МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Методи інформаційно-комунікаційного забезпечення системи "Smart hospital"»

Виконавець: _____ Аліна АНДРЕЄВА
(підпис)

Керівник: _____ Віктор ГНАТЮК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Андреєвої Аліни Ігорівни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Методи інформаційно-комунікаційного забезпечення системи "Smart hospital"»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: дослідження і проєктування методів інформаційно-комунікаційного забезпечення системи "Smart hospital".
4. Зміст пояснювальної записки: Вступ, Залучення інструментів інформаційно-аналітичних систем, формування поняття E-health, Створення ситуаційного диспетчерського центру розумної лікарні з використанням новітніх телекомунікаційних інструментів в умовах урбаністики: методи IP-телефонії, розпізнавання мови та Big Data, Види атак на IP-АТС Asterisk та методи протистояння їм, Охорона праці, Охорона навколишнього середовища.
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: Концептуальна архітектура інформаційно-аналітичної системи Е-медицина, Схема налаштування моніторингу, Схема роботи Corezoid.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	07.09.2022-19.09.2022	Виконано
2	Вступ	23.09.2022-25.09.2022	Виконано
3	Залучення інструментів інформаційно-аналітичних систем, формування поняття E-health	30.09.2022-12.10.2022	Виконано
4	Створення ситуаційного диспетчерського центру розумної лікарні з використанням новітніх телекомунікаційних інструментів в умовах урбаністики: методи IP-телефонії, розпізнавання мови та Big Data	14.10.2022-22.10.2022	Виконано
5	Види атак на IP-АТС Asterisk та методи протистояння їм	23.10.2022-04.11.2022	Виконано
6	Охорона праці	05.11.2022-08.11.2022	Виконано
7	Охорона навколишнього середовища	05.11.2022-08.11.2022	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	08.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Віктор ГНАТЮК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Аліна АНДРЕЄВА
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Методи інформаційно-комунікаційного забезпечення системи "Smart hospital"» містить 77 сторінок, 35 рисунків, 3 таблиці, 17 використаних джерел.

IP-ТЕЛЕФОНІЯ, ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА, E-HEALTH, СИТУАЦІЙНИЙ ЦЕНТР.

Об’єкт дослідження – бізнес-процеси лікарні та команди розробки та технічної підтримки за умови штатних та екстрених ситуацій.

Предмет дослідження – інформаційно-аналітична система для обліку залишків препаратів у закладах охорони здоров’я, ситуаційний центр лікарні та об’єкти, що можуть перебувати під його контролем, інструменти комунікації між користувачами інформаційно-аналітичної системи та розробниками, телекомунікаційні системи, що мають вплив на інфраструктурні об'єкти міста.

Мета кваліфікаційної роботи – дослідження варіантів покращення та впровадження інформаційних систем на прикладі системи "Smart hospital".

Метод дослідження – теоретичні: аналіз, синтез, пояснення, опис, проєктування.

Матеріали кваліфікаційної роботи рекомендується використовувати при оптимізації процесу прийому звернень від пацієнтів, обліку наявності препаратів та їх обігу, обробки та збереження інформації про пацієнтів.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1. Залучення інструментів інформаційно-аналітичних систем, формування поняття E-health 11
1.1. Інформаційно-аналітична система E-health. Модуль «Фронтенд. Внутрішні користувачі» 12
1.2. Інформаційно-аналітична система E-health. Модуль «Фронтенд. Зовнішні користувачі» 15
1.3. Інформаційно-аналітична система E-health. Модуль «Інфраструктура» 16
1.3.1. Моніторинг та управління доступністю 16
1.3.2. Збір контенту 17
1.4. Інформаційно-аналітична система E-health. Модуль «Бекенд» 20
РОЗДІЛ 2. Створення ситуаційного диспетчерського центру розумної лікарні з використанням новітніх телекомунікаційних інструментів в умовах урбаністики: методи IP-телефонії, розпізнавання мови та Big Data 23
2.1. IP-телефонії та методи її підключення і використання 24
2.2. Методи розпізнавання мови 30
2.2.1. Приховані марковські моделі 30
2.2.2. Розпізнавання мовлення на основі динамічного викривлення часу (DTW) 32
2.2.3. Нейронні мережі 33
2.2.4. Глибокі прямі та рекурентні нейронні мережі 33
2.2.5. Наскрізне автоматичне розпізнавання мовлення 34
2.3. Методи аналізу Big Data 36
РОЗДІЛ 3. Види атак на IP-АТС Asterisk та методи протистояння їм 39
3.1. Будова мережі IP-телефонії на базі IP-АТС Asterisk 39
3.2. Аналіз видів можливих атак на сервер Asterisk 42
3.2.1. Перепродаж трафіку (Tollfroud) 42

3.2.2. DDoS-атаки 44
3.3. Багаторівневий захист IP-АТС Asterisk 46
РОЗДІЛ 4. Охорона праці 50
4.1. Вступ 50
4.2. Аналіз умов праці на робочому місці інженера голосових платформ (VoIP інженера) 51
4.2.1. Організація робочого місця інженера голосових платформ 51
4.2.2. Перелік шкідливих та небезпечних виробничих чинників. 53
4.2.3. Розробка заходів з охорони праці 53
4.2.3.1. Мікроклімат робочого місця 54
4.2.3.2. Виробничий шум, ультразвук, інфразвук 54
4.2.3.3. Вібрації 55
4.3. Розробка заходів з охорони праці 56
4.4. Пожежна безпека виробничого приміщення 57
4.5. Розробка інструкції з охорони праці для інженера голосових платформ (VoIP інженера) 60
РОЗДІЛ 5. Охорона навколишнього середовища 66
5.1. Дата-центри та викиди парникових газів 66
5.2. П'ять категорій показників, що використовуються для встановлення цілей . 67
5.3. Рекомендовані показники для звітності щодо сталого розвитку 70
5.4. Вибір правильних шаблонів та стандартів для посібника 71
ВИСНОВКИ 75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 76

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IP (англ. Internet Protocol) – протокол мережевого рівня.

API (англ. Application Programming Interface) – інтерфейс програмування додатків.

DDoS (англ. Distributed Denial of Service) – відмова в обслуговуванні.

FXS (англ. Foreign Exchange Station) – голосовий інтерфейс або порт, що емулює розширення інтерфейсу АТС.

HTTP (англ. HyperText Transfer Protocol) – протокол прикладного рівня.

Hz (герц) – одиниця вимірювання частоти.

ICMP (англ. Internet Control Message Protocol) – міжмережевий протокол керуючих повідомлень.

MFCC (Mel-frequency cepstral coefficients) – Mel-частотні кепстральні коефіцієнти.

SIP (англ. Session Initiation Protocol) – протокол передачі даних.

SQL (англ. Structured Query Language) – мова структурованих запитів.

UCE (англ. Universal Computing Element) – універсальний обчислювальний елемент.

VPN (англ. Virtual Private Network) – віртуальна приватна мережа.

АТС (автоматична телефонна станція) – телефонна станція, що забезпечує автоматичне з'єднання абонентів телефонної мережі.

США (Сполучені Штати Америки) – республіка в Північній Америці.

ВСТУП

Актуальність теми. Роботизація медичних приладів, сучасна медицина та діагностика захворювань надають змогу виконувати ефективне та якісне втручання в організм людини, з високою ймовірністю не завдати ускладнень при лікуванні або плановому обстеженні та врятувати життя у критичних випадках.

Але автоматизація лікарень приватного та державного сектору вимагає радикальніших змін у багатьох напрямках:

- Неефективність складського обліку препаратів. У це поняття входить відсутність управління ресурсом: безліч швидкопсувних препаратів можуть лежати не задіяними в одному закладі охорони здоров'я і закуповуватися через брак для іншої лікарні. Це відбувається через те, що в обліковій системі не визначаються ліки необхідні на закупівлю, їх закуповують загальною стандартною кількістю, що призводить до додаткових витрат державних коштів.
- Затримка при наданні невідкладної медичної допомоги збільшує витрати коштів, які потрібні на відновлення здоров'я пацієнта. При несвоєчасному наданні допомоги витрати на відновлення можуть виявитися в рази більше. Так затримка в транспортуванні автомобілем швидкої медичної допомоги або несвоєчасне визначення діагнозу можуть призвести не тільки до погіршення стану пацієнта, але й спричинити додаткові витрати на препарати, лікування, утримання в палаті або покриття страхових виплат у разі летального випадку.

Мета і завдання дослідження.

Мета дипломної роботи – дослідження варіантів покращення та впровадження інформаційних систем на прикладі системи "Smart hospital".

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Дослідження залучення інструментів інформаційно-аналітичних систем, формування поняття E-health.

2. Створення ситуаційного диспетчерського центру розумної лікарні з використанням новітніх телекомунікаційних інструментів в умовах урбаністики: IP-телефонія та розпізнавання мови, Big Data, алгоритм “Зеленої хвилі”, віртуальна реальність.

3. Дослідження видів атак на інформаційні системи та методів протистояння їм на прикладі IP-телефонії на платформі Asterisk.

Об’єкт дослідження – бізнес-процеси лікарні та команди розробки та технічної підтримки за умови штатних та екстрених ситуацій.

Предметом дослідження – інформаційно-аналітична система для обліку залишків препаратів у закладах охорони здоров’я, ситуаційний центр лікарні та об’єкти, що можуть перебувати під його контролем, інструменти комунікації між користувачами інформаційно-аналітичної системи та розробниками, телекомунікаційні системи, що мають вплив на інфраструктурні об'єкти міста.

Методи досліджень. В роботі використовували теоретичні методи досліджень: аналіз, синтез, пояснення, опис, проєктування.

Наукова новизна отриманих результатів.

Спроєктовано і удосконалено процес ведення обліку використання препаратів по закладам охорони здоров’я, процес прийому і обробки звернень пацієнтів до екстреної медичної служби.

Практичне значення отриманих результатів.

Матеріали роботи рекомендується використовувати для оптимізації процесу прийому звернень від пацієнтів, обробки та збереження інформації про пацієнтів, наявність препаратів та їх обіг.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
ЗАЛУЧЕННЯ ІНСТРУМЕНТІВ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ, ФОРМУВАННЯ ПОНЯТТЯ E-HEALTH

Перш за все, концепція розумної лікарні несе у собі мету залучення та створення телекомунікаційних інструментів, їх впровадження у бізнес-процеси користувачів та працівників для:

- оперативного вирішення екстрених ситуацій з підвищеною ймовірністю порятунку життя пацієнтів внаслідок оптимізації та автоматизації процесів, внаслідок залучення новітніх технологій з коригуванням за позитивним досвідом користувача;
- економії ресурсу (економічна складова лікарні, час обробки запитів від пацієнтів).

На даному етапі розвитку напрямку E-health є декілька інформаційно-аналітичних систем, в які заклади охорони здоров'я самостійно вносять дані по використанню наявних в закладі препаратів, але немає уніфікованої платформи для збору та обробки даної інформації.

Інформаційно-аналітичні системи – це системи збору та опрацювання інформації, які дозволяють виконувати ряд важливих функцій:

- збір даних та вивід даних у аналітичні дешборди;
- напівавтоматизоване введення даних при фіксуванні звернень;
- реалізація координаційних додатків, що дозволяють розміщувати у собі оперативну різнорідну медіа інформацію у режимі історичних даних, аналітики, онлайн-даних тощо [17].

E-health – це електронна система збору інформації з державних та приватних реєстрів, що дозволить консолідувати, обробляти та аналізувати у собі необхідну інформацію про об'єкти та суб'єкти, що напряму або дотично відносяться до бізнес-процесів закладів охорони здоров'я [17].

На рис. 1.1 зображено концептуальну архітектуру пропонованої інформаційно-аналітичної системи E-health [17]:

Рис. 1.1. Концептуальна архітектура інформаційно-аналітичної системи E-health

Таким чином система дозволить:

- проводити облік та аудит препаратів та матеріалів, їх кількість та термін придатності в єдиній системі, не розмежовуючи бухгалтерський та складський облік;
- координаторам збирати інформацію, яка необхідна для прийняття рішення про державні закупівлі необхідних матеріалів, спираючись на аналітичні дані та розрахунки в системі;
- мати єдине вікно координатора, що консолідуватиме у собі контент, дозволить приймати доречні рішення у позаштатних та екстрених ситуаціях;
- виконувати ефективні та оперативні маніпуляції з пацієнтами на виїзді оперативної бригади завдяки медичним карткам онлайн, так як буде відома історія хвороби [17].

1.1. Інформаційно-аналітична система E-health. Модуль «Фронтенд. Внутрішні користувачі»

Інформаційно-аналітична система буде мати користувачів 2 типів: внутрішні і зовнішні. Внутрішні користувачі – це відповідальні особи за внесення даних в систему від кожного закладу, регіональні координатори та постачальники.

Кабінет відповідальної особи по закладу буде містити в собі:

- функціонал звітності по використанню наявних препаратів;
- функціонал внесення перерозподілів на інші заклади охорони здоров'я;
- функціонал внесення надходжень, які були отримані як благодійна або гуманітарна допомога або які були закуплені за кошти місцевого бюджету.

Функціонал звітності по використанню наявних препаратів має відображати позиції, які вносить в систему надавач препаратів (постачальник, заклад, який зробив перерозподіл, або заклад, який закупив позиції за кошти місцевого бюджету) з формою для заповнення даних по використанню або розливу/пошкодженню препаратів, яка стає активною для заповнення двічі на місяць.

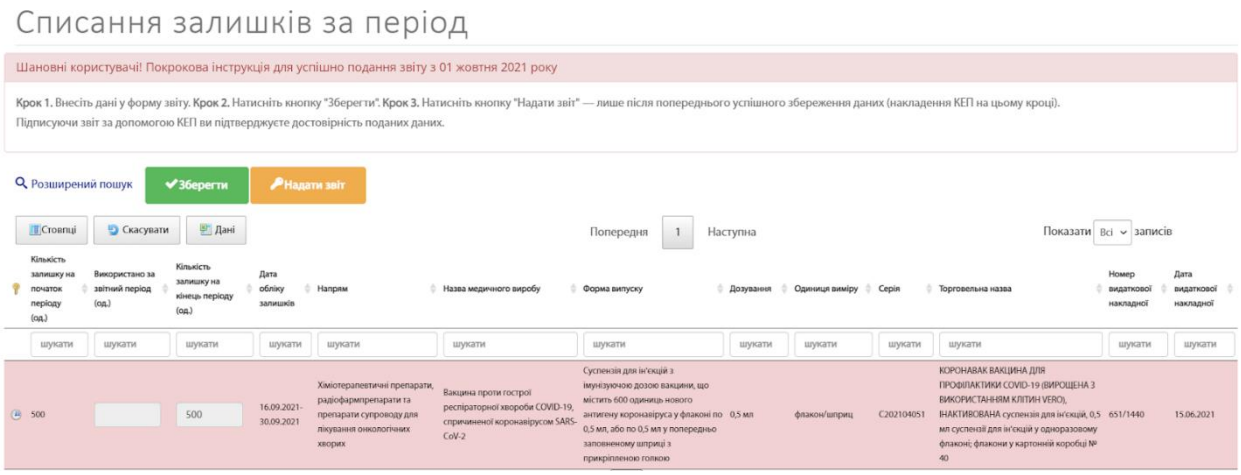

Рис. 1.2. Функціонал звітності по використанню наявних препаратів

Функціонал внесення перерозподілів на інші заклади охорони здоров'я має містити в собі перелік наявних позицій у закладі охорони здоров'я із можливістю перемістити певну кількість препарату в інший заклад.

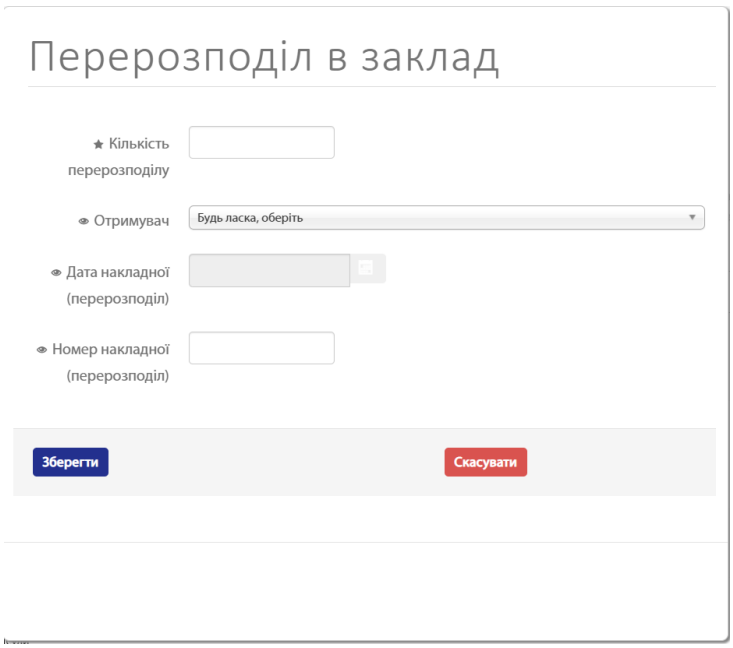

Рис. 1.3. Функціонал внесення перерозподілу

Функціонал внесення надходжень, які були отримані як благодійна або гуманітарна допомога або які були закуплені за кошти місцевого бюджету, повинен давати можливість додати до звіту позиції, які були отримані не за кошти державного бюджету.

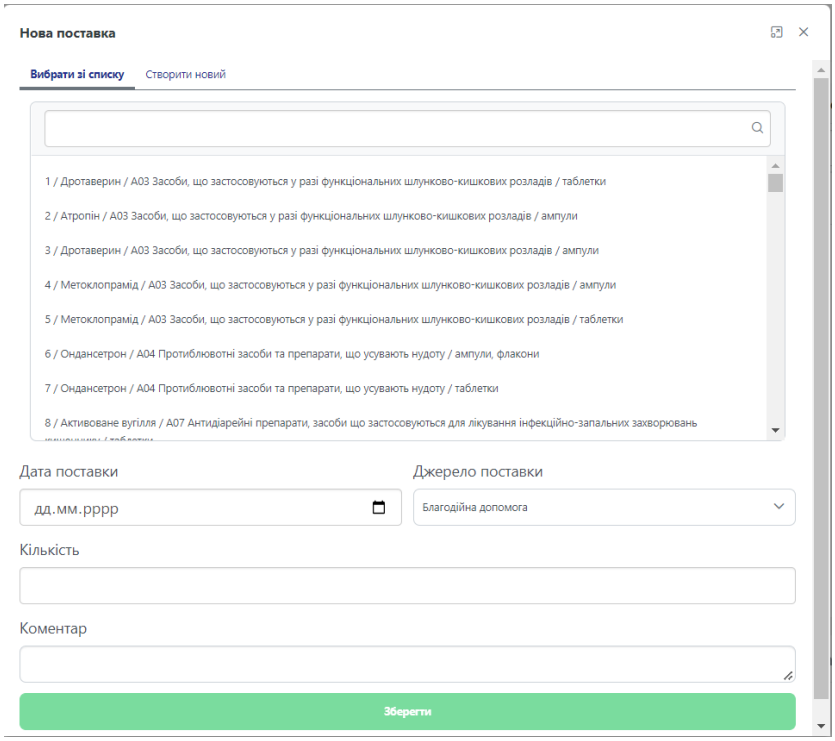

Рис. 1.4. Функціонал внесення надходжень

Кабінет регіонального координатора має вміщувати в собі графік поставок в регіони, статус подачі звітності закладами регіону, дані по відповідальним особам кожного з закладу регіону.

У кабінеті постачальника буде можливість приймати участь у торгах (по аналогії з проведенням аукціонів на платформі Prozorro), можливість завантаження необхідних документів після виграшу і внесення поставок по регіонам і/або закладам.

