МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет комп'ютерних наук та технологій
(повне найменування інституту, факультету)

Кафедра комп'ютерних систем та мереж
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)
бакалавра
(ступінь вищої освіти (освітній ступінь))

на тему **РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ**

Виконав: студент 4 курсу, групи КНТ-518сп спеціальності
123 «Комп'ютерна інженерія»
(код і найменування спеціальності)
Освітня програма (спеціалізація)
«Комп'ютерна інженерія»

Білоусов Вадим Віталійович
(прізвище та ініціали)
Керівник Ільяшенко М.Б.
(прізвище та ініціали)
Рецензент Морщавка С.В.
(прізвище та ініціали)

м. Запоріжжя
2021 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Інститут, факультет інформатики та радіоелектроніки, комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти (освітній ступінь) бакалаврський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)

Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри Кудерметов Р.К.
_____ _____
" " _____ 2021 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТА

Білоусов Вадим Віталійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка системи моніторингу комп'ютерної мережі

керівник проекту (роботи) Ільяшенко Матвій Борисович, к. т. н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "17" березня 2021 року № 81
2. Строк подання студентом проекту (роботи) 06 травня 2021 року
3. Вихідні дані до проекту (роботи) архітектура ЦОД, вимоги до умов експлуатації ЦОД, функціональні характеристики систем електронних сповіщень .

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ; дослідження предметної області використання боту; аналіз існуючих засобів та вибір найкращих варіантів для системи моніторингу і диспетчеризації; розробка Telegram боту для моніторингу поточного стану серверної кімнати

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
Принцип роботи системи;
Основні характеристики месенджерів;
Налаштування Zapier;
Результати роботи.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата: завдання видав	Підпис, дата: прийняв виконане завдання
1-3	Ільяшенко М.Б., к. т. н., доцент		
	Бесєдін О.В. асист.		

7. Дата видачі завдання 01.03.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примі
1	Проведення консультацій з науковим керівником щодо виконання дипломної роботи	01.03.2021 р.	
		15.03.2021 р.	
		20.03.2021 р.	
2	Огляд літературних джерел	01.04.2021 р.	
3	Дослідити предметну область використання Telegram боту	10.04.2021 р.	
		15.04.2021 р.	
4	Розробити Telegram бот для моніторингу поточного стану серверної кімнати	20.04.2021 р.	
5	Оформлення пояснювальної записки та ілюстративного матеріалу.	01.05.2021 р.	

Студент _____ **В.В.Білоусов**
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **М.Б.Ільяшенко**
(підпис) (ініціали та прізвище)

РЕФЕРАТ

ПЗ: 71 стор. 38 рис., 2 табл., 6 джерел.

ЦЕНТРИ ОБРОБКИ ДАНИХ, МОНІТОРИНГ, МЕСЕНДЖЕР, БОТ, КОНТРОЛЬ ПАРАМЕТРІВ, СЕРВЕРНА

Об’єкт дослідження: процес моніторингу фізичних умов центру обробки даних

Предмет дослідження: архітектура ЦОД, вимоги до умов експлуатації обладнання ЦОД, характеристики існуючих систем передачі електронних сповіщень, програма боту моніторингу фізичних умов серверного приміщення.

Мета роботи: розробка найкращого засобу цілодобового моніторингу поточного стану фізичних умов серверного приміщення ЦОД, та засобу сповіщення про критичні ситуації.

Методи дослідження: логічний аналіз інформації про існуючі засоби моніторингу, ознайомлення з доступним теоретичним матеріалом; порівняльний аналіз і вибір найкращих компонентів; програмування, налаштування та експериментальне дослідження розробленої системи .

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

ЦОД – центр обробки даних.

РМА - робоче місце адміністратора.

ПК - персональний комп'ютер.

ІТ - інформаційні технології

ASHRAE - Американське товариство інженерів з опалення, охолодження та кондиціювання повітря.

ДБЖ - Джерело безперебійного живлення.

АУГП - автоматична установка газового пожежогасіння.

ООР – область основної розводки.

ОГР – область горизонтальної розводки.

ОЗР - область зонової розводки.

ОРО - область розводки обладнання.

АСДУ - автоматизована система диспетчеризації та управління.

API - інтерфейс прикладного програмування

ВСТУП

У сучасному світі для нормальної роботи підприємств необхідне серверне обладнання, де зберігаються і накопичуються дані діяльності компанії. Усе серверне обладнання розташовують в одному приміщенні з усіма необхідними для нього умовами. У випадку несправностей в обладнанні порушується нормально роботи частково або всієї компанії. Під час робочого дня несправності виявити швидко, але якщо збій виник у неробочий час коли нікого немає, і якщо при цьому має здійснюватися який-небудь процес, що запускається автоматично по розкладу, то несправність буде виявлена пізно і робота процесу не буде виконана. Причини несправностей можуть бути різноманітні, але, як правило, перед виникненням несправностей відбувається порушення режиму роботи обладнання або інших подій, які можна відслідкувати.

Для підтримання роботи в штатному режимі, для попередження і ліквідації надзвичайних ситуацій, а також для збору даних про технологічні процеси в серверному приміщенні необхідно створити систему автоматичного моніторингу і диспетчеризації. Дана система повинна вирішувати наступні задачі:

- слідкувати за станом роботи ключового обладнання;
- відслідковувати і записувати зміну з різних компонентів ключового обладнання;
- можливість дистанційного ввімкнення/вимкнення ключового обладнання;
- відслідковувати параметри температури в приміщеннях в цілому;
- відслідковувати параметри температури в серверній шафі;
- автоматичний запис в базу температури зовнішнього повітря;
- відслідковувати проникнення до приміщення;
- відслідковувати пожежну сигналізацію;
- можливість відстеження і управління обстановкою в серверній з необмеженої відстані.

