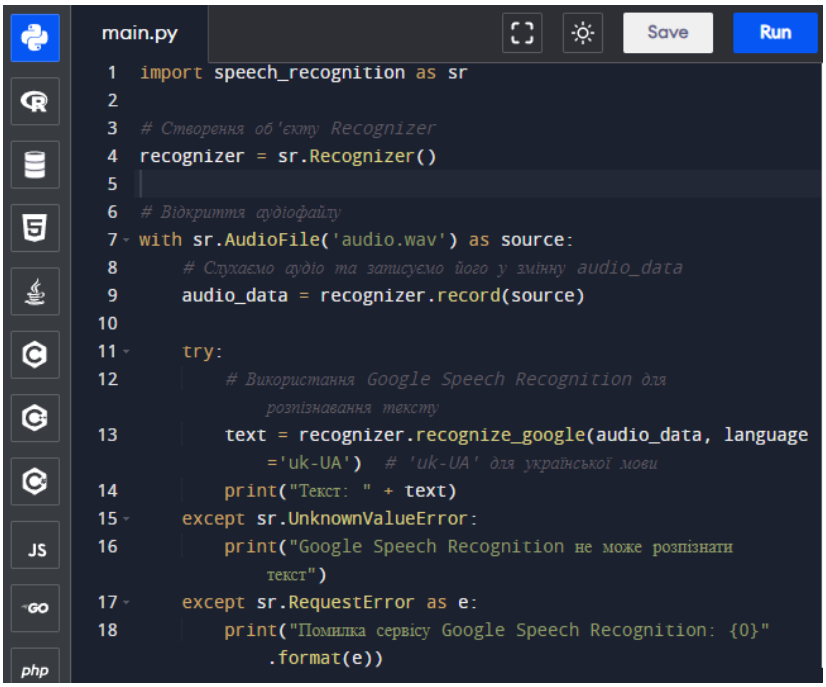

Рис. 5. Фрагмент лістингу програмного коду для перетворення VoIP–медіа повідомлення в текстове представлення

Тематику таких повідомлень задаємо загальним текстовим ідентифікатором IMP предметної області та відповідним специфікатором SM [15, 16, 23]. За допомогою перетворення голосового повідомлення у текстове представлення та процедури символьної конкатенації VPS=IMP & SM отримаємо множину VP текстових повідомлень, які представлені наборами відповідних компонентів конкретних понять

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

де P – потужність множини VP ; VP_i – елемент множини, що визначає набір понять i - того повідомлення.

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

$$\mathrm{VPK} = \left\{\mathrm{VP}_{i*}^{*} | \mathrm{VP}_{i*} \in \mathrm{VP}, \mathrm{VP}_{i*}.\mathrm{theme} \cap \mathrm{IMP} \neq \emptyset\right\}_{i=1}^{P*}$$

$$VPK = \left\{VP_{i*}^{*} | VP_{i*} \in VP, VP_{i*}.theme \cap IMP \neq \emptyset\right\}_{i=1}^{P*}. \quad (2)$$

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 [15, 16, 23].

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 виділених ключових понять

$$LKB\left(VP_i^*\right) =< C_{ik}\left(VP_i^*\right) >_{k=1}^{CPi} \quad (3)$$

Така множина може також 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:

$$BCM = \{(CS_l, NCS_l) | CS_l\}, \quad (4)$$

$$GCM = \{(CS_m, NCS_m) | CS_m \in \bigcup_i LKB(VP_i^*)\} \quad (5)$$

Для знаходження понять, які будуть релевантних 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

$$\mathrm{CSC} = \left\{(CS_l, NCS_l) \left| FCL_l = \frac{NCS_l}{P^*} \right\rangle FF_0\right\}, \quad (6)$$