1.2. Інформаційно-аналітична система E-health. Модуль «Фронтенд. Зовнішні користувачі»

Деяка інформація, яку вводять заклади охорони здоров'я в інформаційно-аналітичну систему, яка не має лікарської таємниці, може бути виведена на загальний огляд. Наприклад, дані про надходження та залишки препаратів по закладам охорони здоров'я можна виводити на окремому сайті, до якого буде доступ у всіх пацієнтів. Це допоможе прибрати корупційну складову і додасть прозорість щодо використання ліків закладами.

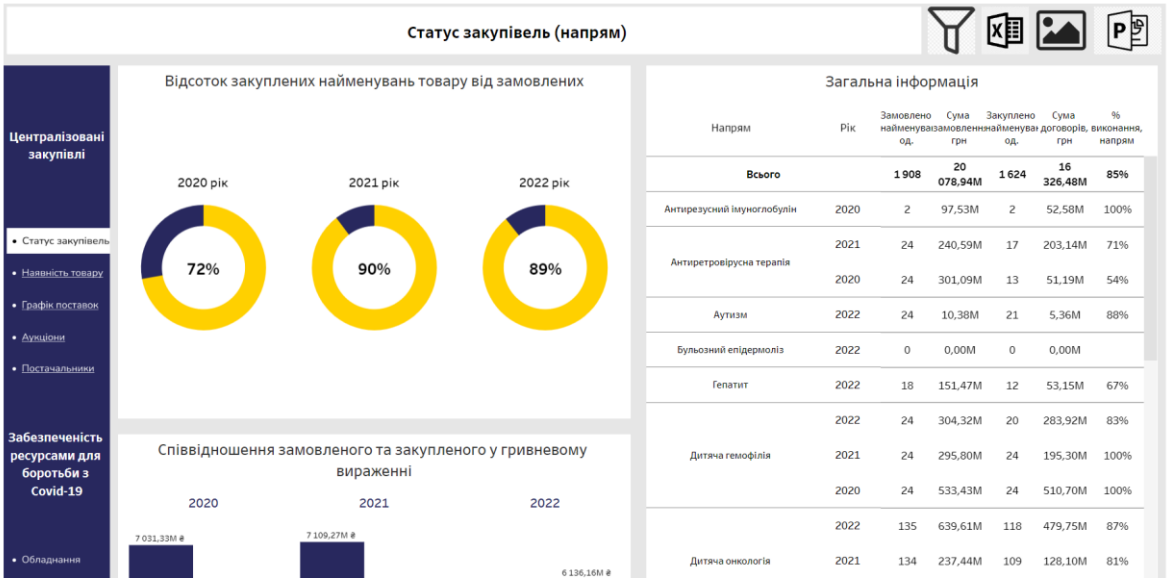

Рис. 1.5. Виведення інформації про надходження препаратів

1.3. Інформаційно-аналітична система E-health. Модуль «Інфраструктура»

Інфраструктура – це один із модулів системи, що дозволяє організувати та інтегрувати збір різнорідних медіа даних у систему та забезпечити захищений, безперебійний процес обробки та використання даних.

1.3.1. Моніторинг та управління доступністю

Моніторинг та управління доступністю пропонується до реалізації за допомогою системи Zabbix. Zabbix – це відкрита система моніторингу та відстеження статусів роботи мережного обладнання, комп'ютерної мережі та серверів.

Для збереження даних використовується база даних (MySQL, PostgreSQL, SQLite або Oracle Database) та веб-інтерфейс написаний на PHP (Hypertext Preprocessor – мова програмування). Система підтримує кілька видів моніторингу:

• Simple checks – перевіряє реакцію та доступність стандартних сервісів (наприклад, SMTP (англ. Simple Mail Transfer Protocol – мережевий протокол) або HTTP) без встановлення програмного забезпечення на хості, за яким ведеться спостереження.

• Zabbix agent – встановлюється на Unix-подібні або Windows-хости для отримання даних про використання дискового простору, мережі, навантаження процесора тощо.

• External check – виконання зовнішніх програм. Також підтримується моніторинг через SNMP (Simple Network Management Protocol – протокол управління) [17].

З погляду користувача система Zabbix ділиться на дві великі частини: сервер і агенти. Сервер розміщується на одній машині, яка збирає та зберігає статистичні дані, а агенти – на тих машинах, з яких збираються дані [1]:

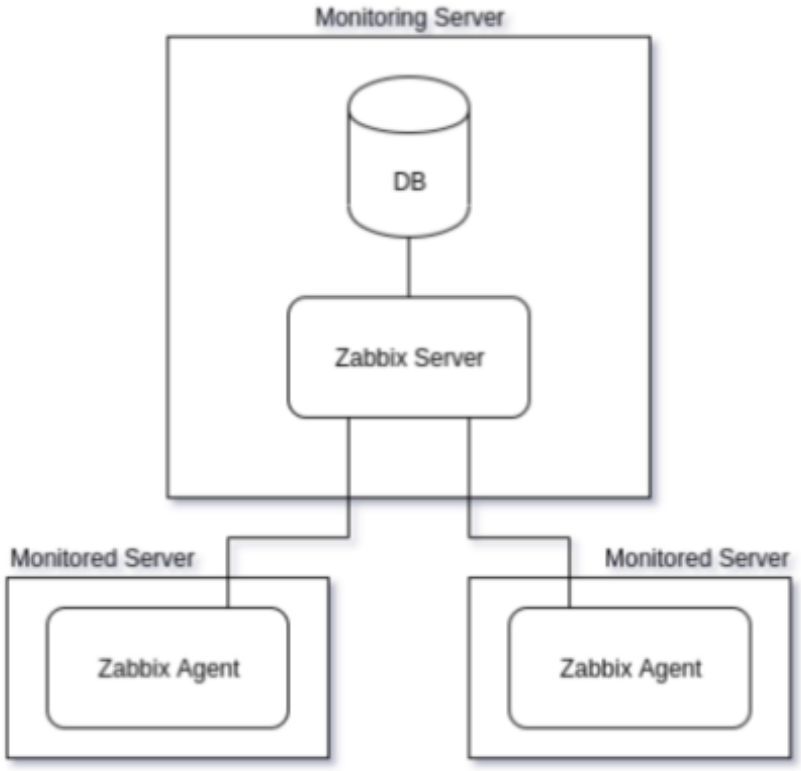

Рис. 1.6. Схема налаштування моніторингу

1.3.2. Збір контенту

Через відсутність єдиного стандарту передачі даних до інформаційних систем, при реалізації необхідно застосувати інструмент, який може приєднатися до будь-якої точки доступу, отримувати та координувати інформацію за допомогою різноманітних API (Application Programming Interface – програмний інтерфейс програми) (DB (англ. DataBase – база даних), JSON (англ. JavaScript Object Notation - текстовий формат обміну даними між комп'ютерами) тощо) [17].

Внаслідок виявлення проблематики до реалізації запропоновано інструмент інтелектуальної побудови бізнес-процесів – Corezoid.

Corezoid – це хмарна ОС (укр. операційна система) для створення IT-рішень (IT – інформаційні технології) з використанням методів автоматичного програмування з явним виділенням станів [17].

Corezoid допомагає реалізовувати та виконувати алгоритми та процеси, а також керувати програмним забезпеченням та технікою будь-якої складності.

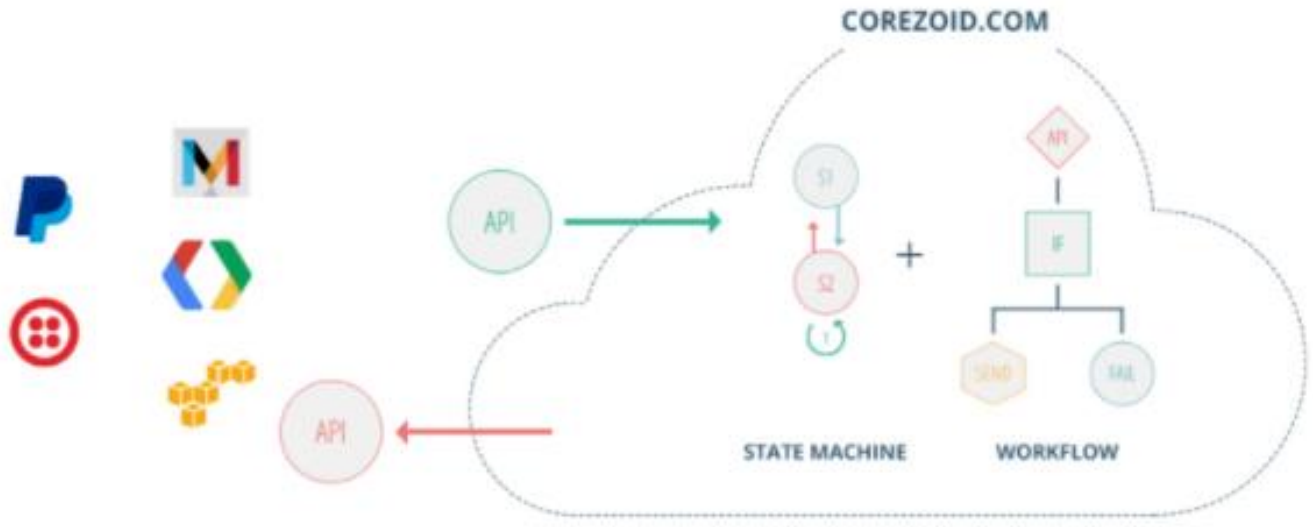

Рис. 1.7. Схема роботи Corezoid

Кожен процес Corezoid складається з вузлів. Кожен вузол має власну унікальну логіку. Заявки рухаються по процесу від одного вузла до іншого, дотримуючись заданої логіки (рис. 1.8).

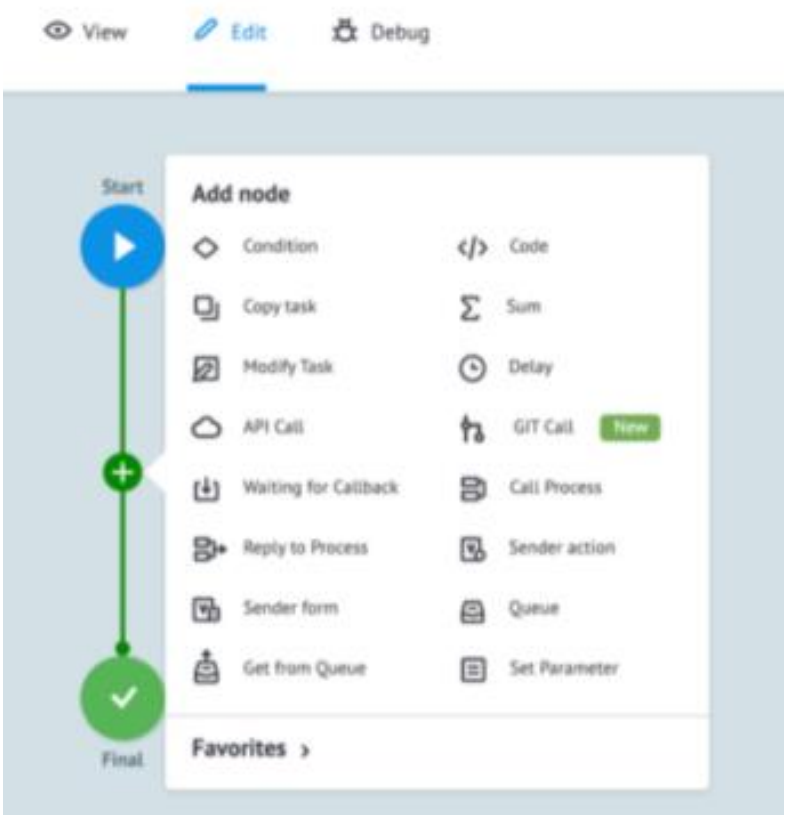

Рис. 1.8. Задання логіки процесу

Процес – це алгоритм або програма, що реалізується за допомогою послідовності, набору чи множини вузлів (рис. 1.9).

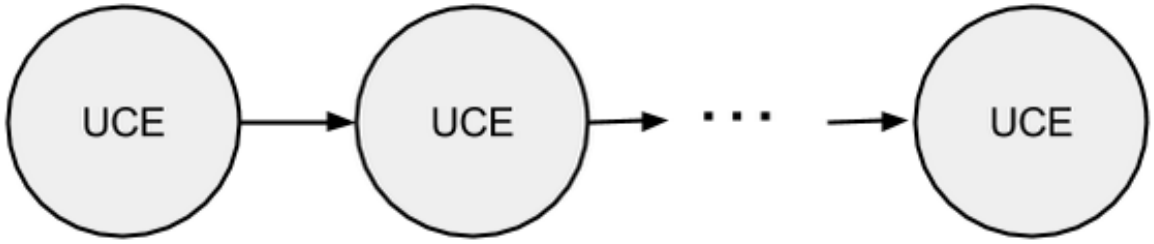

Рис. 1.9. Схема процесу

Вузол – це універсальний обчислювальний елемент, який описує стан об'єктів (рис. 1.10). Вузол має такі характеристики: логіка, функції, лічильники.

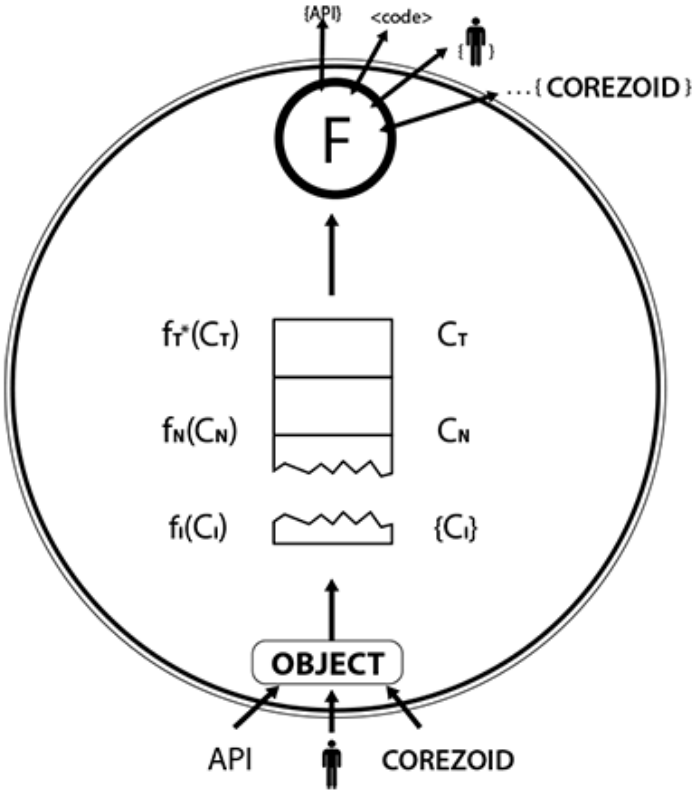

Рис. 1.10. Схема вузла

f – виклик відповідної функції;

F – кожному вузлу ставиться у відповідність функція, яка може бути реалізована через людину, API, код, інший вузол;

Ст – лічильник, час Т найстарішого об'єкта в черзі;

Сп – кількість об'єктів у черзі;

{Сі} – кастомні лічильники;

Черга – це черга з об'єктів у вузлі;

Об'єкт – набір параметрів, що характеризують об'єкт [17].

Відповідно до певних правил у вузлі проводиться обробка інформації про об'єкт, тобто застосовується функція об'єкта.

Функції – це дії, які потрібно виконати над об'єктом із черги у вузлі. Функції можуть бути як API, програмного коду, іншого процесу тощо.

Логіка – інструменти керування логікою у вузлі. Бувають системні та призначені для користувача.

Системна логіка Т – це заданий час, протягом якого може бути об'єкт у вузлі.

Системна логіка N – це задана кількість об'єктів, які можуть бути у черзі вузла.

Лічильники показують лише значення без будь-яких дій (у цьому на відміну від логіки). Також бувають системними та користувальницькими [2].

Таким чином, цей інструмент повністю забезпечує втілення концептуальної ідеї збирання та використання інформації в системі.

1.4. Інформаційно-аналітична система E-health. Модуль «Бекенд»

Програмне забезпечення інформаційно-аналітичної системи призначене для контролю та координації здійснення заходів щодо надання допомоги та інформації та розробки тривожних сигналів, що надходять до пункту централізованого спостереження. Також інформаційно-аналітична система забезпечує функціонування з цими можливостями:

• забезпечення моніторингу, прийому, реєстрації та обробки тривожних сигналів, що надходять до пункту централізованого спостереження в цілодобовому режимі;

• введення в базу даних, накопичення та надійне зберігання тривожних сигналів, що надходять до пункту централізованого спостереження;

• ідентифікація та пошук клієнтів, залежно від певних ознак, перегляду поточного стану у медичній картці;

• перегляд статистичної інформації про ресурси закладу та підказки щодо обсягів та типів позицій для закупівлі.

Загальний високорівневий процес реагування на звернення:

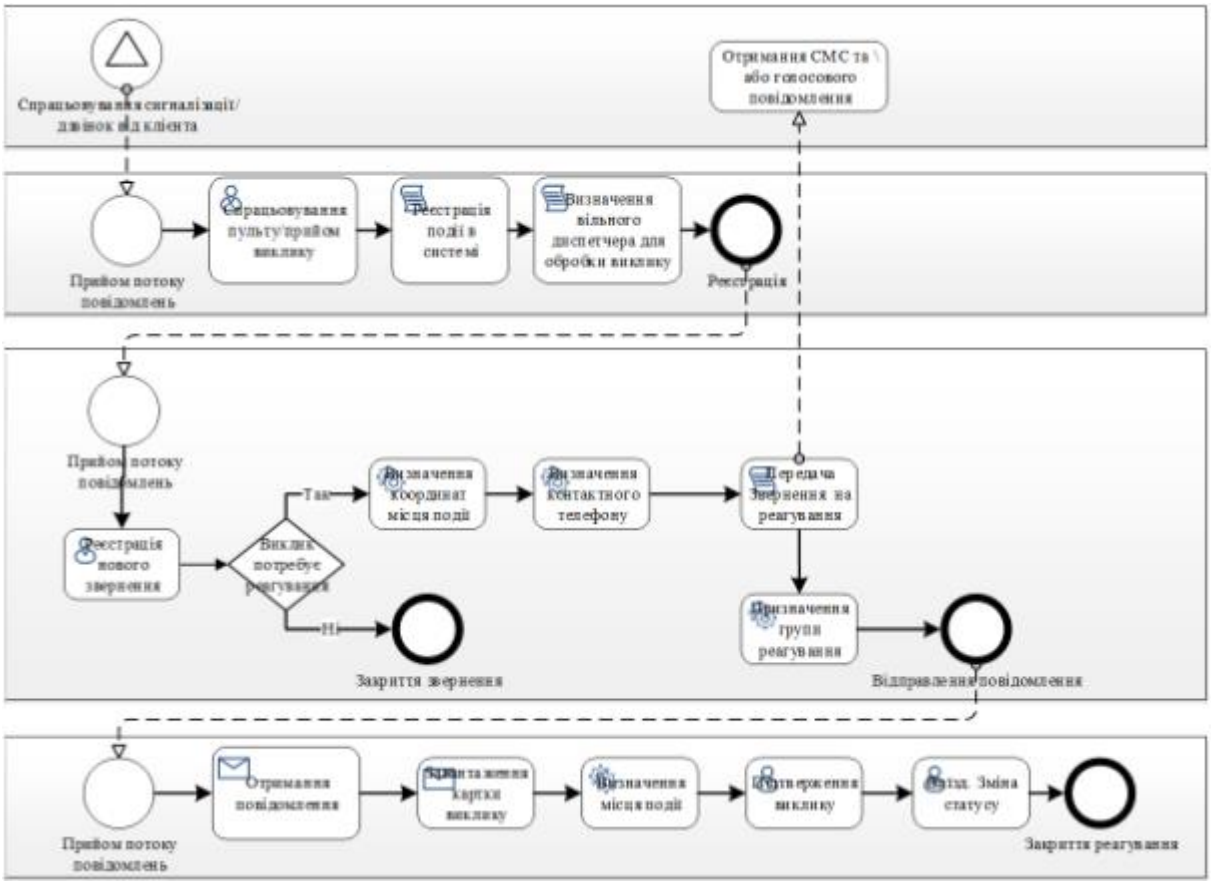

Рис. 1.11. Загальний процес реагування на звернення

Використання електронної взаємодії дозволяє підтримувати довідники об'єктів у актуальному стані. Крім того, всі нові об'єкти реєструються та ведуться з прив'язкою до об'єктів, оцифрованих та провідних у системі управління у реєстрах інших лікарень та державних підприємств.

Вся інформація зберігається у базі даних. Загальна схема бази даних для розділу залишків препаратів по закладах охорони здоров'я може виглядати так:

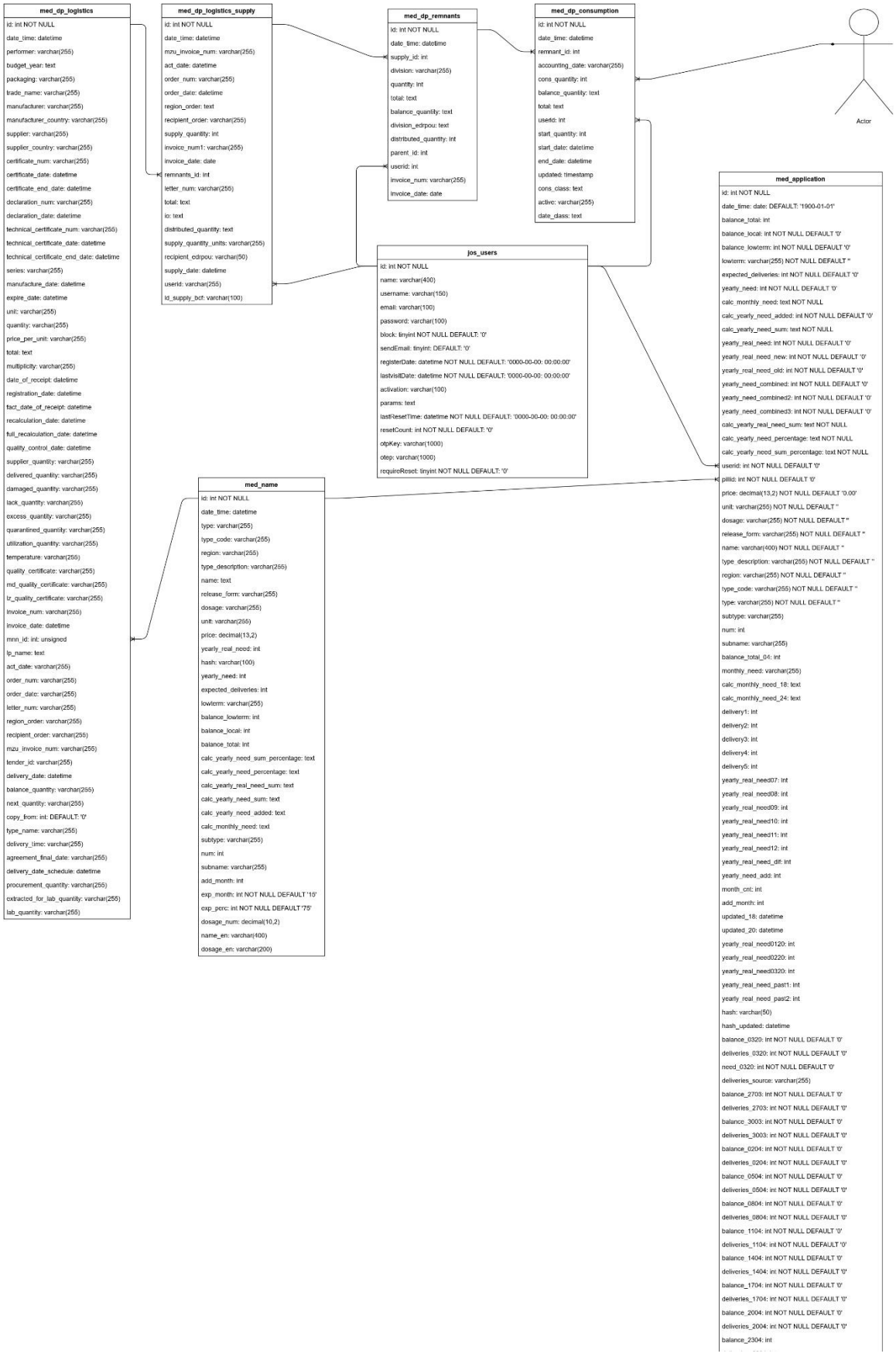

Рис. 1.12. Схема бази даних з даними про залишки препаратів

РОЗДІЛ 2
СТВОРЕННЯ СИТУАЦІЙНОГО ДИСПЕТЧЕРСЬКОГО ЦЕНТРУ РОЗУМНОЇ ЛІКАРНІ З ВИКОРИСТАННЯМ НОВІТНІХ ТЕЛЕКОМУНІКАЦІЙНИХ ІНСТРУМЕНТІВ В УМОВАХ УРБАНІСТИКИ: МЕТОДИ IP-ТЕЛЕФОНІЇ, РОЗПІЗНАВАННЯ МОВИ ТА BIG DATA

Ситуаційний диспетчерський центр відіграє одну з найважливіших ролей у концептуальній системі Smart hospital. Програмно-апаратний комплекс дозволяє побудувати систему, що допоможе приймати ефективні і оперативні рішення у позаштатних та екстренних ситуаціях.

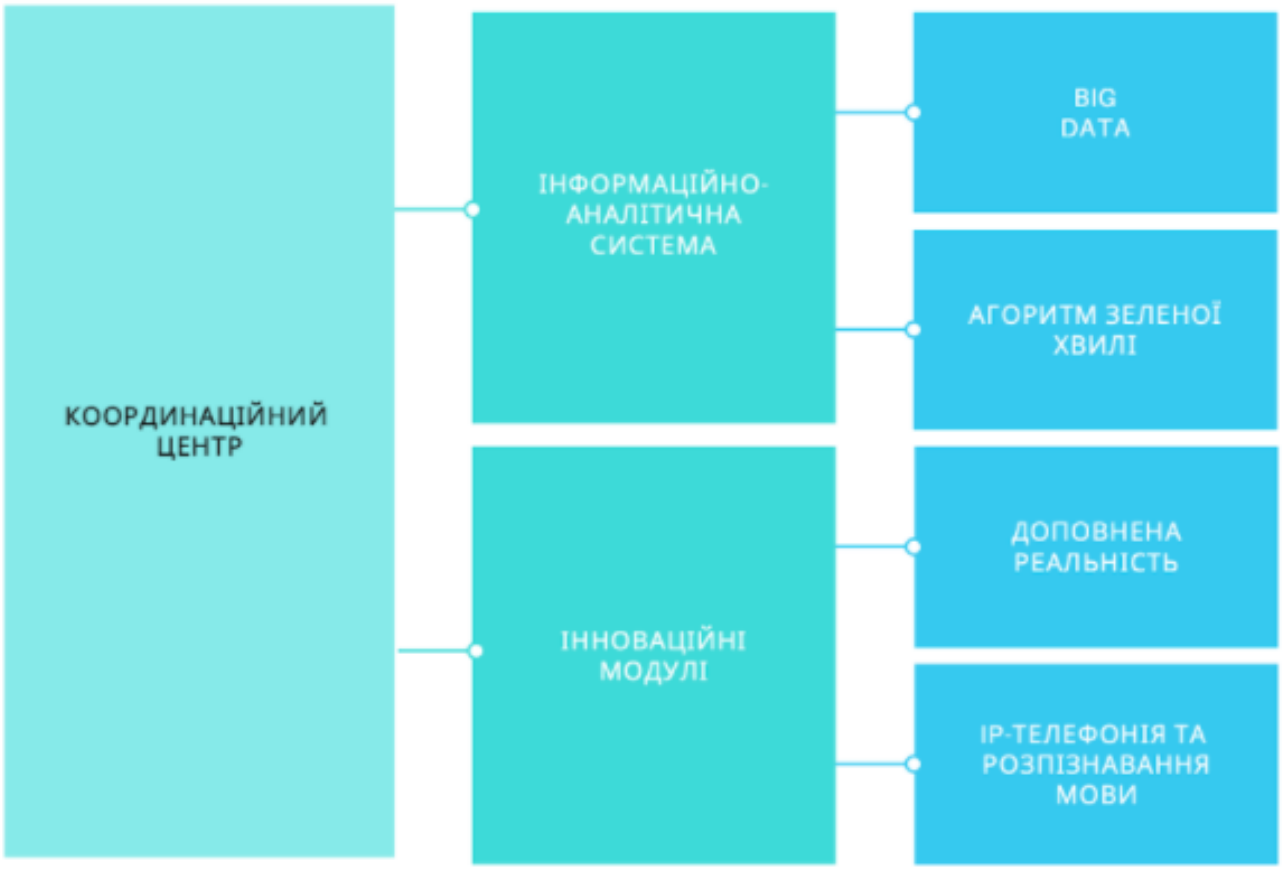

Рис. 2.1. Загальна схема ситуаційного центру

2.1. IP-телефонія та методи її підключення і використання

IP-телефонія є важливим інструментом для роботи не лише ситуаційного диспетчерського центру, але й для підтримки та організації роботи інформаційно-аналітичної системи. Будь-яка система може мати свої недоліки і вразливі місця, тому необхідно мати можливість підтримувати комунікацію між розробниками ІАС і її користувачами. Найоптимальніший варіант для реалізації даного бізнес-процесу – залучення IP-телефонії.

Налаштування IP-телефонії може бути впроваджено двома методами, які залежать від місцерозташування серверів.

1) InHouse-рішення: система телефонії може бути реалізована на серверах, які фізично розташовані в одній локальній мережі з операторами. Даний метод налаштування має ряд недоліків. У такому випадку необхідно мати спеціалізоване приміщення, в якому будуть дотриманні всі умови для безперебійної роботи серверу (температура, вологість, наявність безперебійних джерел живлення, резервного каналу Інтернету); проводити регулярне обслуговування обладнання.

2) SaaS-рішення (хмарне рішення): розташування системи телефонії на хмарних потужностях в дата-центрі. Даний метод має більше переваг, ніж недоліків, тому він користується попитом у користувачів. За щомісячну плату користувач отримує весь функціонал фізичного сервера, але без необхідності його фізичного розташування та обслуговування.

Підключення до постачальника послуг VoIP також можна реалізувати кількома методами:

- Спеціальні телефони VoIP підключаються безпосередньо до IP-мережі за допомогою таких технологій, як дротовий Ethernet або Wi-Fi. Зазвичай вони розроблені в стилі традиційних цифрових бізнес-телефонів;

- Аналоговий телефонний адаптер підключається до мережі та реалізує електроніку та вбудоване програмне забезпечення для роботи звичайного аналогового телефону, підключеного через модульний телефонний гніздо. Деякі домашні Інтернет-шлюзи та кабельні модеми мають цю функцію;

- Програмне забезпечення Softphone, встановлене на мережевому комп'ютері, обладнаному мікрофоном і динаміком, або гарнітурою. Програма зазвичай надає користувачеві панель набору номера та поле відображення для керування програмою за допомогою клацань миші або введення з клавіатури.

Для підтримання зв'язку між користувачем і розробником додається до бізнес-процесу команда технічної підтримки, яка буде обробляти типові звернення, допомагати користувачам працювати в IAC і фіксувати побажання та рекомендації для подальшого покращення роботи системи. Тримати зв'язок з клієнтом зручно в голосових і текстових каналах зв'язку. Прикладом текстового каналу зв'язку є пошта і чат-бот, в якому фіксуються звернення користувачів і створюються задачі на представників команди в залежності від типу і теми звернення.

Голосовий формат зв'язку буде зручним лише у випадку, якщо це реалізовано централізовано, без залучення особистих номерів технічних спеціалістів. Для створення єдиної голосової точки входу звернень від користувачів впроваджується IP-телефонія.

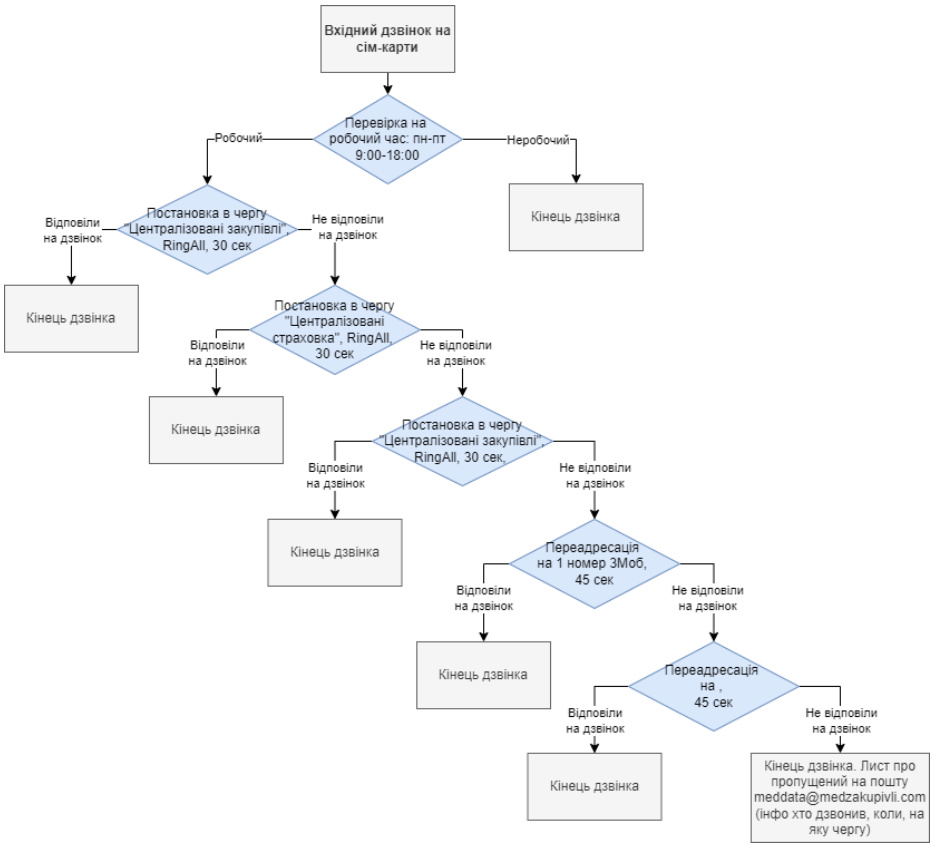

Рис. 2.2. Приклад схеми, за якою реалізується маршрутизація відділу підтримки

Приклад діалплану для реалізації подібної схеми маршрутизації, написаний на відкритій платформі Asterisk:

```
vi /etc/asterisk/extensions.conf
```

```
exten => 333,1,Answer()
exten => 333,2,Background(basic-pbx-ivr-main)
exten => 333,3,WaitExten(5)
exten => 1,1,Goto(managers,s,1)
exten => 2,1,Goto(support,s,1)

[managers]
exten => s,1,Ringing
 same => n,Wait(1)
 same => n,Background(/var/lib/asterisk/sounds/wav/managers)
 same => n,Waitexten(5)
exten => 1,1,Dial(SIP/201)
exten => 2,1,Dial(SIP/202)
exten => 0,1,Goto(outcaling,333,1)

[support]
exten => s,1,Ringing
 same => n,Wait(1)
 same => n,Background(/var/lib/asterisk/sounds/wav/support)
 same => n,Waitexten(5)
exten => 1,1,Dial(SIP/101)
exten => 2,1,Dial(SIP/102)
exten => 0,1,Goto(outcaling,333,1)
```

Рис. 2.3. Діалплан для вхідних дзвінків

Для нагадування користувачам про початок і кінець терміну подачі звітності інформації до системи можна використовувати функціонал IP-телефонії, замість вихідного обдзвону технічної підтримки. Для цього необхідного реалізувати наступну схему:

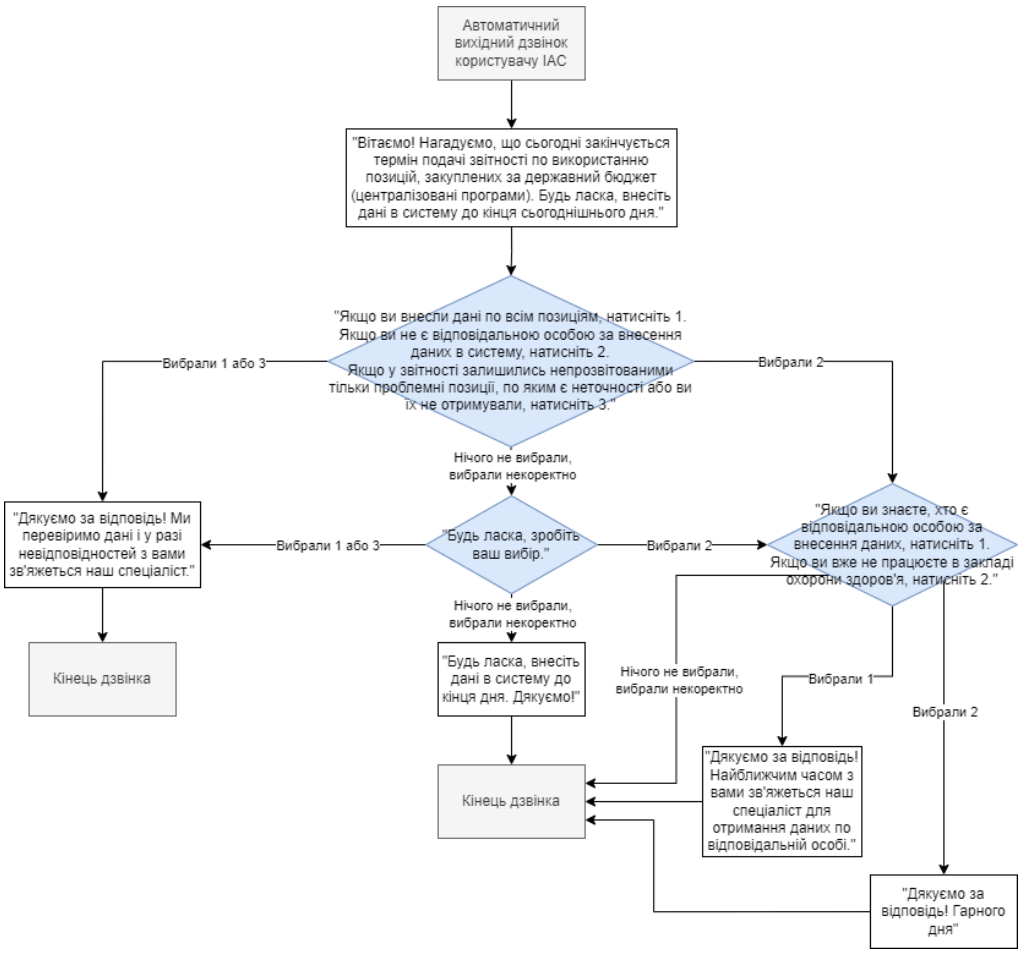

Рис. 2.4. Схема для налаштування автообдзвону

Реалізується функціонал автообдзвону за допомогою відкритої платформи Asterisk і наступного діалплану і скрипта:

```
[outboundmsg1]
exten => s,1,Wait(2)
exten => s,n,Playback(/var/lib/asterisk/sounds/custom/you_call_your_friends_are_collectors)
exten => s,n,Hangup
```

Рис. 2.5. Діалплан

```
#!/bin/sh

while read number; do

cat <<EOF  >  /var/spool/asterisk/$number

Channel: SIP/voip_trunk/$number
Callerid: $number
MaxRetries: 200
RetryTime: 20
WaitTime: 30
Context: outboundmsg1
Extension: s
Priority: 1

EOF

    chown asterisk:asterisk /var/spool/asterisk/$number
    mv /var/spool/asterisk/$number  /var/spool/asterisk/outgoing

    echo "$number"

    number=`expr $number + 1`

    while [ "$?" -eq "0" ]

    do
count_files ()
```

Рис. 2.6. Баш-скрипт

```
{

    count_f=`ls /var/spool/asterisk/outgoing | wc -l`

        if [ "$count_f" -eq "30" ]; then

            sleep 10

            return 0

        else

            return 1

        fi

}

    count_files

    done

done < /var/spool/asterisk/list.txt

exit 0
```

Рис. 2.7. Баш-скрипт (продовження)

Використання IP-телефонії у контактних центрах наразі є традиційним способом отримання якісних телекомунікаційних послуг. Також телефонія відіграє важливу роль у залученні інтелектуальних систем, таких як розпізнавання та аналіз мови [17].