де змінна F_0, належить інтервалу [0.200; 0.500], а її конкретне значення 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 (6). Розглянемо деяку визначену і впорядковану вибірку SCMF, яка також включає відповідні частоти понять у повідомлені

$$\mathrm{SCMF} = \{NCS_l | (CS_l, NCS_l) \in BCM\}. \quad (7)$$

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, то здійснюємо впорядкування цієї множини. Рангові номери присвоюємо лише ключовим концептам. Так CRC_{ik} позначає ранг k-го концепту в і-тому повідомлені. 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, і чим коротше повідомлення, тим швидше відбуватиметься це спадання. Для моделювання такого процесу можна використати кубічний сплайн [16]. Зокрема найтриваліше повідомлення буде мати важливість для цього аргументу рівну 1, якщо похідна дорівнює 0. Вводимо систему ваг $CSG(i) = \frac{csg(i)}{\sum_i csg(i)}$.,, яка матиме нормований характер, та обчислюємо усереднений ранг k-го концепту:

$$RA_k = \sum_i \quad R_{ik} CSG(i) \quad (8)$$

Ранжування концептів здійснюємо на основі усереднення рангів, а їх узгодженість перевіряємо із використанням коефіцієнта конкордації [12]

$$CSW = \frac{12\sum_{k=1}^{K}\left(\sum_{i=1}^{I} R_{ik} CSG(i) - \bar{R}\right)}{I^2(K^3 - K)}, \quad (9)$$

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

$$I(K-1)CSW > \chi^2_{K-1,\alpha} \quad , \quad (10)$$

то таке ранжування є значущим [16].

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 спосіб 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.

Підсистема прийняття рішень відіграє ключову роль в управлінні викликами та маршрутизації дзвінків. Вона будується на основі Asterisk [17, 18] і складається з різних компонентів і правил, які визначають, як система повинна обробляти вхідні та вихідні дзвінки, а також інші події.

Комунікаційний інструмент з відкритим кодом Asterisk включає різноманітні модулі (Рис. 6). Наприклад, один модуль може дозволити системі Asterisk зв'язуватися з аналоговими телефонними лініями, в той час як інший може додати можливості звітування про дзвінки [14]. Asterisk зазвичай не працює без певного підключення або взаємодії з іншими мережевими пристроями або файлами у локальній системі [17].

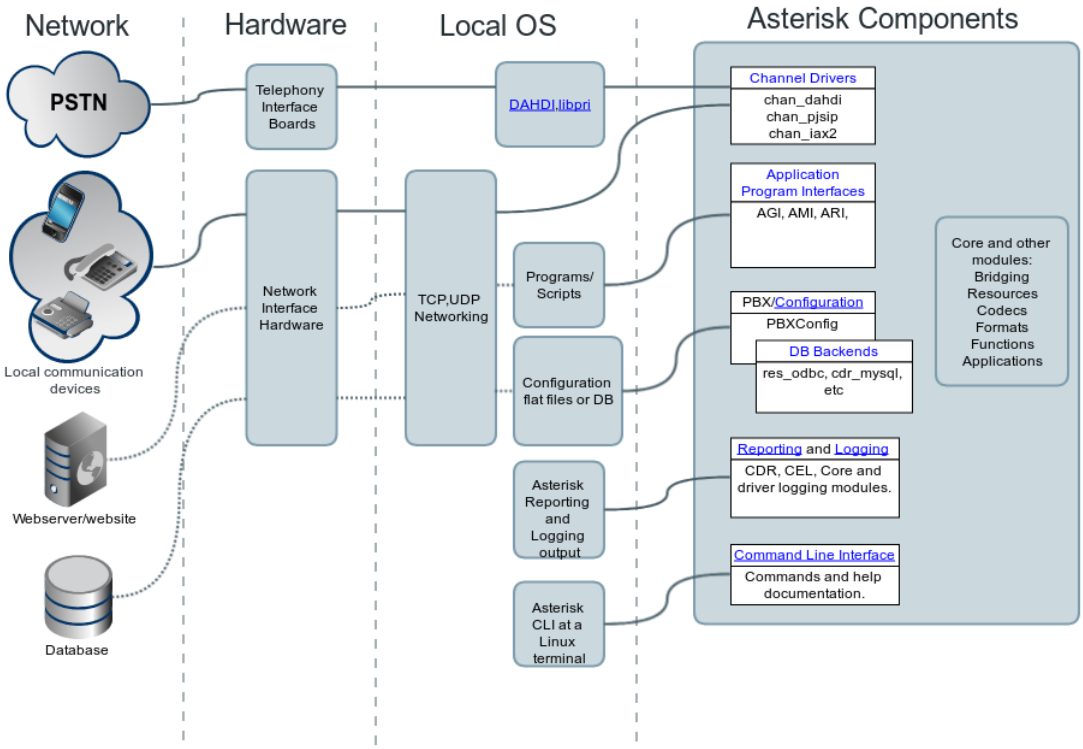

Рис. 6. Система Asterisk [17]