Приклад налаштування маршрутизації на платформі Asterisk:

```
exten => _X.,1,NoOp(${CALLERID(all)})
same =>n,Gotoif($["${EXTEN:0:5}"="77777"]?test,${EXTEN},1)
same =>n,NoOp(${CHANNEL})
same =>n,NoOp(${AVALIABLEALISA})
same => n,ExecIf($["${AVALIABLEALISA}"="FALSE"]?SoftHangup(${CHANNEL}))
;same =>n,GotoIf($["${EXTEN}"="0966109242"]?TestSoftHangup,${EXTEN},1)
;same =>n,SoftHangup(${CHANNEL})
same =>n,Answer()
;same =>n,GotoIf($["${EXTEN}"="0966109242"]?TestSoftHangup,${EXTEN},1)
same =>n,Playback(helloalica)
same =>n,Playback(beep)
same =>n,Macro(mix-recorder);OPTIMA-2292
same =>n,Noop(${STRFTIME(${EPOCH},,%H:%M:%S %d-%m-%Y)})
same =>n,Set(date=${STRFTIME(${EPOCH},,%H:%M:%S %d-%m-%Y)})
same =>n,NoOp(${UNIQUEID})
same =>n(start),Noop()
same =>n,MRCPRecog("/var/lib/asterisk/agi-bin/city.xml",t=5000)
same =>n,StopMixMonitor();OPTIMA-2292
same =>n,Set(attempt=1)
same =>n,NoOp(${result} // ${RECOG_RESULT})
same =>n,AGI(/usr/local/sbin/parse.sh,${RECOG_RESULT})
same =>n,NooP(${city})
same =>n,Set(CALLERID(num)=${EXTEN})
same =>n,Noop(${CALLERID(num)} ${CALLERID(name)})
same =>n,Set(CHANNEL(language)=ua)
same =>n,ExecIf($["${city}"="BUSY"]?Agi(/usr/local/sbin/insert_table_new.sh,${CALLERID(num)},${date},${UNIQUEID},$
{city},${attempt}))
same =>n,GotoIf($["${city}"="BUSY"]?secretar)
```

Рис. 2.8. Приклад діалплану

```
same =>n,ExecIf($["${city}"="OTHER"]?Playback(povtoralica))
same =>n,ExecIf($["${city}"="OTHER"]?Playback(beep))
same =>n,ExecIf($["${city}"="OTHER"]?Macro(mix-recorder);OPTIMA-2292
same =>n,ExecIf($["${city}"="OTHER"]?MRCPRecog("/var/lib/asterisk/agi-bin/city.xml",t=5000))
same =>n,StopMixMonitor();OPTIMA-2292
same =>n,ExecIf($["${city}"="OTHER"]?Set(attempt=2))
same =>n,NoOp(${result} // ${RECOG_RESULT})
same =>n,ExecIf($["${city}"="OTHER"]?AGI(/usr/local/sbin/parse.sh,${RECOG_RESULT}))
same =>n,GotoIf($["${city}"=""]?secretar)
;same =>n,StopMixMonitor();test2292
same =>n,Playback(${city})
same =>n,ExecIf($["${city}" = "OTHER"]?Wait(1))
same =>n,Agi(/usr/local/sbin/insert_table_new.sh,${CALLERID(num)},${date},${UNIQUEID},${city},${attempt})
same =>n,ExecIf($["${city}"="KYIV"]?Dial(SIP/kievDC-kievmrcp/501-579))
same =>n,ExecIf($["${city}"="LVIV"]?Dial(SIP/kievDC-kievmrcp/502-579))
same =>n,ExecIf($["${city}"="ZAPORIZHZHIA"]?Dial(SIP/kievDC-kievmrcp/503-579))
same =>n,ExecIf($["${city}"="KHERSON"]?Dial(SIP/kievDC-kievmrcp/520-579))
same =>n,ExecIf($["${city}"="DNIPRO"]?Dial(SIP/kievDC-kievmrcp/505-579))
same =>n,ExecIf($["${city}"="KAMIANSKE"]?Dial(SIP/kievDC-kievmrcp/517-579))
same =>n,ExecIf($["${city}"="RIVNE"]?Dial(SIP/kievDC-kievmrcp/509-579))
same =>n,ExecIf($["${city}"="DUBNO"]?Dial(SIP/kievDC-kievmrcp/525-579))
```

Рис. 2.9. Приклад діалплану

```
same =>n,ExecIf($["${city}"="OTHER"]?Noop(Otherbroken))
same =>n,ExecIf($["${city}"="OTHER"]?Dial(SIP/kievDC-kievmrcp/579579-${CALLERID(num)}))
same =>n(secretar),Dial(SIP/kievDC-kievmrcp/579579-${CALLERID(num)})
same =>n,Hangup()
```

Рис. 2.10. Приклад діалплану

2.2. Методи розпізнавання мови

Як акустичне моделювання, так і моделювання мови є важливими частинами сучасних статистичних алгоритмів розпізнавання мовлення. Приховані марковські моделі (HMM) широко використовуються в багатьох системах. Мовне моделювання також використовується в багатьох інших програмах обробки природної мови, таких як класифікація документів або статистичний машинний переклад.

2.2.1. Приховані марковські моделі

Сучасні системи розпізнавання мови загального призначення базуються на прихованих моделях Маркова. Це статистичні моделі, які виводять послідовність символів або величин. HMM використовуються для розпізнавання мовлення, тому що мовний сигнал можна розглядати як частково стаціонарний сигнал або короткочасний стаціонарний сигнал. У короткому часовому масштабі (наприклад, 10 мілісекунд) мова може бути апроксимована як стаціонарний процес. Мовлення можна розглядати як марковську модель для багатьох стохастичних цілей.

Інша причина популярності HMM полягає в тому, що їх можна навчити автоматично, а також вони прості та зручні для використання. У розпізнаванні мовлення прихована модель Маркова виводить послідовність n-вимірних дійсних векторів (де n є малим цілим числом, наприклад 10), виводячи один із них кожні 10 мілісекунд. Вектори складатимуться з кепстральних коефіцієнтів, які отримують за допомогою перетворення Фур’є короткого часового вікна мовлення та декореляції спектра за допомогою косинусного перетворення, а потім беруть перші (найзначніші) коефіцієнти. Прихована модель Маркова матиме тенденцію мати в кожному стані статистичний розподіл, який є сумішшю діагональних коваріаційних гаусів, які дадуть вірогідність для кожного спостережуваного вектора. Кожне слово або (для більш загальних систем розпізнавання мовлення) кожна фонема матиме різний вихідний розподіл; прихована модель Маркова для послідовності слів або фонем створюється шляхом об’єднання окремих навчених прихованих моделей Маркова для окремих слів і фонем.

Вище описано основні елементи найпоширенішого підходу до розпізнавання мовлення на основі HMM. Сучасні системи розпізнавання мовлення використовують різні комбінації низки стандартних методів, щоб покращити результати порівняно з базовим підходом, описаним вище. Типова система з великим словниковим запасом потребує контекстної залежності для фонем (тому фонеми з різним лівим і правим контекстом мають різні реалізації як стани HMM); він використовуватиме кепстральну нормалізацію для нормалізації для іншого мовця та умов запису; для подальшої нормалізації мовця він може використовувати нормалізацію довжини голосового тракту (VTLN) для нормалізації між чоловіками та жінками та лінійну регресію максимальної ймовірності (MLLR) для більш загальної адаптації мовця. Функції матимуть так звані дельта- та дельта-дельта-коефіцієнти для фіксації динаміки мовлення, а також можуть використовувати гетероскедастичний лінійний дискримінантний аналіз (HLDA); або можна пропустити дельта- та дельта-дельта-коефіцієнти та використати сплайсинг і проекцію на основі LDA з наступним, можливо, гетероскедастичним лінійним дискримінантним аналізом або глобальним напівзв'язаним коваріаційним перетворенням (також відомим як лінійне перетворення максимальної правдоподібності або MLLT). Багато систем використовують так звані дискримінаційні методи навчання, які обходяться без суто статистичного підходу до оцінки параметрів HMM і натомість оптимізують певну міру навчання, пов'язану з класифікацією. Прикладами є максимальна взаємна інформація (MMI), мінімальна помилка класифікації (MCE) і мінімальна телефонна помилка (MPE).

Декодування мовлення (термін для того, що відбувається, коли системі представлено нове висловлювання та має обчислити найбільш ймовірне вихідне речення), ймовірно, використовуватиме алгоритм Вітербі, щоб знайти найкращий шлях, і тут є вибір між динамічним створенням комбінована прихована марковська модель, яка включає в себе як інформацію про акустичну, так і про мовну моделі та попередньо об'єднує її статично (підхід перетворювача кінцевого стану, або FST).

Можливе вдосконалення декодування полягає в тому, щоб зберегти набір хороших кандидатів замість того, щоб просто зберегти найкращого кандидата, і використовувати кращу функцію підрахунку балів (повторне оцінювання), щоб оцінити цих

хороших кандидатів, щоб ми могли вибрати найкращого відповідно до цього вдосконаленого балу. Набір кандидатів можна зберігати або як список (підхід списку N-найкращих), або як підмножину моделей (решітку). Повторна оцінка зазвичай виконується, намагаючись мінімізувати ризик Байєса (або його наближення): замість того, щоб брати вихідне речення з максимальною ймовірністю, ми намагаємося взяти речення, яке мінімізує очікування даної функції втрат щодо усі можливі транскрипції (тобто ми беремо речення, яке мінімізує середню відстань до інших можливих речень, зважених за їхньою оціненою ймовірністю). Функція втрат зазвичай є відстанню Левенштейна, хоча це можуть бути різні відстані для конкретних завдань; набір можливих транскрипцій, звичайно, скорочується, щоб підтримувати зручність. Було розроблено ефективні алгоритми для повторного оцінювання решіток, представлених у вигляді зважених перетворювачів кінцевого стану з редагованими відстанями, представленими як перетворювач кінцевого стану, що перевіряє певні припущення.

2.2.2. Розпізнавання мовлення на основі динамічного викривлення часу (DTW)

Динамічне викривлення часу — це підхід, який історично використовувався для розпізнавання мовлення, але зараз значною мірою витіснений більш успішним підходом на основі HMM.

Динамічне викривлення часу — це алгоритм для вимірювання подібності між двома послідовностями, які можуть відрізнятися за часом або швидкістю. Наприклад, схожість у моделях ходьби буде виявлено, навіть якщо на одному відео людина йшла повільно, а на іншому – швидше, або навіть якщо під час одного спостереження спостерігалися прискорення та уповільнення. DTW застосовувався до відео, аудіо та графіки – справді, будь-які дані, які можна перетворити на лінійне представлення, можна аналізувати за допомогою DTW.

Добре відомим додатком було автоматичне розпізнавання мовлення, щоб справлятися з різними швидкостями мовлення. Загалом, це метод, який дозволяє комп’ютеру знаходити оптимальну відповідність між двома заданими послідовностями (наприклад, часовими рядами) з певними обмеженнями. Тобто послідовності

«викривляються» нелінійно, щоб відповідати одна одній. Цей метод вирівнювання послідовності часто використовується в контексті прихованих марковських моделей.

2.2.3. Нейронні мережі

Нейронні мережі з'явилися як привабливий підхід до акустичного моделювання в ASR наприкінці 1980-х років. Відтоді нейронні мережі використовувалися в багатьох аспектах розпізнавання мовлення, таких як класифікація фонем, класифікація фонем за допомогою багатоцільових еволюційних алгоритмів, розпізнавання ізольованих слів, аудіовізуальне розпізнавання мовлення, аудіовізуальне розпізнавання мовця та адаптація мовця.

Нейронні мережі роблять менше явних припущень щодо статистичних властивостей функцій, ніж HMM, і мають кілька якостей, що робить їх привабливими моделями розпізнавання для розпізнавання мови. Коли нейронні мережі використовуються для оцінки ймовірностей сегмента ознак мовлення, вони дозволяють проводити дискримінаційне навчання природним і ефективним способом. Однак, незважаючи на їх ефективність у класифікації короткочасних одиниць, таких як окремі фонеми та ізольовані слова, ранні нейронні мережі рідко були успішними для завдань безперервного розпізнавання через їх обмежену здатність моделювати часові залежності.

Один із підходів до цього обмеження полягав у використанні нейронних мереж як попередньої обробки, трансформації ознак або зменшення розмірності на етапі перед розпізнаванням на основі HMM. Однак нещодавно LSTM і пов'язані з ним рекурентні нейронні мережі (RNN) і нейронні мережі із затримкою часу (TDNN) продемонстрували покращену продуктивність у цій галузі.

2.2.4. Глибокі прямі та рекурентні нейронні мережі

Також досліджуються глибокі нейронні мережі та автокодери з усуненням шуму. Глибока нейронна мережа прямого зв'язку (DNN) — це штучна нейронна мережа з кількома прихованими шарами одиниць між вхідним і вихідним рівнями. Подібно до дрібних нейронних мереж, DNN можуть моделювати складні нелінійні

зв’язки. Архітектури DNN генерують композиційні моделі, де додаткові рівні дозволяють компонувати функції з нижчих рівнів, надаючи величезну здатність до навчання та, таким чином, потенціал моделювання складних шаблонів мовних даних.

Успіх DNN у розпізнаванні мовлення великого словника стався в 2010 році промисловими дослідниками у співпраці з академічними дослідниками, де були прийняті великі вихідні рівні DNN на основі контекстно-залежних станів HMM, побудованих за допомогою дерев рішень. Перегляньте вичерпні огляди цієї розробки та сучасного стану станом на жовтень 2014 року в нещодавній книзі Springer від Microsoft Research. Дивіться також пов’язану історію автоматичного розпізнавання мовлення та вплив різних парадигм машинного навчання, зокрема глибокого навчання, у останніх оглядових статтях.

Одним із фундаментальних принципів глибокого навчання є відмова від ручної розробки функцій і використання необроблених функцій. Цей принцип вперше був успішно досліджений в архітектурі глибокого автокодера на «необроблених» спектрограмах або функціях лінійного банку фільтрів, показуючи його перевагу над функціями Mel-Cepstral, які містять кілька етапів фіксованого перетворення спектрограм. Нещодавно було показано, що справжні «необроблені» характеристики мовлення, форми хвилі, дають чудові результати розпізнавання мовлення у великому масштабі.

2.2.5. Наскрізне автоматичне розпізнавання мовлення

З 2014 року спостерігався великий дослідницький інтерес до «наскрізного» ASR. Традиційні фонетичні підходи (тобто всі моделі, засновані на HMM) вимагали окремих компонентів і навчання моделі вимови, акустичної та мовної моделі. Наскрізні моделі спільно вивчають усі компоненти розпізнавача мови. Це важливо, оскільки спрощує процес навчання та розгортання. Наприклад, модель мови n-gram необхідна для всіх систем на основі HMM, а типова модель мови n-gram часто займає кілька гігабайт пам’яті, що робить її непрактичною для розгортання на мобільних пристроях. Отже, сучасні комерційні системи ASR від Google і Apple (станом на 2017 рік) розгортаються в хмарі та потребують підключення до мережі, а не локального пристрою.

Перша спроба наскрізного ASR була з системами на основі часової класифікації коннекціоністів (CTC), представленими Алексом Грейвсом з Google DeepMind і Navdeep Jaitly з Університету Торонто в 2014 році. Модель складалася з рекурентних нейронних мереж і рівня CTC. Спільно модель RNN-CTC вивчає вимову та акустичну модель разом, однак вона не здатна вивчати мову через припущення умовної незалежності, подібні до HMM. Отже, моделі CTC можуть безпосередньо навчитися відображати акустику мовлення англійським символам, але моделі допускають багато поширених орфографічних помилок і повинні покладатися на окрему мовну модель для очищення транскриптів. Пізніше Baidu розширив роботу з надзвичайно великими наборами даних і продемонстрував певний комерційний успіх китайською та англійською мовами. У 2016 році Оксфордський університет представив LipNet, першу наскрізну модель читання з губ на рівні речення, яка використовує просторово-часові згортки в поєднанні з архітектурою RNN-CTC, що перевершує продуктивність людського рівня в обмеженому наборі граматичних даних. У 2018 році компанія Google DeepMind представила масштабну архітектуру CNN-RNN-CTC, яка досягає в 6 разів кращої продуктивності, ніж у експертів-людей.

Альтернативним підходом до моделей на основі CTC є моделі на основі уваги. Моделі ASR на основі уваги були введені одночасно Чаном та ін. Університету Карнегі-Меллона та Google Brain і Bahdanau et al. Університет Монреаля в 2016 році. Модель під назвою «Listen, Attend and Spell» (LAS) буквально «слухає» акустичний сигнал, звертає «увагу» на різні частини сигналу та «викладає» транскрипцію одним символом. зараз. На відміну від моделей на основі CTC, моделі на основі уваги не мають припущень про умовну незалежність і можуть безпосередньо вивчати всі компоненти розпізнавача мовлення, включаючи вимову, акустику та мовну модель. Це означає, що під час розгортання немає необхідності носити мовну модель, що робить її дуже зручною для програм з обмеженою пам’яттю. До кінця 2016 року моделі на основі уваги досягли значного успіху, зокрема перевершили моделі CTC (з моделлю зовнішньої мови або без неї). Починаючи з оригінальної моделі LAS, були запропоновані різні розширення. Latent Sequence Decompositions (LSD) було запропоновано Університетом Карнегі-Меллона, Массачусетським технологічним інститутом і Google

Brain для прямого виділення одиниць підслів, які є більш природними, ніж англійські символи; Оксфордський університет і Google DeepMind розширили LAS до «Watch, Listen, Attend and Spell» (WLAS), щоб керувати читанням по губах, перевищуючи продуктивність людського рівня.

2.3. Методи аналізу Big Data

Світом керують дані, і вони аналізуються щосекунди. Глобальне опитування McKinsey показало, що коли організації використовують дані, це приносить користь клієнтам і бізнесу, створюючи нові послуги на основі даних, розробляючи нові бізнес-моделі та стратегії, а також продаючи продукти та утиліти на основі даних. Стимул для інвестування та впровадження інструментів і методів аналізу даних величезний, і компаніям потрібно буде адаптуватися, впроваджувати інновації та розробляти стратегію для цифрового ринку, що розвивається.

У звіті McKinsey про великі дані визначено низку методів і технологій великих даних, які беруть участь у різних галузях, таких як статистика, інформатика, прикладна математика та економіка. Оскільки ці методи покладаються на різні дисципліни, інструменти аналітики можна застосовувати як до великих даних, так і до інших менших наборів даних:

1) А/Б тестування: ця техніка аналізу даних передбачає порівняння контрольної групи з різними тестовими групами, щоб визначити, які методи або зміни покращать певну об’єктивну змінну. Прикладом є аналіз того, яка копія, текст, зображення чи макет підвищить рівень конверсії на сайті електронної комерції. Big Data знову вписуються в цю модель, оскільки вони можуть тестувати величезні числа, однак цього можна досягти, лише якщо групи мають достатньо великий розмір, щоб отримати значні відмінності.

2) Об'єднання та інтеграція даних: завдяки поєднанню набору методів, які аналізують та об’єднують дані з багатьох джерел і рішень, аналітика стає ефективнішою та потенційно точнішою, ніж якщо б вона була зроблена з одного джерела даних.

3) Видобуток даних: поширений інструмент, який використовується в аналітиці великих даних. Інтелектуальний аналіз даних витягує шаблони з великих наборів даних шляхом поєднання методів статистики та машинного навчання в рамках керування базами даних.

4) Машинне навчання: добре відоме в галузі штучного інтелекту машинне навчання також використовується для аналізу даних. Виходячи з інформатики, воно працює з комп'ютерними алгоритмами, щоб виробляти припущення на основі даних. Цей метод забезпечує прогнози, які були б неможливі для аналітиків.

5) Обробка природної мови (NLP): цей інструмент аналізу даних, відомий як спеціалізація інформатики, штучного інтелекту та лінгвістики, використовує алгоритми для аналізу людської (природної) мови.

6) Статистика: ця техніка працює для збору, організації та інтерпретації даних у рамках опитувань та експериментів.

Інші методи аналізу даних включають просторовий аналіз, прогнозне моделювання, вивчення правил асоціації, аналіз мережі та багато іншого. Технології, які обробляють, керують та аналізують ці дані, належать до зовсім іншої та великої сфери, яка так само розвивається з часом. Крім методів і технологій, цінні дані будь-якої форми чи розміру. Якщо керувати ними точно й ефективно, вони можуть розкрити безліч відомостей про бізнес, продукти та ринок [16].

У США аналітика Big Data використовується найактивніше: понад 55% компаній із різних галузей працюють із цією технологією. У Європі та Азії затребуваність аналітики великих даних набагато нижча – близько 53% [17].

Наприклад, у США сепсис посідає 10 місце у рейтингу причин смерті серед хвороб. Щороку сепсис виникає приблизно в 1 млн. американців, від 28% до 50% їх вмирає. На лікування сепсису щорічно витрачається близько 20 млрд. доларів [17].

При цьому основна причина смертельних випадків – недостатній лікарський контроль. Пацієнти виписуються зі шпиталю або отримують першу допомогу і після цього за ними не спостерігають. Однак після цього великий ризик розвитку сепсису, симптоми якого – жар, озноб, прискорене дихання та пульс, висипання, розгубленість та дезорієнтація – схожі на симптоми інших поширених захворювань. Часто пацієнти

надто пізно звертаються до лікаря або захворювання не вдається правильно діагностувати на ранніх стадіях. В результаті швидко розвивається септичний шок і відбувається часто незворотне ураження багатьох органів [17].

Для контролю стану пацієнтів пропонується використовувати сертифікований пристрій HealthPatch від компанії Vital Connect, який збиратиме основні показники стану пацієнтів, включаючи навіть пози та рух (при сепсисі вони змінюються). Далі інформація надходить на сервери ClearStory Data, де поєднується з іншими медичними даними про пацієнтів і аналізується в реальному часі за допомогою рішення на базі Apache Spark. У перспективі такі пристрої будуть отримувати всі пацієнти, які вийшли зі шпиталів і отримали першу допомогу, за якими може йти сепсис. Подібна система, але з меншим рівнем аналізу даних, вже успішно реалізована в Сінгапурі [4][17].

Результат: створено рішення, яке дозволяє системі охорони здоров'я США значно знизити смертність від сепсису (загального зараження крові) [17].

Таким чином, використання технології у концепції розумної лікарні є невід'ємною частиною її реалізації [17].

РОЗДІЛ 3
Види атак на IP-АТС Asterisk та методи протистояння їм

3.1. Будова мережі IP-телефонії на базі IP-АТС Asterisk

IP-телефонія – це технологія, що дозволяє використовувати Інтернет або будь-яку іншу IP-мережу для проведення міжнародних та міжміських телефонних розмов та передачі факсу в режимі реального часу [17].

Будь-яка мережа IP-телефонії використовує мережу передачі, найчастіше це комп'ютерна мережу. Голос у таких мережах передається у цифровому вигляді за допомогою RTP (Real-time Transport Protocol – протокол транспортування інформації в реальному часі) пакетів [17].

Під IP-телефонією мається на увазі голосовий зв'язок, що здійснюється мережами передачі даних, зокрема IP-мережами. На сьогоднішній день IP-телефонія все більше витісняє традиційні телефонні мережі за рахунок легкості реалізації, низької вартості дзвінка, простоти конфігурації, високої якості зв'язку та відносної безпеки з'єднання [5][17].

Під час проєктування та реалізації системи необхідно звернути увагу на дизайн мережі.

Устаткування IP телефонії для офісу може включати цілий комплекс пристроїв (рис. 3.1), кожне з яких виконує певні функції:

- АТС для IP телефонії. Це основний комутаційний пристрій, що не тільки забезпечує підключення до традиційних послуг зв'язку, але і створює локальну мережу передачі даних всередині компанії, розвантажуючи зовнішню лінію. Такий комплекс обладнання має широкий вибір додаткових функцій, який гідно оцінили власники бізнесу – автоматична або ручна переадресація, внутрішній безкоштовний зв'язок, конференц-зв'язок, утримання виклику та заборона (обмеження) вхідних дзвінків з певних номерів та багато іншого;

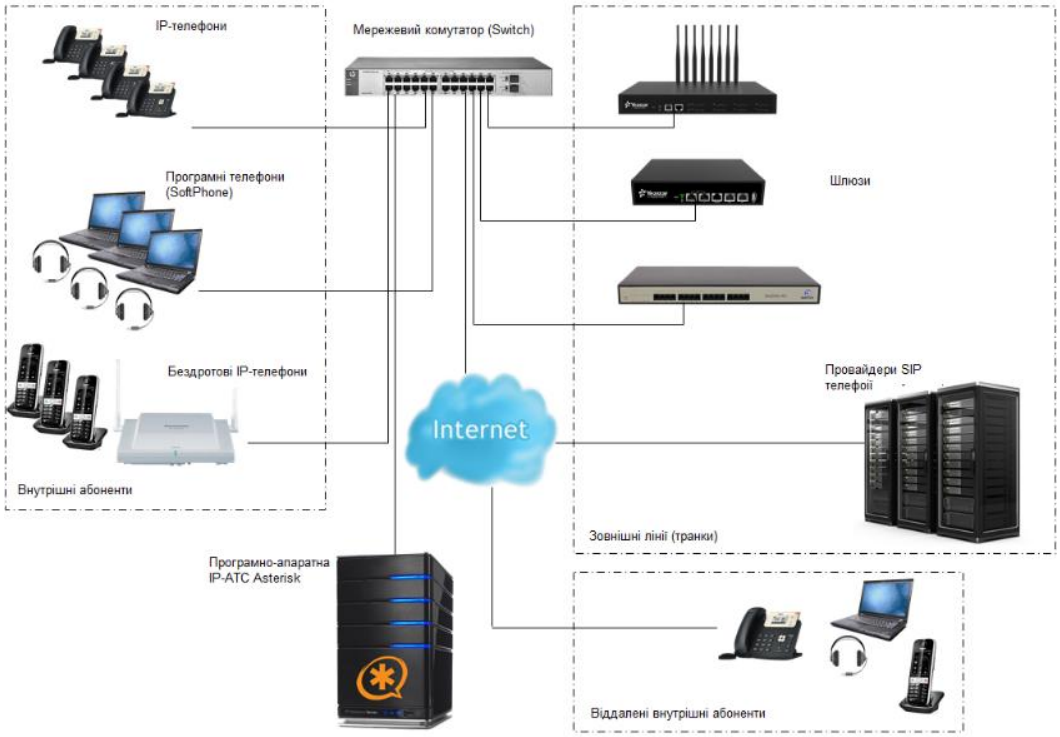

Рис. 3.1. Мережа IP телефонії [6]

- сервер для IP телефонії. Серверні станції забезпечують контроль локальної мережі та об'єднують АТС та користувача. Всередині кожного сервера можуть бути цифрові та аналогові пристрої для перетворення (кодування) сигналу, а також спеціальні плати для транслювання інформації на різні зовнішні пристрої. Завдяки уніфікованим елементам, при необхідності можна суттєво розширити абонентську внутрішню мережу або оснастити сервер GSM (модуль для мобільного цифрового стільникового зв'язку) модулем для повноцінного мобільного зв'язку;
- телефони для IP телефонії. Це кінцеві термінали здійснення обміну інформацією між абонентами. Зовні вони нічим не відрізняються від стандартних телефонів, але мають спеціальний роз'єм, завдяки якому вони підключаються до мережі. Також багато сучасних апаратів підтримують функцію відеозв'язку, що суттєво розширює їх функціональність;
- гарнітура для IP телефонії. Це допоміжні пристрої, які є незамінними для роботи call-центрів. На відміну від звичайної трубки, гарнітура кріпиться на голові оператора, звільняючи руки, що дозволяє співробітнику компанії одночасно вести роз-

мову і працювати за комп'ютером. Крім того, гарнітура суттєво підвищує якість сигналу та усуває ефект відлуння, в порівнянні з підключенням мікрофона через зовнішні динаміки;

- програми для IP телефонії. Нормальну функціональність зв'язку неможливо забезпечити без спеціального програмного забезпечення, призначеного для кодування сигналу, його перетворення, стиснення пакетів даних, контролю за трафіком та інших функцій [6][17].

Часто без будь-якої потреби Asterisk підключають до мережі за найбільш уразливою схемою, зображеною на рис. 3.2.

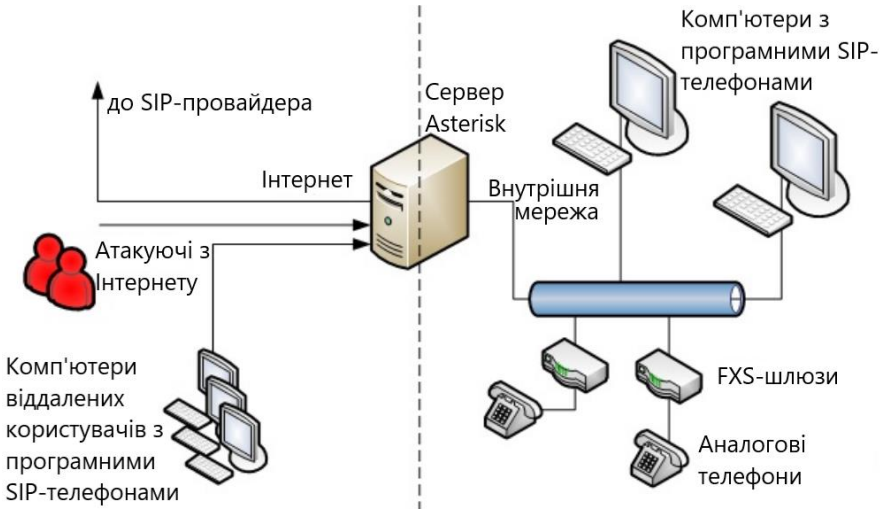

Рис. 3.2. Не рекомендована схема підключення Asterisk через зовнішню адресу

Факт доступності Asterisk в Інтернеті – головна загроза безпеці всієї системи. Будь-який слабкий пароль або будь-яка вразливість у вихідному коді Asterisk можуть бути використані атакуючими, щоб отримати несанкціонований доступ до АТС та дзвонити за рахунок компанії-власника сервера Asterisk. У найкращому разі метою атакуючих може стати відмова в обслуговуванні [17].

Стійкі паролі та регулярні оновлення, звичайно ж, знижують ризик. Ще сильніше за нього можна знизити спеціалізованими засобами захисту, а саме – міжмережевими екранами (МЕ). Якщо підключати Asterisk так, як показано на рис. 3.3, то сервер буде безпечно закритий за периметром локальної мережі [17].

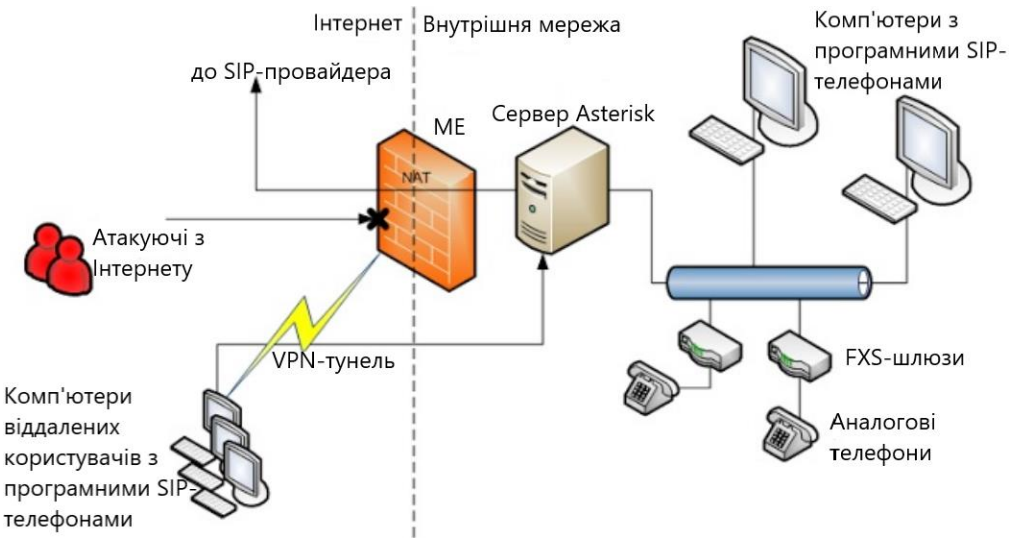

Рис. 3.3. Рекомендована схема підключення Asterisk з використанням ME

ME пропускає вихідний трафік від сервера Asterisk до SIP провайдеру і назад через динамічні правила NAT (англ. Network Address Translation – технологія перетворення приватних IP-адрес на зовнішні IPv4). А можливість підключення користувачів віддалених офісів забезпечується через VPN-тунель. Користувач спочатку підключається по VPN до мережі підприємства, а потім по віртуальному каналу - до сервера Asterisk. Asterisk більше не видно із зовнішньої мережі, недоступний атакуючим [7][17].

3.2. Аналіз видів можливих атак на сервер Asterisk

3.2.1. Перепродаж трафіку (Tollfroud)

Перепродаж трафіку – один із найзручніших способів заробляння грошей хакерами. Зламавши станцію і направивши дзвінки на дорогі міжнародні напрямки, хакер отримує якусь винагороду на свої електронні гаманці, які далі переводяться в готівку і виходять реальні гроші. Наочна схема зображено на рис. 3.4 [17].

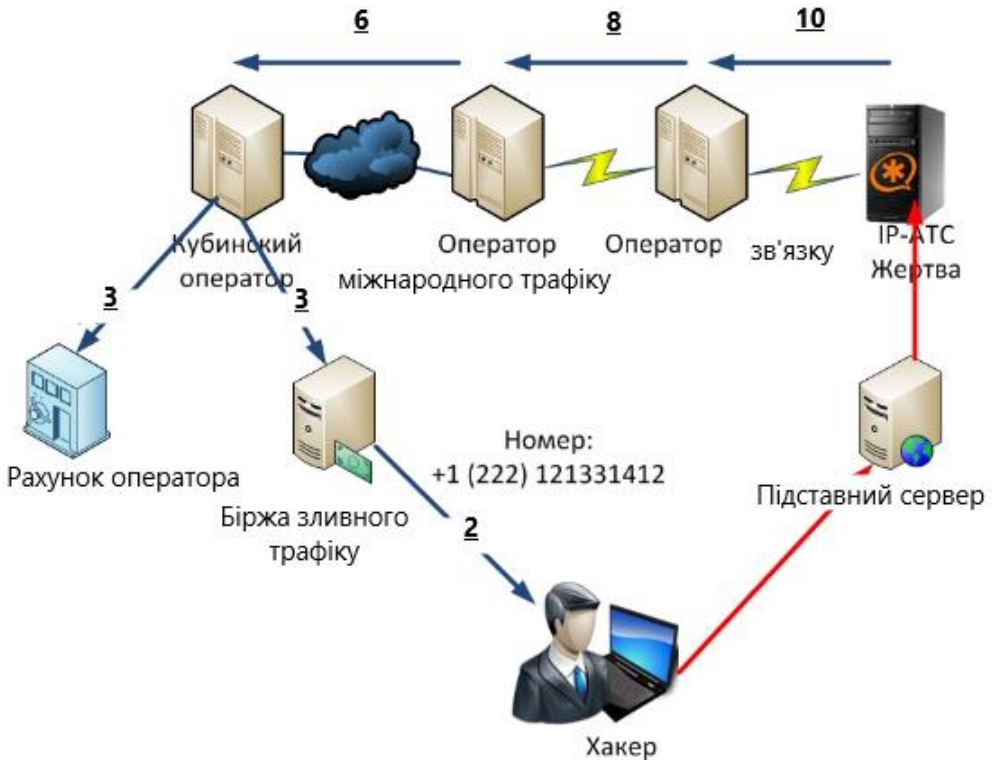

Рис. 3.4. Схема перепродажу трафіку

Розглянемо схему детальніше. Є хакер, який бажає заробити гроші шляхом перепродажу трафіку. Він йде на біржу зливного трафіку, реєструється та отримує певний пул номерів, які можуть його ідентифікувати надалі. Далі через якісь підставні сервери знаходяться і, якщо виходить, зламуються сервери IP-АТС. Далі на номери, надані хакеру на біржі зливного трафіку, починають дзвонити. Дзвінки платні. Допустимо, дзвінок коштує 10 грн (оплата жертви оператору). Дзвінок направляється, як правило, за кордон (як правило це Куба, Палестина, Румунія, Латвія тощо), до країн, де не приділяється належної уваги кібер-злочинності, тобто де є можливість займатися таким бізнесом. І так жертва платить Оператор зв'язку 10 грн. за хвилину. ОС виходить на міжнародні лінії через оператор міжнародного трафіку (ОМТ), якому він платить 8 грн за хвилину, далі ОМТ спрямовує дзвінок на місцевого оператора (Куба, Палестина та ін.), який займається «відмиванням» голосового трафіку і сплачує йому вже 6 грн. за хвилину, даний оператор розподіляє гроші таким чином – частина грошей йде йому в оплату за послуги (так скажімо, заробляє цю суму – залишає у себе на рахунку), а частина грошей спрямовує на біржу зливного трафіку, де зареєстрований хакер. Далі біржа, залишивши собі 1 грн, дві платить хакеру [8][17].

3.2.2. DDoS-атаки

DDoS (Distributed Denial of Service attack) – це вторгнення, яке задовольняє співвідношення «багато порушників – одна жертва». Вторгнення вважається розподіленим, якщо його етапи виконуються від імені різних джерел у мережі. Події, що становлять розподілене вторгнення, скоординовані. Джерела, від імені яких виконується розподілене вторгнення (атака), взаємопов'язані [17].

Простий трафік – це HTTP запити. Основа запиту – HTTP-заголовок. Сторона, що запитує, може використовувати скільки завгодно заголовків, надаючи їм потрібні властивості. Зловмисники, які проводять DDoS, можуть змінювати ці заголовки, тому їх важко розпізнати як атаки [17].

HTTP(S) GET-запит - спосіб запитує дані на сервері. Цей запит може "попросити" сервера передати якийсь файл, зображення, сторінку або скрипт для відображення у веб-браузері. HTTP(S) GET-флуд – DDoS атака прикладного рівня (7) моделі OSI. Зловмисник посилає потужний потік запитів на сервер для переповнення ресурсів. І тут сервер перестає відповідати запити реальних користувачів [17].

HTTP(S) POST-запит - метод, суть якого полягає в тому, що дані розміщуються в тілі запиту для подальшої обробки на сервері. HTTP POST-запит кодує інформацію, що передається, і поміщає на форму, а потім відправляє цей контент на сервер. Цей метод використовують, коли потрібно передавати великі обсяги даних. HTTP(S) POST-флуд - тип DDoS-атаки, при якому кількість POST-запитів переповнюють сервер, в результаті він не може відповісти на них. Це спричиняє аварійну зупинку сервера з відповідними наслідками [17].