Канали часто використовують проміжну інфраструктуру для взаємодії з іншими каналами. Приведемо основні компоненти та принципи роботи підсистеми прийняття рішень в Asterisk:

1. Dialplan (План набора):
   - Extensions.conf: Основний конфігураційний файл, в якому визначаються правила маршрутизації дзвінків. В ньому прописані контексти, розширення та команди.
   - Контексти: Логічні групи розширень, що дозволяють організувати різні сценарії обробки дзвінків. Контексти забезпечують ізоляцію між різними наборами правил.
2. AGI (Asterisk Gateway Interface):
   - Механізм, який дозволяє запускати зовнішні скрипти для обробки дзвінків. Скрипти можуть бути написані на різних мовах програмування (Perl, Python, PHP і т.д.) і можуть взаємодіяти з Asterisk через стандартний ввід/вивід.
3. AMI (Asterisk Manager Interface):
   - Інтерфейс для взаємодії з Asterisk в реальному часі через TCP-з'єднання. Використовується для моніторингу та управління дзвінками, а також для отримання інформації про стан системи.
4. Розширення та пріоритети:
   - Кожне розширення в dialplan має послідовність пріоритетів, що визначають порядок виконання команд. Кожна команда виконується послідовно, поки не досягнуто кінцевої точки або не відбулося перенаправлення дзвінка.
5. Функції та застосунки:
   - Asterisk має велику кількість вбудованих функцій та застосунків, таких як Dial(), Playback(), VoiceMail(), які можуть бути використані в dialplan для різних завдань, таких як здійснення дзвінків, відтворення записів, обробка голосової пошти тощо.
6. Контрольні структури:

- У dialplan можна використовувати умовні вирази (GotoIf, ExecIf) та цикли для створення більш складних логічних сценаріїв.

7. База даних:

Dialplan – ядро будь-якої системи Asterisk- визначає, як обробляються вхідні та вихідні дзвінки. Dialplan складається зі списку інструкцій або кроків [19]. Діалоговий план Asterisk задається у файлі конфігурації з назвою *extensions.conf*.Файл extensions.conf зазвичай знаходиться у каталозі */etc/asterisk/,* але його розташування може змінюватися залежно від способу встановлення Asterisk. Інші поширеними місцями розташування цього файлу *є /usr/local/asterisk/etc/* та */opt/asterisk/etc/.*

Програма Playback() використовується для відтворення раніше записаного звукового файлу через каналом. При використанні програми Playback() ввід від користувача просто ігнорується.

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. Вона може бути розгорнута на "голому" обладнанні, віртуальних машинах і контейнерах як у локальному, так і в хмарному середовищі [20].Kafka працює як кластер з одного або декількох серверів, який може охоплювати кілька центрів обробки даних або хмарних регіонів. Деякі з цих серверів утворюють рівень зберігання даних, так звані брокери. На інших серверах працює Kafka Connect для безперервного імпорту та експорту даних у вигляді потоків подій, щоб інтегрувати Kafka з існуючими системами, такими як реляційні бази даних, а також з іншими кластерами Kafka. Кластер Kafka має високу масштабованість і відмовостійкість: якщо один із серверів вийде з ладу, інші візьмуть на себе його роботу, щоб забезпечити безперервну роботу без втрати даних.

Клієнти дозволяють писати розподілені додатки та мікросервіси, які читають, записують та обробляють потоки подій паралельно, в масштабі та відмовостійкості навіть у випадку проблем з мережею або збоїв у роботі машини. Kafka постачається з декількома такими клієнтами, які доповнюються десятками клієнтів, наданих спільнотою Kafka: клієнти доступні для Java та Scala, включно з бібліотекою Kafka Streams вищого рівня, для Go, Python, C/C++ та багатьох інших мов програмування, а також REST API.