Всі перелічені запити також передаються HTTPS, посилаються дані, у разі шифруються. І такий захист грає на користь хакерів. Адже для виявлення такого запиту сервер має спочатку розшифрувати його. А розшифрувати поток запитів під час такої атаки дуже складно, і це створює додаткове навантаження на сервер [17].

ICMP-флуд (Smurf-атака). Дуже небезпечний тип атаки. Хакер відправляє підробку ICMP-пакет, у якому адреси атакуючого змінюється на адресу жертви. Всі вузли надсилають відповідь на отриманий ping-запит. Для цього в більшості випадків використовують велику мережу, щоб комп'ютер-жертва не мала жодних шансів [17].

UDP-флуд (User Datagram Protocol – протокол транспортного рівня моделі OSI) (або атака Fraggle). За своїм типом аналогічний ICMP флуду, але в цьому випадку застосовуються пакети UDP. Через насичення смуг пропускання відбувається відмова в обслуговуванні сервера жертви [17].

SYN-флуд (англ. Synchronize sequence numbers – синхронізація номерів послідовності). В основі такої атаки лежить запуск великої кількості одночасних TCP-з'єднань (англ. Transmission Control Protocol – протокол управління передачею) через посилання SYN-пакету з неіснуючою зворотною адресою [17].

Надсилання "важких пакетів". При такому вигляді атаки злодій відсилає пакети сервера, що витрачають процесорний час, але не насичують смугу пропускання. В результаті відбувається збій у системі, і користувачі не можуть отримати свої ресурси.

Переповнення сервера лог-файлами. При некоректній системі ротації лог-файлів шахрай може надсилати об'ємні пакети, які незабаром займуть вільне місце на жорсткому диску сервера. В результаті – збій у системі [17].

Помилки програмного коду. Деякі зловмисники з досвідом у цій сфері діяльності розробляють спеціальні програми-експлоїти, що дозволяють атакувати складні системи комерційних організацій. Для цього вони шукають помилки в коді програм, які можуть призвести до завершення служби [17].

Недоліки у програмному коді. Та ж ситуація: хакери шукають помилки в коді програм або ОС (операційна система), при цьому змушують їх опрацьовувати виняткові ситуації, в результаті програми виходять з ладу [9][17].

3.3. Багаторівневий захист IP-АТС Asterisk

Говорячи про безпеку рішення IP-АТС в цілому потрібно розуміти, що безпека будується не тільки на безпеці самого Asterisk, так само потрібно забезпечити безпеку та оточення Asterisk [17].

Типові помилки, які допускаються адміністраторами Asterisk.

1. Відсутність мережного екрана (відсутність iptables, або вимкнений iptables, або налаштований неправильно).

2. Старі дистрибутиви та програмне забезпечення (старе програмне забезпечення може містити вразливості. Необхідні постійні оновлення системи).

3. Стандартні логіни та паролі (Web-інтерфейс, SQL, обладнання).

4. Дизайн мережі (Asterisk та обладнання, що працює з ним на зовнішній адресі без захисту – це ласий шматочок для хакерів).

5. Помилки конфігурації.

6. Відсутність контролю за системою (немає контролю логів) [9][17].

На жаль, проблеми з IP-АТС Asterisk останнім часом стали частішими. Тому багато хто вважає, що Asterisk небезпечна система. Однак цю тезу хочеться заперечити. По-перше, якщо говорити про можливості самого Asterisk, то має дуже багатий набір інструментів із забезпечення безпеки. Проте він дуже часто зазнає зламів. Чому так? Справа все в адміністраторі цієї системи. Немає єдиної галочки для активації безпеки Asterisk. Безпека такої мережі – це вживання ряду комплексних заходів, про які, як правило, адміністратори забувають, тим самим наражають на Астеріськ загрози. Розглянемо варіанти захисту від перепродажу трафіку. За допомогою грамотно написаного dialplan (план маршрутизації дзвінків) можна значно підвищити безпеку. Перше, що рекомендується, – це поділ абонентів на контексти зі своїми правилами маршрутизації [17].

В sip.conf:

```
[1000]
context = from_chef
[1001]
context = from_it
[1002]
context = from_fin
```

Рис. 3.5. Внесення в asterisk/sip.conf

Розділення за контекстами дозволяє нам наділити різними правами абонентів на телефонний зв'язок. Це важливо, тому що не всім потрібно, скажімо, дзвонити за міжнародними напрямками. Далі контекстам призначаємо правила [17].

```
[allow]
exten =>_X., n, Dial(SIP/operator/${EXTEN}) ;Дозволяємо будь-які дзвінки через оператора
exten => _[12]XXX, n, Dial(SIP/${EXTEN}) ;Дозволяємо внутрішні з'єднання
[from_chef]
exten=> _X., n, Goto(allow,${EXTEN},1) ;Всі дзвінки направляємо в створений контекст [allow]
[from_it]
exten=> _9810., n, Hungup() ;Обмежуємо міжнародні напрямки
exten=> _X., n, Goto(allow,${EXTEN},1) ;Всі дзвінки направляємо в контекст [allow]
[from_fin]
exten=> _9810., n, Hungup() ;Обмежуємо міжнародні напрямки
exten=> _989., n, Hungup() ;Обмежуємо направлення на стільникові напрямки
exten=> _X., n, Goto(allow, ${EXTEN},1) ;Всі дзвінки направляємо в контекст [allow]
```

Рис. 3.6. Вихідна маршрутизація відділів

Тим самим фінансовому відділу забороняємо дзвінки на міжнародні та стільникові напрями. IT підрозділи заборонені лише міжнародні напрями. Ну а керівнику дозволяємо будь-які з'єднання [10][17].

Для того, щоб отримувати інформацію про заборонені дзвінки на пошту, вчимо Asterisk фіскалити про порушення. Для цього додамо ще один контекст [alarm]. І спрямовуємо в цей контекст заборонені дзвінки [17].

```
[alarm]
exten => _9810X., 1, playback(zaboroneno) ;Повідомляємо абоненту, що йому заборонений даний напрям
exten => _9810X., n, System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} | mail -s «8-10 ALARM» it_admin@ukr.net) ;Фіскалить на пошту, якщо будуть міжнародні дзвінки
exten => _9810X., n, Hangup()
```

Рис. 3.7. Контекст для заборонених вихідних дзвінків

Таким чином, не тільки блокуємо заборонені напрямки, а й у разі інциденту отримуємо повідомлення, хто намагається додзвонитися. Тим самим вчасно зможемо

зрозуміти, що сервер зламаний, а не тоді, коли надійдуть величезні рахунки за зв'язок [17].

Такий план маршрутизації безпечний у тому випадку, якщо доступ до контексту є лише у керівника, як це передбачається. Але можна захистити цей контекст від несанкціонованого використання ресурсів компанії. У dialplan ми можемо прописати функцію IVR (Interactive Voice Response – інтерактивне голосове меню), яка виконуватиме роль пароля для доступу до здійснення дзвінків на заборонені напрямки [17].

Ось чому добре використовувати Asterisk, dialplan дозволяє гнучко налаштувати маршрутизацію. Можемо забороняти напрямки за різними параметрами, можемо розмежувати права абонентам, можемо налаштувати повідомлення про заборонені дзвінки, також можна налаштувати обмеження дзвінків за часом, за введенням pin-коду та багато іншого, що дозволяє підвищити безпеку IP-АТС [17].

Тепер розглянемо варіанти захисту ще від однієї загрози, яка може загрожувати роботі сервера IP телефонії – DdoS-атаки.

Методи боротьби з DDoS можна розділити на два види: активні та пасивні. Пасивні – це заздалегідь підготовлені методи обережності та запобігання атакі. Активні застосовуються у разі, якщо атака вже відбувається зараз [11].

Основний пасивний метод - це, звичайно ж, запобігання. Багато хто вважає цей метод несуттєвим, але все-таки в більшості випадків він є основним [17].

В основі профілактики має лежати виключення таких факторів як особистісна та ворожість, конкуренція, релігійні чи інші розбіжності. Якщо вчасно усунути подібні причини і зробити відповідні висновки, DDoS не торкнеться вашої мережі. Але це метод більше стосується управління, а чи не технічної боку проблеми.

Використання програмного та апаратного забезпечення.

Сьогодні багато компаній-виробників розробили спеціальні та вже готові рішення для захисту від DDoS-атак. Це програмне забезпечення різних видів захисту малих та найбільших мереж для різних типів організацій. Це також вважається пасивним методом захисту, оскільки є превентивним способом [17].

Фільтрування та блокування трафіку, що походить від атакуючих машин дає можливість знизити або зовсім погасити атаку. Існує два способи фільтрації: маршрутизація за списками ACL (англ. Access Control List - список правил, що забороняють або дозволяють використання ресурсів мережі) та використання міжмережевих екранів. Використання списків ACL дозволяє фільтрувати другорядні протоколи, не торкаючись при цьому протоколів TCP і не уповільнюючи швидкість роботи користувачів з ресурсом. Міжмережні екрани використовуються лише для захисту приватних мереж (рис. 3.3) [17].

Зворотний DDoS – перенаправлення трафіку на атакуючого. Якщо мережа має достатні серверні потужності, можна не лише подолати атаку, а й вивести з ладу атакуючого устаткування [17].

Усунення уразливостей – тип захисту націлений на усунення помилок у системах чи службах. На жаль, такий спосіб захисту не працює проти флуд-атак [17].

Побудова розподільчих систем дозволяє обслуговувати користувачів навіть якщо деякі вузли стають недоступними через DDoS-атаки. Для цього використовується мережне або серверне обладнання різних типів, яке розміщується у різних ДЦ (дата-центрах). Також часто встановлюють дублюючу (резервну) систему. Це вигідно робити для великих проєктів, які хвилюються за свою репутацію та мають величезну кількість користувачів [17].

Моніторинг – встановлення спеціальної системи моніторингу та оповіщення. Вона дозволить обчислити DDoS-атаку за певними критеріями. Моніторинг безпосередньо не захищає систему, що атакується, але дозволяє вчасно зреагувати і запобігти збою в системі роботи ресурсу. Наприклад, оповіщення про недостатнє залишок місця на дисках сервера, про перезавантаження або повне відключення сервера. Це, звісно, пасивний спосіб захисту.

Придбання сервісу захисту від DDoS-атак – дає можливість захиститися від багатьох типів DDoS-атак, використовуючи цілий комплекс механізмів фільтрації небажаного трафіку до атакуючих серверів. Щоправда, коштують такі послуги дорого [12].

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

4.1. Вступ

Загальні вимоги до проведення робочих процесів зі сторони охорони праці полягає в наступному:

- безпечність технічного обладнання при перевезенні, монтажі, налаштуванні та користуванні (експлуатації), параметрів і видів енергоспоживання, організації робочих місць;
- безпечність технічного процесу, що складається з безпечності обладнання, матеріалів і сировини, що використовуються, операцій, що проводяться, і безпосередньо організації технічного процесу;
- сертифікація та стандартизація виконуваних технічних процесів та обладнання з метою забезпечення безпечності праці.

Досягти виконання всіх перелічених пунктів можливо шляхом усунення прямого контакту працівників з небезпечними робочими чинниками, впровадженні комплексів механізації, дистанційного керування процесами та автоматизації, покращення технічних процесів для мінімізації впливу шкідливих чинників, безпечного розташування обладнання, дотримання пожежної безпеки, організації безпечного робочого місця робітника, формування та дотримання інструкцій з охорони праці.

У цьому розділі буде досліджено і розроблено заходи з охорони праці для інженера голосових платформ (VoIP інженера). Робоче місце інженера – кабінет в офісному приміщенні.

4.2. Аналіз умов праці на робочому місці інженера голосових платформ (VoIP інженера)

Шкідливий виробничий фактор – це небажане явище, яке супроводжує виробничий процес. Його вплив на працівника може призвести до погіршення стану здоров’я людини, зниження ефективності праці, виробничих чи професійних захворювань і навіть смерті внаслідок захворювання.

Небезпечний виробничий фактор – це небажане явище, яке супроводжує виробничий процес і яке за певних умов може призвести до травми або іншого раптового погіршення здоров'я працівника (гостре отруєння, гостре захворювання) і навіть може стати причиною раптової смерті.

4.2.1. Організація робочого місця інженера голосових платформ (VoIP інженера)

Офісний кабінет розрахований для робочого місця для 4 осіб. Його загальна площа дорівнює:

$$A = a * b \, [\text{м}^2], \tag{4.1}$$

$$A = 4 * 5 = 20 \, \text{м}^2, \tag{4.2}$$

де a – довжина і b – ширина (рис. 4.1).

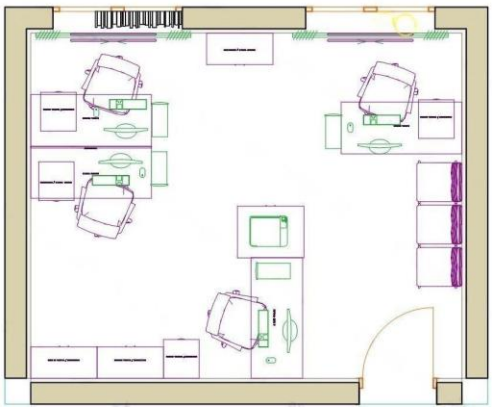

Рис. 4.1. Схема розташувань робочих місць

Робоча площа однієї людини приблизно дорівнює:

$$A_{\text{людини}} = \frac{A}{n}\ [\text{м}^2], \tag{4.3}$$

$$A_{\text{людини}} = \frac{20}{4} = 5\ \text{м}^2, \tag{4.4}$$

де n – кількість робітників.

Об’єм кімнати можна визначити як:

$$V = A\ * h\ [\text{м}^3], \tag{4.5}$$

$$V = 20\ * 2{,}5 = 50\ \text{м}^3, \tag{4.6}$$

де h – висота кабінета.

Периметр кабінету дорівнює:

$$P = 2a + \ 2b\ [\text{м}], \tag{4.7}$$

$$P = 2 * 4 + \ 2 * 5 = 18\ \text{м}, \tag{4.8}$$

Усі розміри затверджені будівельними нормами України СНиП 2.09.02-85 «Производственные здания» [24].

Кабінет обладнаний 4 стельовими світильниками та 2 вікнами. Також має різні шини живлення (на 220В).

Найбільш сприятливим мікрокліматом на робочому місці є:

- Температура: не вище 24°С;
- відносна вологість: 40-60%;
- швидкість повітря: 0,2м/с.

Для підтримки оптимальних значень мікроклімату використовується система опалення та кондиціонування. Також наявні джерела шуму, такі як електричні прилади, звуки проїжджої частини під вікном. Кабінет забезпечений аптечкою першої медичної допомоги та вогнегасником.

4.2.2. Перелік шкідливих та небезпечних виробничих чинників.

Відповідно до гігієнічних нормативів ГН від 08.04.2014 №248 «Гігієнічна класифікація праці за показниками шкідливості та небезпеки факторів виробничого середовища, важкості та напруженості трудового процесу» можна виділити перелік шкідливих і небезпечних факторів для нашого випадку. Вони належать до групи фізичних факторів і групи хімічних факторів:

- мікроклімат (температура, вологість, швидкість руху повітря);

- неіонізуючі електромагнітні поля та випромінювання: електростатичні поля, постійні магнітні поля, електричні та магнітні поля промислової частоти (50 Гц), електромагнітне випромінювання радіочастотного діапазону, електромагнітне випромінювання оптичного діапазону, зокрема лазерне та ультрафіолетове;

- вібрація (місцева, загальна);

- освітлення: природне (відсутність або недостатність), штучне (недостатнє освітлення, прямі та відбиті сліпучі відблиски тощо) [25].

4.2.3. Розробка заходів з охорони праці

Залежно від шкідливого і небезпечного фактору розрізняють наступні методи захисту і нормування:

- нормалізація мікроклімату приміщень і робочих місць (провітрювання, кондиціонування повітря, опалення тощо);

- захист від електромагнітного випромінювання;

- захист від надмірного шуму та вібрації (шумоізоляція, віброізоляція);

- захист від ураження електричним струмом (захисне заземлення тощо).

Аналіз перерахованих шкідливих і небезпечних факторів наведено нижче.

4.2.3.1. Мікроклімат робочого місця

Аналіз фактору мікроклімату полягає в порівнянні оптимальних умов праці з фактичними згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень», категорія IIб:

Таблиця 4.1

Порівняння характеристик мікроклімату

	Холодний сезон		Теплий сезон	
	Оптимально	Реально	Оптимально	Реально
Температура, °С	17-19	18	21-23	25
Вологість, %	60-40	55	60-40	50
Швидкість повітря, м/с	0.2	0.1	0.3	0.1

Таблиця 4.1 показує, що всі параметри знаходяться в допустимих межах, крім температури в теплий період року. Для поліпшення умов праці необхідно збільшити кількість повітроохолоджувачів на робочому місці [26].

4.2.3.2. Виробничий шум, ультразвук, інфразвук

Шумове середовище, в якому працює інженер голосових платформ, може відрізнятися.

Аналіз фактора мікроклімату полягає в порівнянні оптимальних умов праці з фактичними згідно з ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»:

Таблиця 4.2

Порівняння шумових характеристик

	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц								
	31.5	63	125	250	500	1000	2000	4000	8000
Оптимально	93	79	70	63	58	55	52	50	49

Закінчення таблиці 4.2

Реально	49	62	70	78	79	81	86	72	64

Таблиця 4.2 показує, що шумове забруднення з різних джерел у цьому кабінеті є високим, і, таким же чином, вплив такого рівня шумового забруднення на здоров'я персоналу, зайнятого в кабінеті, може бути вплинуто [27].

4.2.3.3. Вібрації

Вібрація, що діє на людину, має дуже широкий діапазон частот – від десятих часток до кількох тисяч Гц. Характерними ознаками шкідливого впливу вібрації на людину є можливі зміни функціонального стану людини. Це, перш за все, підвищення стомлюваності, збільшення часу рухової реакції, порушення вестибулярної реакції. Медичні дослідження встановили, що вібрація подразнює периферичні нервові закінчення, розташовані на ділянках тіла людини, які сприймають зовнішні коливання. В кабінеті ми маємо такі джерела вібрації, як: електричні прибори, кондиціонер, лампа і т.д.

При дії постійного параметра місцевої та загальної вібрації згідно з ДСН 3.3.6. 039-99 «Державні санітарні норми виробничої загальної та локальної вібрації», що нормується, є середньоквадратичне значення віброшвидкості (V) і віброприскорення (ω) або їх логарифмічні рівні в дБ в діапазоні октавних смуг із середнім геометричним. частоти Оцінка ступеня шкідливого впливу вібрації на людину здійснюється за спектром віброшвидкості [28].

Таблиця 4.3

Порівняння вібраційної характеристики

	Виміряні пікові рівні віброприскорення, дБ							
	120	125	130	135	140	145	150	155
	Допустима кількість імпульсів за 1 годину							
Опти-мально	160000	50000	16000	5000	1600	500	160	50

Закінчення таблиці 4.3

Реа-льно	151200	90000	57000	-	-	-	-	-

Як ви можете бачити, таблиця 4.3 показує, що кількість імпульсів за 1 годину в деяких випадках набагато вище, ніж це повинно бути.

4.3. Розробка заходів з охорони праці

Під оптимальними мікрокліматичними умовами розуміють сукупність таких характеристик мікроклімату, які забезпечують збереження нормального теплового стану організму без активації механізмів терморегуляції при тривалому і системному впливі на людину. Вони забезпечують тепловий комфорт і створюють передумови для більш високого рівня продуктивності праці. Система контролю мікроклімату повинна бути правильно підібрана з точки зору продуктивності; неправильно підібрана система призводить до коливань внутрішньої температури, що несприятливо для працівників. Вентиляцію робочої зони слід пристосовувати до джерел вологи в приміщенні та час від часу зменшувати, особливо у випадку дуже низької вологості зовнішнього повітря. Постійний моніторинг факторів мікроклімату - це реєстрація даних незайманих може бути корисною для інвестиційних інвестицій у вентиляцію будівель та схвалення.