На рисунку 7 зображено як два різних клієнти-продюсери публікують, незалежно один від одного, нові події в темі. Події з однаковим ключем (позначені кольором на рис. 7) записуються в один розділ.

Щоб забезпечити стійкість і доступність даних, кожну тему можна реплікувати, навіть між георегіонами або центрами обробки даних. Така реплікація виконується на рівні тематичних розділів. Типовим параметром є коефіцієнт реплікації 3, тобто завжди буде три копії даних.

Apache Flink – це фреймворк і рушій розподіленої обробки для обчислень з урахуванням стану над необмеженими і обмеженими потоками даних. Flink був розроблений для роботи в усіх поширених кластерних середовищах, виконання обчислень зі швидкістю в пам'яті і в будь-якому масштабі [21].

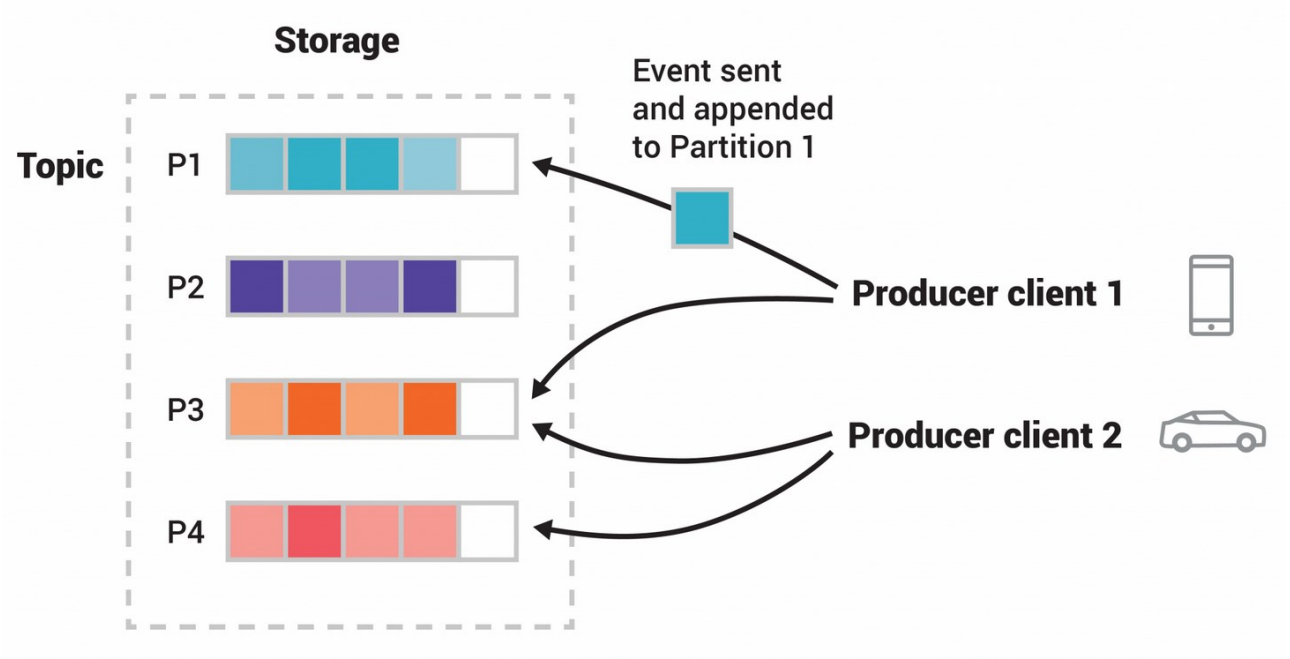

Рис. 7. Приклад теми з чотирьох розділів P1-P4 [20]

Будь-які дані генеруються як потік подій. Наприклад, транзакції за кредитною карткою, вимірювання датчиків, машинні журнали або взаємодія користувачів на веб-сайті чи в мобільному додатку – всі ці дані генеруються як потік. Дані можна обробляти як необмежені або обмежені потоки. Необмежені потоки мають початок, але не мають визначеного кінця.. Необмежені потоки повинні оброблятися безперервно, тобто події повинні негайно оброблятися після того, як вони були отримані. Обробка необмежених даних часто вимагає,

щоб події надходили в певному порядку, наприклад, в порядку їх виникнення, щоб мати можливість міркувати про повноту результату.