Основні заходи захисту людини від шкідливого впливу вібрації у виробничих умовах можна поділити на технічні, організаційні, лікувально-профілактичні, колективні та індивідуальні.

Технічні заходи включають:

- зниження вібрації в джерелі її виникнення (вибір на стадії проєктування кінематичних і технологічних схем, що знижують динамічні навантаження в обладнанні та ін.);

- зменшення активної вібрації на шляху поширення від джерела (вібропоглинання, віброгасіння, віброізоляція).

До організаційних заходів відносяться:

- організаційно-технічні (своєчасний ремонт і технічне обслуговування обладнання згідно технологічного регламенту, контроль допустимих рівнів вібрації, дистанційне керування вібронебезпечним обладнанням);

- організаційно-режимні (здійснення відповідного режиму праці та відпочинку, заборона залучення до вібраційної роботи осіб молодше 18 років тощо);

До лікувально-профілактичних заходів відносяться:

- періодичні медичні огляди;

- лікувальні процедури (фізіологічні процедури, вітаміно- та фітотерапія).

На роботах зі шкідливими і небезпечними умовами праці, такими як підвищений рівень шуму, працівникам безкоштовно видаються спеціальні елементи відповідно до встановлених норм, які є обов'язковим мінімумом для безкоштовної видачі роботодавцем засобів індивідуального захисту, що визначають захисні властивості. засобів індивідуального захисту та умови їх використання [29]. Це затверджено наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від 16 квітня 2009 року № 62, зареєстрованим у Міністерстві юстиції України 12 травня 2009 року за № 424/16440.

4.4. Пожежна безпека виробничого приміщення

Пожежна небезпека – можливість виникнення та (або) розвитку пожежі в будь-якій речовині, процесі, стані. Слід зазначити, що пожеж безпечних не буває, якщо вони не створюють прямої загрози життю та здоров'ю людини, то завдають чи призводять до значних матеріальних втрат. Коли людина перебуває в зоні впливу пожежі, вона може потрапити під дію наступних небезпечних та шкідливих факторів:

- токсичні продукти згоряння;

- вогонь;

- підвищена температура середовища;

- дим;

- недостатність кисню;

- руйнування будівельних конструкцій;

- вибухи, закінчення небезпечних речовин, що відбуваються в результаті пожежі;

- паніка.

Метою пожежної безпеки об'єкта є запобігання виникненню пожежі на певному чинними нормативами рівні, а у разі виникнення пожежі – обмеження її поширення, своєчасне виявлення, гасіння пожежі, захист людей та матеріальних цінностей.

Для співробітників дуже важливим є дотримання елементарних правил пожежної безпеки під час перебування на робочому місці (в офісі). Адже безвідповідальне ставлення до таких, здавалося б, дрібниць, як покинутий недопалок або залишений без нагляду електрообігрівач, може спричинити пожежу. Часто спалах відбувається через неправильне зберігання в приміщенні легкозаймистих речовин, спалах електропроводки через перевантаження електромережі, неакуратне поводження з вогнем у місцях приготування їжі.

- меблі та обладнання необхідно розміщувати таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (завширшки не менше 1 м). Евакуаційні шляхи та виходи необхідно постійно утримувати вільними, нічим не захаращувати;

- електромережі, електроприлади та апаратуру експлуатувати лише у справному стані з урахуванням вказівок та рекомендацій підприємств-виробників. У разі виявлення пошкоджень електромереж, вимикачів, розеток та інших електровиробів слід негайно вимкнути їх та вжити необхідних заходів щодо приведення в пожежобезпечний стан;

- документи, папір та інші горючі матеріали слід зберігати на відстані не менше 1 м від електрощитів; 0,5 м від електросвітильників; 0,6 м від сповіщувачів автоматичної пожежної сигналізації та 0,15 м від пристроїв центрального водяного опалення.

- засоби протипожежного захисту слід утримувати у справному стані.

Усі працівники повинні вміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння, знати місце знаходження.

Відстань від найбільш віддаленого місця приміщення до місця розташування вогнегасника має перевищувати 20 м.

У службових приміщеннях не допускати:

- будову тимчасових електромереж;

- прокладання електричних проводів безпосередньо на горючій основі;

- Експлуатація електроприладів, що мають механічні пошкодження;

- захаращення підступів до засобів пожежогасіння;

- куріння, використання легкозаймистих рідин;

- проведення вогневих, зварювальних та інших робіт без спеціального дозволу;

- включення електронагрівальних приладів (чайників, кип'ятильників тощо) без негорючих підставок та в тих місцях, де їх використання не передбачено (або заборонено);

- захаращення шляхів евакуації та евакуаційних виходів.

Адміністрація має зобов'язати відповідального за протипожежний стан службових приміщень після закінчення роботи:

- оглядати приміщення, переконуватись у відсутності порушень, які можуть призвести до пожежі;

- перевіряти, щоб усюди було вимкнено освітлення, електроживлення приладів та обладнання (за винятком електрообладнання, яке за вимогами технології має працювати цілодобово).

У випадку, якщо пожежі не вдалося уникнути, необхідно:

- терміново повідомити пожежну охорону за телефоном 101, зазначити адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище;

- організувати евакуацію людей та матеріальних цінностей;

- повідомити про виникнення пожежі адміністрації та чергову (за її наявності);

- відключити, при необхідності, струмоприймачі та вентиляцію;

- розпочати гасіння пожежі наявними первинними засобами пожежогасіння;

- організувати зустріч підрозділів пожежної охорони та надати їм консультаційну та іншу допомогу у процесі гасіння пожежі.

4.5. Розробка інструкції з охорони праці для інженера голосових платформ (VoIP інженера)

Орієнтовна інструкція з охорони праці для інженера голосових платформ (VoIP інженера):

1. **Загальні вимоги безпеки при роботі з ноутбуком та іншою оргтехнікою.**

1.1. Інструкція розроблена на основі ДНАОП 0.00-8.03-93 "Порядок обробки та затвердження власником нормативних актів про охорону праці, що діють на підприємстві", "Положення про розроблення інструкцій з охорони праці", ДНАОП 0.00-4.12-99 "Типові положення про навчання охорони праці, Наказ Міністерства соціальної політики України 14.02.2018 № 207 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями.

1.2. За цією інструкцією користувач персонального комп'ютера інструктується перед початком роботи (первинний інструктаж), а потім через кожні 6 місяців (повторний інструктаж).

Результати інструктажу заносяться до «Журналу реєстрації інструктажів з питань охорони праці», у журналі після проходження інструктажу має бути підпис інструктируючого та користувача.

1.3. Користувач повинен:

1.3.1. Дотримуватись правил внутрішнього трудового розпорядку.

1.3.2. Не допускати до робочої зони сторонніх осіб.

1.3.3. Не виконувати вказівки, що суперечать правилам охорони праці.

1.3.4. Пам'ятати про особисту відповідальність за виконання правил охорони праці та безпеку працівників.

1.3.5. Вміти надавати першу медичну допомогу постраждалим від нещасних випадків.

1.3.6. Вміти користуватись первинними засобами пожежогасіння.

1.3.7. Дотримуватись правил особистої гігієни.

1.4. Основні небезпечні та шкідливі виробничі фактори, які можуть вплинути на користувача:

а) фізичні:

- нерівномірність розподілу яскравості у полі зору;

- ураження електричним струмом;

б) психофізіологічні:

- напруга зору;

- напруга уваги;

- Інтелектуальні навантаження;

- емоційні навантаження;

- монотонність праці;

1.5. Освітлювальні установки повинні забезпечувати рівномірне освітлення та не повинні утворювати сліпучих відблисків на клавіатурі, а також на екрані монітора у напрямку очей.

1.6. При роботі з ноутбуком та іншою оргтехнікою не допускається розташування робочого місця у приміщеннях без природного освітлення, без наявності природної чи штучної вентиляції.

1.7. Робоче місце з комп'ютером і оргтехнікою має розміщуватися з відривом щонайменше 1м від стіни, від стіни з віконними отворами - з відривом щонайменше 1,5м.

1.8. Кут нахилу екрана монітора чи ноутбука по відношенню до вертикалі має становити 10-15 градусів, а відстань до екрана – 500-600 мм.

1.9. Кут зору екрану має бути прямим і складати 90 градусів.

1.10. Для захисту від прямих сонячних променів повинні передбачатися сонцезахисні пристрої (плівка з металізованим покриттям, регульовані жалюзі з вертикальними панелями та ін.).

1.11. Висвітлення має бути змішаним (природним та штучним).

1.12. Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість при розміщенні екрана, клавіатури, документів та відповідного обладнання.

1.13. Робоче крісло має бути стійким і дозволяти працівникові з екранними пристроями легко рухатися та займати зручне положення.

1.14. У приміщенні кабінету та на робочому місці необхідно підтримувати чистоту та порядок, проводити систематичне провітрювання.

1.15. Про всі виявлені під час роботи несправності обладнання необхідно доповісти безпосередньому керівнику.

1.16. Про нещасний випадок очевидець, який виявив його працівника або сам потерпілий, повинні доповісти безпосередньо керівнику установи та вжити заходів щодо надання медичної допомоги.

1.17. Особи, винні у порушенні вимог цієї інструкції, притягуються до дисциплінарної відповідальності відповідно до чинного законодавства.

2. **Вимоги безпеки перед початком роботи з комп'ютером (ноутбуком) та іншою оргтехнікою.**

2.1. Оглянути та переконатися у справності обладнання. У разі виявлення несправності роботи не приступати. Повідомити про це керівника і лише після усунення несправності та його вирішення, розпочати роботу.

2.2. Перевірити освітлення робочого місця за необхідності вжити заходів для його нормалізації.

2.3. Перевірте наявність та надійність захисного заземлення обладнання.

2.4. Перевірте стан електричного шнура та вилки.

2.5. Перевірити справність вимикачів та інших органів керування персональним комп'ютером та оргтехнікою.

2.6. Ретельно провітрити приміщення з персональним комп'ютером та оргтехнікою.

2.7. Включити ПК та перевірити стабільність та чіткість зображення на екрані, переконатися у відсутності запаху диму від комп'ютера та оргтехніки.

3. **Вимоги безпеки під час роботи з комп'ютером, ноутбуком, принтером, ксероксом, сканером іншою оргтехнікою.**

3.1. Вмикайте та вимикайте ноутбук та іншу оргтехніку тільки вимикачами, забороняється виключати витягування вилки з розетки.

3.2. Забороняється знімати захисні пристрої та працювати без них.

3.3. Не допускати до комп'ютера та оргтехніки сторонніх осіб, які не беруть участь у роботі.

3.4. Забороняється переміщати та переносити ноутбук, принтер, будь-яке обладнання, що знаходиться під напругою.

3.5. Забороняється під час роботи пити будь-які напої, приймати їжу.

3.6. Забороняється фізичне втручання у пристрій ноутбука, принтера, сканера, ксероксу під час їх роботи.

3.7. Забороняється залишати увімкнене обладнання без нагляду.

3.8. Забороняється класти предмети на комп'ютерне обладнання, монітори, екрани та оргтехніку.

3.9. Строго виконувати загальні вимоги щодо електробезпеки та пожежної безпеки.

3.10. При усуненні стрижки паперу на ксероксі або принтері, щоб уникнути ураження електрострумом, необхідно відключити обладнання від електромережі. Необхідно також вимикати обладнання від мережі при тривалому простої.

3.11. Самостійно розбирати та проводити ремонт електронної та електронно-механічної частини комп'ютера, периферійних пристроїв, оргтехніки категорично забороняється. Ці роботи може виконувати лише спеціаліст або інженер з технічного обслуговування комп'ютерної техніки.

3.12. Сумарний час безпосередньої роботи з персональним комп'ютером та іншою оргтехнікою протягом робочого дня має бути не більше 6 годин.

3.13. Тривалість безперервної роботи з персональним комп'ютером та іншою оргтехнікою без регламентованої перерви не повинна перевищувати 2 години. Через кожну годину роботи слід робити перерву тривалістю 15 хв.

3.14. Під час регламентованих перерв з метою зниження нервово-емоційної напруги, втоми зорового аналізатора, усунення впливу гіподинамії та гіпокінезії, запобігання розвитку познотонічної втоми слід виконувати комплекси вправ для очей або організовувати фізкультурні паузи.

3.15. Комп'ютер, будь-які його периферійні пристрої, оргтехніку необхідно використовувати у відповідності з експлуатаційною документацією до них.

3.16. При виконанні роботи потрібно бути уважним, не звертати уваги на сторонні речі.

3.17. Про всі виявлені несправності та збої в роботі апаратури необхідно повідомити безпосередньо інженера з обслуговування комп'ютерної техніки.

4. **Вимоги безпеки після закінчення роботи з ноутбуком та іншою оргтехнікою.**

4.1. Вимкніть оргтехніку від електромережі, для чого необхідно відключити тумблери, а потім акуратно витягнути штепсельні вилки з розетки.

4.2. Протерти зовнішню поверхню комп'ютера чистою вологою тканиною. При цьому не допускайте використання розчинників, одеколону, препаратів в аерозольній упаковці.

4.3. Забрати робоче місце.

4.4. Ретельно провітрити приміщення з персональним комп'ютером та іншою оргтехнікою.

5. **Вимоги техніки безпеки та безпеки життєдіяльності в аварійних ситуаціях при роботі з комп'ютером та іншою оргтехнікою.**

5.1. Якщо на металевих частинах обладнання виявлено напругу (відчуття струму), заземлюючий провід обірвано, необхідно вимкнути обладнання, негайно доповісти керівнику про несправності електрообладнання і без його вказівки до роботи не починати.

5.2. У разі припинення подачі електроенергії вимкнути обладнання.

5.3. При появі незвичайного звуку, запаху паленого, мимовільного відключення комп'ютера та оргтехніки, негайно припинити роботу і повідомити керівника.

5.4. У разі виникнення пожежі негайно вимкнути обладнання, знеструмити електромережу за винятком освітлювальної мережі, повідомити про пожежу всім працюючим і розпочати гасіння вогнища пожежі наявними засобами пожежогасіння.

5.5. При нещасному випадку необхідно, перш за все, звільнити потерпілого від травмуючого фактора, викликати екстрену медичну допомогу за номером 103, зберегти наскільки можна місце травмування в тому стані, в якому воно було на момент травмування. При звільненні постраждалого від дії електроструму слідкуйте за тим, щоб самому не опинитися в контакті з струмопровідною частиною та під напругою [15].

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

5.1. Дата-центри та викиди парникових газів

Парниковий газ (ПГ) – це будь-які газоподібні сполуки, які поглинають інфрачервоне випромінювання, утримують тепло в атмосфері та сприяють виникненню парникового ефекту. Відповідно до «Рамкової конвенції про зміну клімату» та «Кіотського протоколу» існує шість основних парникових газів: двоокис вуглецю (CO2); метан (CH4); перфторвуглеці (ПФВ); гідрофторвуглеці (ГФВ); закис азоту (N2O); Гексафторид сірки (SF6).

Відповідно до Протоколу з парникових газів та ISO 14064 існує три категорії викидів парникових газів, включаючи Scope1, Scope2 та Scope3 (як показано на малюнку 5.1).

• Scope1 – Прямі викиди ПГ: усі прямі викиди, що знаходяться під оперативним контролем організації.

• Scope2 – Непрямі викиди парникових газів, пов'язані з енергетикою: Непрямі викиди, що виникають внаслідок покупної електроенергії, тепла, пари або охолодження.

• Scope3 – Інші непрямі викиди ПГ: Інші непрямі викиди з таких джерел, як ділові поїздки, управління відходами та виробничо-збутовий ланцюжок.

Викиди категорії 1 розрахувати найпростіше, тоді як дані категорії 3 отримати важче. Викиди вуглецю категорії 2, як правило, можуть бути здійснені вашою комунальною компанією. Згідно з дослідженням Carbon Intelligence, понад 80% викидів компанії належать до категорії 3. Але для енергоємних дата-центрів викиди категорії 3 наближаються до 50% протягом терміну служби дата-центру. Оскільки дані області охоплення 3 все ще перебувають у стадії розробки, її визначено як провідну метрику.

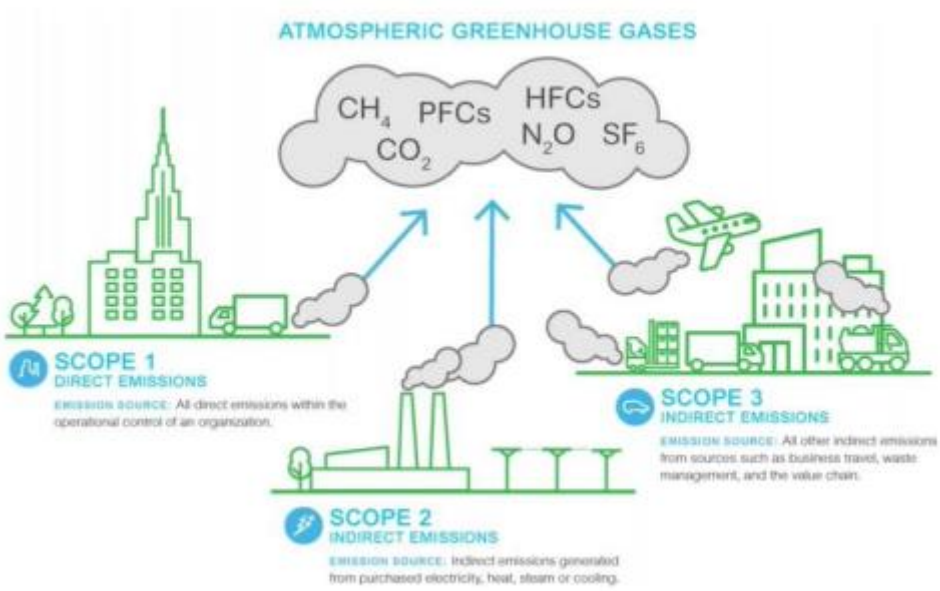

Рис. 5.1. 3 категорії викидів ПГ від організації

Виходячи з перелічених вище категорій, викиди ПГ від дата-центру пов'язані не тільки з їх власною діяльністю та споживанням електроенергії, але і з придбанням товарів. Викиди ПГ (Область охоплення 3) можуть включати непрямі викиди з таких джерел, як поїздки, керування відходами та ланцюжок створення вартості дата-центру.

Наприклад, викиди можуть включати будівництво дата-центра (купівля товарів та послуг); поїздки співробітників на роботу (автомобілі, автобуси тощо); ділові поїздки (літак, поїзд, оренда автомобілів, готелі тощо).

5.2. П'ять категорій показників, що використовуються для встановлення цілей

У міру того, як світ стає все більш автоматизованим та цифровим, індустрія дата-центрів переживає швидке зростання, щоб підтримати цю трансформацію. В результаті в центрі уваги опинилися питання енергоспоживання та загальної екологічної стійкості. Оператори дата-центрів беруть на себе зобов'язання щодо забезпечення стійкості у межах своїх екологічних, соціальних і управлінських програм (ESG).

На рисунку 5.2 показаний типовий процес покращення екологічної стійкості. Пропонується п'ять категорій показників для операторів дата-центрів, щоб встановити цілі екологічної стійкості відповідно до унікальних характеристик дата-центрів. Також є список стандартизованих, добре зрозумілих метрик з визначеннями та додатками для кожної категорії для вимірювання прогресу. Також визначено список найбільш відповідних структур та стандартів сталого розвитку для керівництва щодо встановлення цілей, звітності та сертифікації.

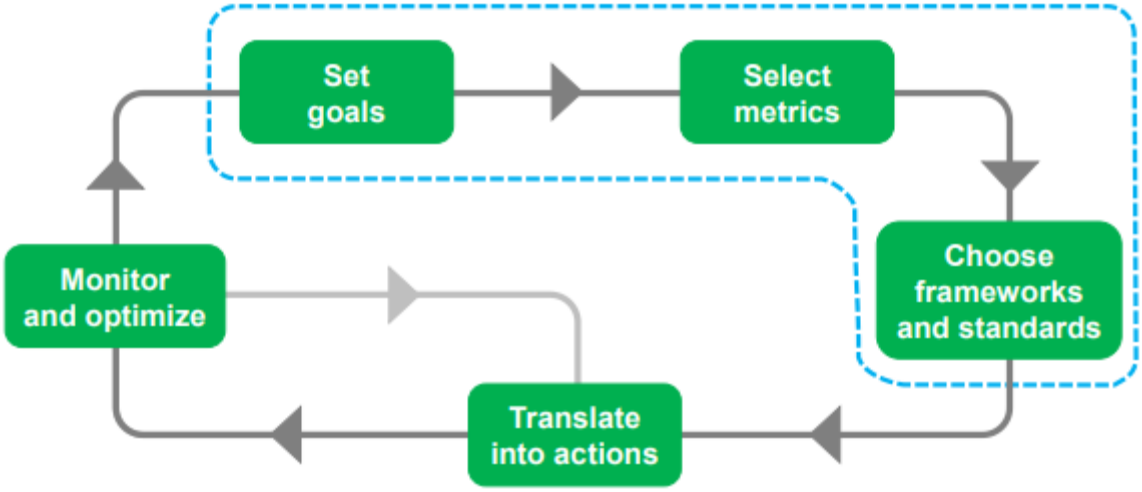

Рис. 5.2. Кроки оптимізації стійкості центру обробки даних

Визначено 23 показники стійкості, які застосовуються до ЦОД, за п'ятьма категоріями показників. Ці категорії являють собою цілісний підхід до вирішення проблеми екологічної стійкості. Опис кожної з цих категорій:

• Енергія. За деякими оцінками, споживання енергії у дата-центрах становить 1-2% від загальносвітового енергоспоживання, це найбільший ресурс, який використовують ДЦ. Швидке зростання, що продовжується, і прогнозоване майбутнє зростання ДЦ роблять енергоспоживання та ефективність важливим напрямом на шляху сталого розвитку ДЦ. На додаток до скорочення споживання за рахунок ефективної роботи використання відновлюваних джерел енергії допомагає скоротити викиди парникових газів (ПГ), представлені в споживанні електроенергії. Звіти про споживання енергії, енергоефективність та використання відновлюваних джерел енергії важливі для

операторів ДЦ, щоб показати їх прогрес у зусиллях з мінімізації свого вуглецевого сліду.

• Викиди парникових газів (ПГ) – CO2 та інші гази, такі як CH4, ПФУ, ДФУ, класифікуються як парникові гази. Ці викиди парникових газів, також звані «викидами вуглецю», роблять основний внесок у зміну клімату і є однією з найнагальніших проблем, які стоять сьогодні перед суспільством. Відповідно до Протоколу з викидів парникових газів та ISO 14064 існує три категорії викидів парникових газів: обсяг 1, обсяг 2 та обсяг 3. Звітність про викиди парникових газів важлива для операторів ДЦ, щоб продемонструвати свої зусилля щодо боротьби зі зміною клімату.

• Вода. Градирні та інші методи випарного охолодження є популярними рішеннями щодо відведення тепла для ДЦ через їх високу ефективність та велику холодопродуктивність. Однак механізмом відведення тепла у цих технологіях охолодження є випаровування, на яке витрачається значна кількість води. Дослідження Uptime Institute показало, що центр обробки даних потужністю 1 МВт із традиційними методами охолодження використовує близько 25 мільйонів літрів води на рік. Крім того, традиційне виробництво електроенергії потребує великої кількості води, що набагато більше, ніж води, яка використовується для охолодження ДЦ. Звіт про світовий розвиток водних ресурсів від Організації Об'єднаних Націй показав, що використання води для виробництва електроенергії було вчетверо більше, ніж використання води для охолодження на місці. Райони з дефіцитом води привернули до себе особливу увагу з боку місцевих органів влади. Використання регенерованої або оборотної води замість прісної води допомагає знизити навантаження на місцеві водні ресурси. Звітність про використання води стає все більш важливою для операторів центрів обробки даних як частина їх загальних цілей сталого розвитку.

• Відходи. Під час будівництва та експлуатації ДЦ виробляють значну кількість відходів. Мінімізація утворення відходів у ланцюжку поставок та видалення відходів зі звалищ за рахунок повторного використання та переробки є ключовою стратегією підвищення екологічної стійкості. Методології та процеси проєктування економіки замкнутого циклу підтримують поліпшення у цій галузі. Звітність про утворення та

перенаправлення відходів набуває все більшого значення і, ймовірно, стане звичайним явищем у найближчому майбутньому.

• Земля та біорізноманіття. ДЦ мають прямий вплив на землю, на якій вони побудовані, і опосередкований вплив на землю з боку ланцюжка поставок. У порівнянні із загальною площею, що займають комерційні офісні будівлі, ДЦ займають відносно невелику площу. Однак для ДЦ з виділеними сонячними/вітряними електростанціями вплив на землю та біорізноманіття може бути значним для окремих організацій. Вимір впливу на землю та біорізноманіття поширене в таких галузях, як гірничодобувна промисловість, але є новим для індустрії ДЦ.

5.3. Рекомендовані показники для звітності щодо сталого розвитку

Було відібрано та рекомендовано 23 показники на основі наступних восьми правил:

• Актуально та важливо для центрів обробки даних;

• Відбиває вплив на довкілля прямо чи опосередковано;

• Простота реалізації (тобто доступність даних, розрахунок);

• Простота спілкування всередині організацій;

• Простота порівняльного аналізу у різних організаціях;

• Практичний (може бути легко перетворений на дії з поліпшення);

• Застосовується до всіх географічних регіонів (тобто регіонів, країн тощо);

• Стандартизовано та може бути визначено кількісно.

Дотримуючись цих правил, було визначено 23 ключові показники, за якими оператори ДЦ повинні повідомляти про екологічну стійкість у цілісній формі (як показано на рисунку 5.3). Оператори ДЦ повинні використовувати ці показники для встановлення цілей та демонстрації прогресу (наприклад, за роками).

Ці показники мають бути зібрані, виміряні або розраховані на основі кількох точок даних протягом звітного періоду (дванадцятимісячний період).

Metric categories	Key metrics	Units	Recommendations		
			Beginning (11)	Advanced (18)	Leading (23)
Energy (5)	• Total energy consumption	kWh	✓	✓	✓
	• Power usage effectiveness (PUE)	Ratio	✓	✓	✓
	• Total renewable energy consumption	kWh	✓	✓	✓
	• Renewable energy factor (REF)	Ratio		✓	✓
	• Energy Reuse Factor (ERF)	Ratio			✓
GHG emissions (9)	• GHG emissions: (Scope 1)	$mtCO_2e$	✓	✓	✓
	• Location-based GHG emissions: (Scope 2)	$mtCO_2e$	✓	✓	✓
	• Market-based GHG emissions: (Scope 2)	$mtCO_2e$	✓	✓	✓
	• GHG emissions: (Scope 3)	$mtCO_2e$			✓
	• Location-based carbon intensity (Scope 1+ Scope 2)	$mtCO_2e/kWh$	✓	✓	✓
	• Market-based carbon intensity (Scope 1+ Scope 2)	$mtCO_2e/kWh$	✓	✓	✓
	• Carbon usage effectiveness (CUE)	$mtCO_2e/kWh$	✓	✓	✓
	• Total carbon offsets	$mtCO_2e$		✓	✓
	• Hour-by-hour supply and consumption matching	TBD			✓
Water (4)	• Total site water usage	m^3	✓	✓	✓
	• Total source energy water usage	m^3		✓	✓
	• Water usage effectiveness (WUE)	m^3/kWh	✓	✓	✓
	• Total water use in supply chain	m^3			✓
Waste (4)	• Total waste generated	tons		✓	✓
	• Waste landfilled	tons		✓	✓
	• Waste diverted	tons		✓	✓
	• Waste diversion rate	Ratio		✓	✓
Land & biodiversity (1)	• Mean species abundance (MSA)	MSA/km^2			✓

$mtCO_2e$ = Metric tons of carbon dioxide equivalent

Рис. 5.3. 23 метрики для звітності про екологічну стійкість

5.4. Вибір правильних шаблонів та стандартів для посібника

Шаблони та стандарти використовуються, щоб допомогти організаціям вимірювати та повідомляти про стійкість. Шаблони містять загальні рекомендації і, як правило, не є обов'язковими, тоді як стандарти можуть бути прийняті юрисдикціями та стати обов'язковими.

Шаблон сталого розвитку може бути заплутаним та складним. Було визначено 17 найбільш відповідних систем та стандартів сталого розвитку для ДЦ по всьому світу (як показано на рисунку 5.4). Оператори ДЦ можуть використовувати їх як посібник зі стандартизації звітності з екологічної стійкості.

Applications	Frameworks and standards	Spectrum	Attributes
Target setting (4)	• UN Sustainability Development Goals (SDGs) • Science-Based Targets Initiative (SBTi) • RE100 • CE100	• Leaders setting sustainability goals • Corporate emissions • Power footprint • Circular economy	Call for action Initiative Initiative Programme
Reporting (9)	• Sustainability Accounting Standards Board (SASB) • Carbon Disclosure Project (CDP) • Global Reporting Initiative (GRI) • Dow Jones Sustainability Indices (DJSI) • Global Real Estate Sustainability Benchmark (GRESB) • Task Force on Climate-related Financial Disclosures (TCFD) • GHG Protocol Accounting and Reporting Standard • ISO/IEC 30134: Information technology- Data centers - Key performance indicators • ISO 14604: GHG Emissions Inventories and Verification	• Corporate ESG indicators • Corporate GHG emissions, water • Climate Change, ESG indicators • Corporate ESG indicators • ESG Benchmark for Real Assets • Corporate climate-related financial • Corporate emissions • Data center operation resource efficiency • Corporate emissions and removals	Standard Framework Framework Benchmark Benchmark Framework Standard Standard Standard
Certifying (4)	• Leadership in Energy and Environmental Design (LEED) • ENERGY STAR • ISO 50001: Energy Management System • Building Research Establishment Environmental Assessment Method (BREEAM)	• Corporate Building Energy Use • Energy use in buildings and plants • Corporate Energy Use • Built Environment Assets	Rating system Framework Standard Standard

Рис. 5.4. 17 найбільш відповідних систем та стандартів сталого розвитку

Ці структури можуть бути згруповані в наступні три категорії залежно від їхньої функції або призначення:

• Постановка цілей: ці шаблони використовуються для встановлення надійних, науково обґрунтованих та реалістичних цілей у сфері сталого розвитку. Цілі можуть бути внутрішніми або опублікованими ззовні. Наприклад, система цілей ООН у сфері сталого розвитку (ССР) включає 17 конкретних цілей, які є закликом до дії для всіх країн щодо сприяння процвітанню та захисту планети. Це чудове джерело для організацій, щоб встановити внутрішні цілі.

• Звітність. Подібно до фінансової звітності, оператори ДЦ можуть використовувати ці схеми як керівництво для надання якісної та кількісної нефінансової інформації для оцінки своїх показників сталого розвитку. Наприклад, проєкт Carbon Disclosure Project (CDP) — популярна структура, яка допомагає великим компаніям інтегрувати інформацію про довкілля та наслідки для бізнесу у фінансову звітність.

• Сертифікація. Ці схеми надають організаціям кошти на сертифікацію своїх поліпшень у сфері сталого розвитку шляхом виконання мінімальної кількості вимог

чи балів. Наприклад, LEED - це добре відома рейтингова система будівель для оцінки екологічних характеристик та заохочення сталого проєктування.

Навіть менший список може бути непосильним для деяких ДЦ. У цих випадках рекомендовано використовувати послуги сторонніх консультантів, які мають досвід роботи в галузі сталого розвитку, бажано з досвідом роботи в ДЦ. Існує матриця, що показує взаємозв'язок між показниками, структурами та стандартами, як показано на рисунку 5.5.

Metric categories	Key metrics	Recommended frameworks/standards
Energy (5)	• Total energy consumption • Power usage effectiveness (PUE) • Total renewable energy consumption • Renewable energy factor (REF) • Energy Reuse Factor (ERF)	• SASB • ISO/IEC 30134-2 • RE100 • ISO/IEC 30134-3 • ISO/IEC 30134-6
GHG emissions (9)	• GHG emissions: (Scope 1) • Location-based GHG emissions: (Scope 2) • Market-based GHG emissions: (Scope 2) • GHG emissions: (Scope 3) • Location-based carbon intensity (Scope 1+ Scope 2) • Market-based carbon intensity (Scope 1+ Scope 2) • Carbon usage effectiveness (CUE) • Total carbon offsets • Hour-by-hour supply and consumption matching	• GHG Protocol or ISO 14064 • GHG Protocol or ISO 14064 • GHG Protocol or ISO 14064 • GHG Protocol or ISO 14064 • GHG Protocol or ISO 14064 • GHG Protocol or ISO 14064 • ISO/IEC 30134-8 • N/A, see a White Paper on this topic. • No frameworks or standards available
Water (4)	• Total site water usage • Total source energy water usage • Water usage effectiveness (WUE) • Total water use in supply chain	• ISO/IEC 30134-9 • No frameworks or standards available • ISO/IEC 30134-9 • No frameworks or standards available
Waste (4)	• Total waste generated • Waste landfilled • Waste diverted • Waste diversion rate	• GRI 300: Environmental - 306 • GRI 300: Environmental - 306 • GRI 300: Environmental - 306 • GRI 300: Environmental - 306
Land & biodiversity (1)	• Mean species abundance (MSA)	• N/A, see a White Paper on this topic.

Рис. 5.5. Матриця між 23 ключовими показниками, шаблонами та стандартами

Перш ніж компанія зможе поставити цілі або впровадити ESG у свою бізнес-стратегію та діяльність, вона має вирішити, як вимірювати показники та складати звіти щодо них. Визначення показників екологічної стійкості, які має відслідковувати бізнес ДЦ, є однією з найважливіших проблем, з якими він стикається. Зростання тиску з боку інвесторів, регулюючих органів, акціонерів, клієнтів і співробітників вимагає більшої прозорості звітності про вплив на довкілля діяльності їх ДЦ. Прозорість,

заснована на метриках, може підвищити внутрішню цінність, відстежуючи та повідомляючи про показники стійкості, щоб допомогти вносити поліпшення, та зовні, повідомляючи про показники стійкості, щоб допомогти підвищити прозорість для заінтересованих сторін.

Не всі компанії ДЦ знаходяться на тому самому етапі свого шляху, тому виділяють 23 показники для трьох етапів звітності: початковий, просунутий і провідний.

Початковий рівень є базовою звітністю щодо використання енергії та води, а також щодо викидів парникових газів. Початковий рівень містить основні показники, необхідні кожної компанії. На просунутому рівні до початкового рівня додаються докладніші показники енергії, води та парникових газів, а також додається нова категорія відходів. Провідний етап додає ще більше деталей до існуючих категорій та вводить категорію землі та біорізноманіття. Рекомендується враховувати ці показники на кожному рівні для компаній, щоб максимально чітко уявити свою екологічну стійкість та відповідати вимогам галузі [14].

ВИСНОВКИ

У роботі було досліджено проблематики сучасної медицини та шлях їх вирішення через концепцію Smart hospital. У майбутньому створення ситуаційного диспетчерського центру розумної лікарні на базі запропонованих технологій та розвиток розумного міста допоможуть втілювати в життя концепції проєктів:

• «Алгоритм Зелена Хвиля»: управління дорожньою інфраструктурою міста для своєчасного надання допомоги екстреним службам у кризових ситуаціях та ухвалення рішення про активацію алгоритму, адже він є дієвим, але ресурсозатратним;

• Використання віртуальної реальності у ситуаційних центрах для швидкої координації працівників під час вирішення екстрених ситуацій (теракт, техногенна катастрофа тощо).

Дані проєкти не підлягають детальному розгляду у роботі, оскільки вимагають залучення концепцій розумного міста та змін на законодавчому рівні, проте існують як логічний розвиток цієї концепції.

Таким чином, використання технологій Big Data та мовної аналітики у поєднанні з системою E-health допоможуть відображати необхідні дані, що знаходяться у реєстрах установ, та підказувати працівникам оптимальні алгоритми взаємодії, будуючи причинно-наслідковий зв'язок, відображаючи картину подій у повному, необхідному розрізі, аналізуючи прийняті рішення та коригуючи їх наступного разу.

Системи класу екстреного реагування мають бути високоточними, швидкодіючими та оснащуватись заходами підвищеного рівня безпеки.

Розглянуті приклади можливих атак на систему телефонії досліджувалися на основі реальних позаштатних ситуацій працівників телекомунікаційної сфери, що інтерв'юються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zabbix: мониторим всё подряд (на примере Redis'a) [Електронний ресурс]. – 2020. – Режим доступу: https://habr.com/ru/post/485538/ (дата звернення 06.06.2021 р.) – Назва з екрана.

2. Corezoid process engine. Введение [Електронний ресурс]. – 2019. – Режим доступу: https://doc.corezoid.com/v2/docs/protocol-description-v2 (дата звернення 06.06.2021 р.) – Назва з екрана.

3. Big Data (Великі дані) [Електронний ресурс]. – 2018. – Режим доступу: https://www.it.ua/knowledge-base/technology-innovation/big-data-bolshie-dannye (дата звернення 06.06.2021 р.) – Назва з екрана.

4. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма MapReduce [Електронний ресурс]. – 2015. – Режим доступу: https://habr.com/ru/post/267361/ (дата звернення 06.06.2021 р.) – Назва з екрана.

5. Меггелен Дж. Asterisk: будущее телефонии, 2-е издание / Дж. Меггелен, Л. Мадсен, Дж. Смит – СПб: Символ-Плюс, 2009. – 656 с.

6. Платов М. Asterisk и Linux – миссия IP-телефония / М. Платов – 2005 г. - № 31. – С. 12-19.

7. Платов М. Asterisk и Linux: миссия IP-телефония. Действие 2 / М. Платов – 2005 р. - № 32. – С. 32-38.

8. База знаний Asterisk [Електронний ресурс] – Режим доступу: asterisk.ru/knowledgebase (дата звернення 06.06.2021 р.) – Назва з екрана.

9. ХабрХабр. Безопасность в VoIP сетях [Електронний ресурс] — Режим доступу: habrahabr.ru/post/145206 (дата звернення 06.06.2021 р.) – Назва з екрана.

10. Росляков А.В. IP-телефония / А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева – М.: Эко-Трендз, 2003. -252 с.

11. Гольдштейн Б.С. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий – М.: Радио и связь, 2001. -336 с.

12. CITForum. Безопасность IP-телефонии – полевые зарисовки. А. Веселов [Електронний ресурс] — Режим доступу: citforum.ru/security/articles/ipsec (дата звернення 06.06.2021 р.) – Назва з екрана.

13. Распознавание речи [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/226143/ (дата звернення 06.06.2021 р.) – Назва з екрана.

14. Lin P. Guide to Environmental Sustainability Metrics for Data Centers / Paul Lin, Robert Bunger – Schneider Electric, 2018, -67 с.

15. ІНСТРУКЦІЯ №8 З ОХОРОНИ ПРАЦІ ПРИ РОБОТІ З НОУТБУКОМ ТА ІНШОЮ ОРГТЕХНІКОЮ [Електронний ресурс]. – 2020. – Режим доступу: https://docs.google.com/document/d/1H5eEKmnPTmpt-EDh2ELh4uO8HyZIlX_z/edit?usp=sharing&ouid=102328814915979090980&rtpof=true&sd=true (дата звернення 11.11.2022 р.) – Назва з екрана.

16. Big Data Analysis Techniques [Електронний ресурс]. – 2019. – Режим доступу: https://www.getsmarter.com/blog/career-advice/big-data-analysis-techniques/ (дата звернення 11.11.2022 р.) – Назва з екрана.

17. Андреєва А. Інформаційно-комунікаційне забезпечення концепції "Розумна лікарня" – 2021. -50 с.