Обмежені потоки мають визначений початок і кінець. Обробка обмежених потоків може здійснюватися шляхом поглинання всіх даних перед виконанням будь-яких обчислень. Впорядковане поглинання не є обов'язковим для обробки обмежених потоків, оскільки обмежений набір даних завжди можна відсортувати. Обробка обмежених потоків також відома як пакетна обробка.

Точний контроль часу та стану дозволяє Flink запускати будь-які програми на необмежених потоках. Обмежені потоки обробляються алгоритмами та структурами даних, спеціально розробленими для наборів даних фіксованого розміру, що забезпечує потрібну продуктивність.

Apache Flink є розподіленою системою і вимагає обчислювальних ресурсів для виконання додатків. Flink інтегрується з усіма поширеними менеджерами кластерних ресурсів, такими як Hadoop YARN та Kubernetes, але також може бути налаштований для роботи як окремий кластер [21].

Під час розгортання Flink автоматично визначає необхідні ресурси на основі налаштованого паралелізму програми і запитує їх у менеджера ресурсів. У разі збою Flink замінює контейнер, що вийшов з ладу, запитуючи нові ресурси. Вся комунікація для відправки або управління додатком відбувається за допомогою REST-дзвінків. Це полегшує інтеграцію Flink у багато середовищ.

Flink призначений для запуску потокових додатків з підтримкою стану в будь-якому масштабі. Додатки розпаралелюються на тисячі завдань, які розподіляються і паралельно виконуються в кластері. Таким чином, додаток може використовувати практично необмежену кількість процесорів, оперативної пам'яті, дискового та мережевого вводу-виводу. Більше того, Flink легко підтримує дуже великий стан програми. Його асинхронний та інкрементний алгоритм встановлення контрольних точок забезпечує мінімальний вплив на затримки обробки, гарантуючи при цьому однозначну узгодженість стану.

Додатки Flink з підтримкою стану оптимізовані для локального доступу до стану. Стан задачі завжди зберігається в пам'яті або, якщо розмір стану перевищує доступний обсяг пам'яті, в ефективних для доступу структурах даних на диску, як показано на рисунку 8. Таким чином, завдання виконують всі обчислення, звертаючись до локального, часто в пам'яті, стану, що призводить до дуже низьких затримок при обробці [21]. Flink гарантує однократну узгодженість стану у випадку збоїв, періодично та асинхронно виконуючи контрольну точку локального стану у довготривале сховище.

Підсистема звітності та аналітики базується на інтеграції із візуалізацією даних з використанням ПЗ з відкритим вихідним кодом Grafana. Це 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. На рисунку 9 наведено приклад дашборду, налаштованого за допомогою веб-інтерфейсу Grafana [22].

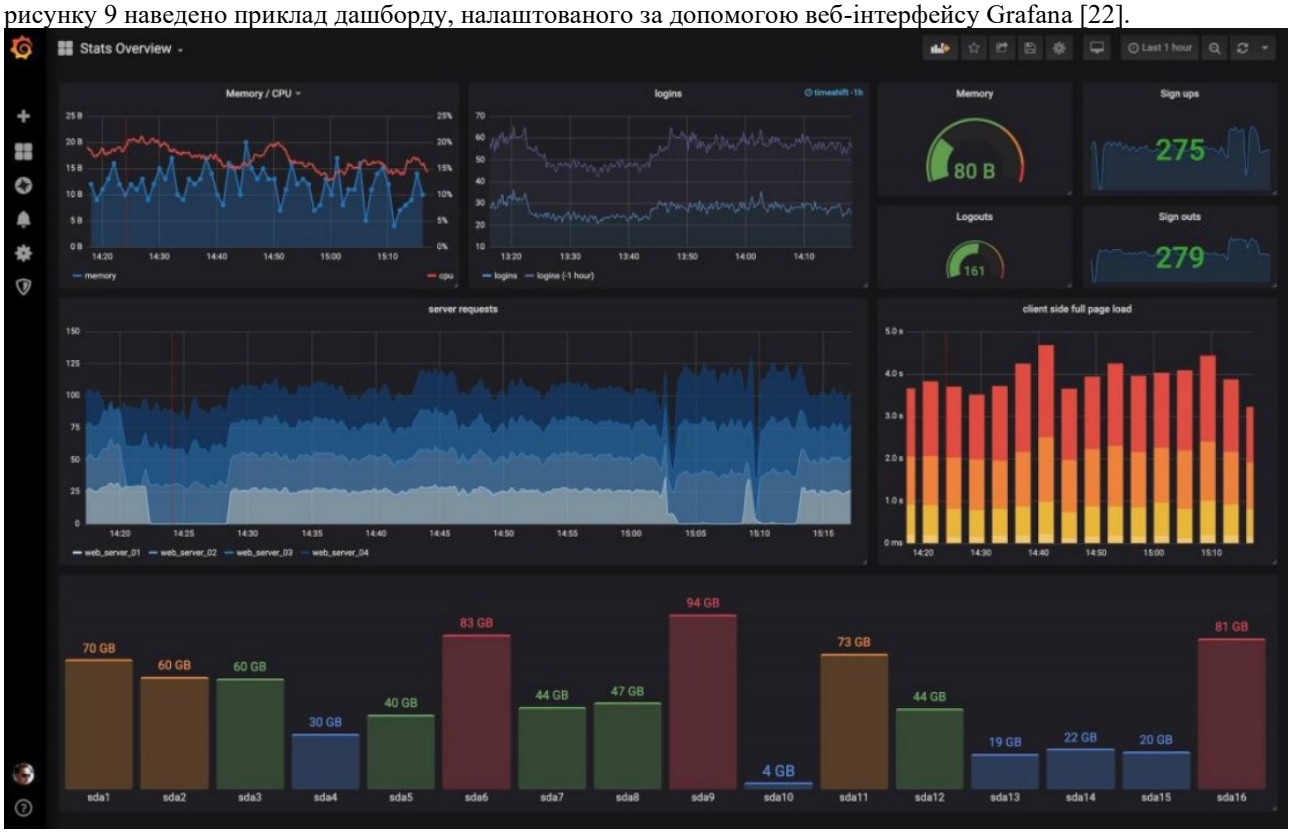

Рис. 8. Дашборд веб-інтерфейсу Grafana [22]

Функція, яка робить Grafana дійсно популярною, – це можливість легко ділитися дашбордами з іншими.

Зазвичай запускають дашборди, використовуючи існуючі журнали. Якщо ще немає центрального місця для зберігання логів з різних частин додатку, Scalyr з дашбордом Grafana. Можна додати Scalyr як джерело даних на інформаційну панель за допомогою плагіна з відкритим вихідним кодом. За допомогою плагіна можна переглядати метрики на основі логів у Grafana, а потім перейти на сайт Scalyr, щоб переглянути ваші логи більш детально [22].

Grafana – це інструмент аналізу та моніторингу баз даних з відкритим вихідним кодом, який легко встановити на будь-яку операційну систему. Доступ до нього здійснюється через браузер, тому його можна розгорнути у хостинговій компанії, а потім надати доступ до нього.

Можна відображати всі дані (навіть з декількох джерел) у будь-якому форматі, який найбільше підходить. Існує широкий вибір візуалізацій вбудованих і доступних через спільноту. Можна налаштувати панелі за допомогою кольору і прозорості - все, що має сенс для візуалізації. Можна створювати власні плагіни візуалізації.

Для забезпечення подальшої 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 [22].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Розроблені система AISES-VoIP (Architecture of an Intelligent System for Ensuring the Security of VoIP) 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. В таблиці 2. представлено результати порівняння основних показників, які впливають на ефективність системи контролю нетипової поведінки користувачів IP-телефонії.

Таблиця 2

Порівняння систем контролю нетипової поведінки користувачів IP-телефонії

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

Експериментальні дослідження також виявили кілька областей для подальшого вдосконалення. Наприклад, підвищення точності алгоритмів машинного навчання за рахунок використання більшого обсягу навчальних даних та розширення набору показників для аналізу поведінки користувачів. Крім того, доцільно розглянути можливість впровадження додаткових функцій, таких як автоматизоване реагування на виявлені загрози та детальне звітування про аномалії.

З врахуванням викладеного вище, розроблено структурно-функціональну схему архітектури інтелектуалізованої системи контролю нетипової поведінки користувачів IP-телефонії (рис. 9).

З постійним розвитком технологій штучного інтелекту все важливішим стає напрямок використання інтелектуальних засобів для аналізу контенту в системі VoIP. З врахуванням цього, розроблено узагальнену і структурно-функціональну схеми інтелектуалізованої системи забезпечення безпеки використання IP-телефонії в корпоративній мережію.

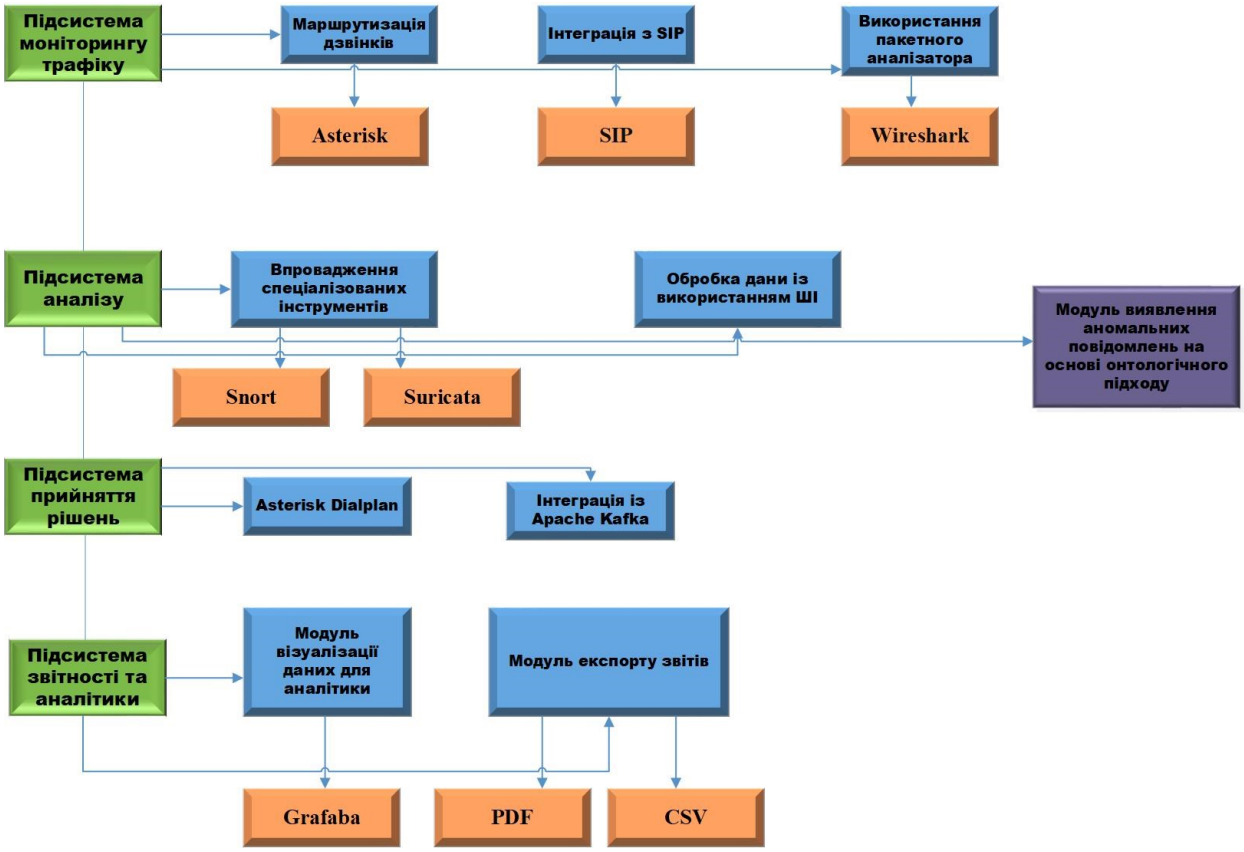

Рис. 9. Структурно-функціональна схема архітектури інтелектуалізованої системи

Запропонована система базується на знання-орієнтованому підході з використанням онтології, та сучасних програмно-інтерпретованих засобах інтелектуального аналізу даних, що дозволило забезпечити підвищення рівня виявлення аномалій у поведінці користувачів корпоративної IP-телефонії.

Ключовим елементом інтелектуалізованої системи аналізу нетипової поведінки користувачів IP-телефонії є реалізація методів обробки природної мови. Це дозволяє створити більш ефективну систему виявлення аномального трафіку та потенційно небезпечних комунікацій.

Запропоновано онтологію опису VoIP повідомлень в системі IP-телефонії, здійснено формалізацію основних понять у формі окремих концептів, та описано зв'язки між цими поняттями.

Здійснено тестування та апробація системи ISMAB-VoIP, включаючи тестування модулів збору та обробки даних, аналізу поведінки та прийняття рішень. В роботі досліджено можливість інтеграції системи з існуючими інфраструктурами підприємств, що підтвердило можливість її масштабування.

Впровадження таких систем є вкрай важливим у сучасних умовах зростання кіберзагроз і внутрішніх ризиків, що дозволяє своєчасно реагувати на потенційні загрози та захищати корпоративні дані від несанкціонованого доступу та витоків інформації.

У подальших дослідженнях планується вдосконалення методів та засобів інтелектуального аналізу даних, розширення функціональних можливостей системи для підвищення рівня безпеки і стабільності корпоративних VoIP.

References

1. 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

2. 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

3. 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

4. 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. https://doi.org/10.1109/ACCESS.2023.3334212.

5. 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. https://doi.org/10.1109/ECAI.2018.8678992

6. 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. https://doi.org/10.47839/ijc.16.4.910

7. Романець, І. (2024). Захист від термінації трафіку в IP-мережі на основі нечіткої логіки. Measuring And Computing Devices In Technological Processes, (1), 186–193. https://doi.org/10.31891/2219-9365-2024-77-23

8. Doan A. (2023). What Is VoIP? The Newbie's Guide to Voice over IP. URL: https://www.nextiva.com/blog/what-is-voip.html.

9. 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/

10. 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.

11. Sharpe R., Warnicke E., Lamping U. (2021). Wireshark User's Guide. URL: https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs.

12. DeVito A. (2024). Suricata vs Snort: A Comprehensive Review. URL: https://www.stationx.net/suricata-vs-snort/.

13. Snort and Suricata. (2023). URL: https://habr.com/companies/selectel/articles/744478/

14. Müller S. (2024). Powering Network Analytics with Machine Learning & A. Rohde & Schwarz, URL: https://www.ipoque.com/blog/powering-network-analytics-with-ml-ai.

15. 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.

16. Romanets I.Eu. (2024). ONTOLOGICAL APPROACH IN THE USING SECURITY SYSTEM IP TELEPHONY. *Opto-electronic information-power technologies*. 47, 1 2024), 240–252. DOI: https://doi.org/10.31649/1681-7893-2024-47-1-240-252.

17. Asterisk Documentation. (2020). URL: https://docs.asterisk.org/Fundamentals/Asterisk-Architecture/.

18. Asterisk Documentation. (2020). URL: https://docs.asterisk.org/Fundamentals/Asterisk-Architecture/Asterisk-Architecture-The-Big-Picture/

19. 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

20. What is Apache Kafka. (2022). Kafka. URL: https://kafka.apache.org/intro

21. What is Apache Flink? (2024). Apache Software Foundation. URL: https://flink.apache.org/what-is-flink/flink-architecture/

22. Manage Test Results. (2023). Grafana Labs Documentation. URL: https://grafana.com/docs/grafana-cloud/testing/k6/analyze-results/manage-test-results/

23. 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. https://doi.org/10.3390/s21248320