- сповіщення про несправності різними способами;
- система повинна працювати на власних каналах зв’язку.

За станом серверного обладнання необхідно здійснювати моніторинг з максимальною точністю, тому необхідно брати показники температури з декількох точок, також передбачити канал моніторингу живлення і канал ввімкнення. Моніторинг температури технічних комплектуючих також дозволить оцінювати навантаження даних і прогнозувати їх вихід з ладу.

Стоїть задача віддаленого моніторингу і диспетчеризації серверного приміщення, тобто робота з сервером на відстані. Це означає, що визначаються як мінімум дві підсистеми: робоче місце адміністратора (РМА) і серверне приміщення. Проте щоб організувати необмежений по відстані моніторинг необхідно ввести третю підсистему – засоби зв’язку.

Підсистема РМА представляє собою віддалений ПК чи ноутбук із встановленою керуючою системою і з підключеними комунікаційними засобами. Є головною керуючою ланкою системи. Саме звідси посилаються на керований об’єкт команди моніторингу, приймаються відповіді із значеннями датчиків, обробляються і регулярно заносяться на зберігання і аналіз у базу даних. Команди повинні бути узгоджені з керуючою системою об’єкту. РМА по черзі опитує всі початково створенні на ньому канали опиту і по ходу опиту створюється динаміка змін в роботі системи. У випадку масштабування системи керуюча програма РМА легко змінюється, але ці зміни мають бути узгоджені з керуючою системою об’єкта.

Підсистема об’єкта моніторингу – це серверне приміщення, яке є керованим об’єктом. Все обладнання, за яким здійснюється моніторинг знаходиться тут. Вся керуюча система в серверному приміщенні укладена в контролері. На ньому записана програма , яка по команді з РМА буде виконувати потрібні дії. Команди з РМА і контролером узгоджені.

Підсистема зв’язку. За умовами створення системи повинен бути реалізований зв’язок, який дозволить опитувати об’єкт з необмеженої відстані. Сервери розраховані на цілодобову роботу. Але часто відбуваються позаштатні

ситуації, такі як зависання чи відключення живлення у будівлі. В цьому випадку обладнання перестає виконувати свої функції. В таких випадках за допомогою даної системи стає можливим віддалено перезапустити роботу обладнання. Після перезапуску сервер автоматично почне виконувати свої функції.

Раніше системи моніторингу відправляли повідомлення за допомогою E-mail або SMS. Ці засоби сповіщення мають свої мінуси: поштову скриньку необхідно перевіряти на наявність нових листів, тобто відсутній миттєвий доступ до інформації, лише за запитом. У випадку SMS сповіщень недолік з миттєвим сповіщенням усунутий, але присутня фінансова проблема – кожне SMS повідомлення коштує грошей. У випадку з Telegram повідомлення безкоштовні, якщо пристрій, з якого використовується Telegram під’єднаний до мережі інтернет.

Сповіщення миттєві, як тільки надходить нове повідомлення з системи моніторингу ви отримуєте сповіщення про це від додатку.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ВИКОРИСТАННЯ БОТУ

Створення центрів обробки даних - процедура складна і тривала. Чи допоможе стандартизація цього процесу зменшити ризики ненадійної роботи обладнання і виключити необхідність додаткових вкладень для усунення недоліків? Згідно з оцінкою Gartner Group, середньосвітовий обсяг призначених для користувача даних, що припадає на одну компанію, становить 120 терабайт. У свою чергу, за розрахунками IDC, в минулому році за одну годину в світі відправлялося 35 млрд. повідомлень. Якщо враховувати ці числа, то виходить, що на одне повідомлення припадає приблизно 3,4 Мб інформації. Звичайно, більшість листів електронної пошти не супроводжуються об'ємними повідомленнями. Але не так вже й мало вкладень містять вибірки з корпоративних баз даних або ж презентації з графічними слайдами і відео. Розмір такого вкладення - кілька десятків мегабайт. Для підготовки подібного повідомлення залучаються потужні обчислювальні ресурси. Крім того, самі бази даних десятками обробляються в різного роду програмах, що охоплюють практично всі аспекти діяльності компанії. Інтенсивні потоки даних, що циркулюють в інформаційних системах багатьох підприємств, вимагають особливої організації IT-інфраструктури. Вона повинна адаптуватися до мінливих вимог бізнесу і, зокрема, забезпечувати постійне зростання продуктивності використовуваних рішень і максимальну ефективність їх експлуатації.

Варіантом вирішення цієї проблеми може бути концентрація обчислювальних ресурсів і розподіл їх функцій між додатками. Такий підхід централізованих обчислень отримав назву «віртуалізація ресуріс». Результатом реалізації цієї концепції є центри обробки даних (ЦОД).

1.1 Загальні дані про центр обробки даних

Дата-центр, або центр обробки даних (ЦОД), – це комплекс потужних серверів, дискових сховищ і технічних рішень, спрямованих на автоматизацію і безперебійну роботу комерційних процесів. Іншими словами ЦОД – це приміщення, призначене для розміщення обладнання для обробки і зберігання данних.

1.1.1 Принципи роботи ЦОД:

Віртуалізація. Рішення, що дозволяє зменшити кількість використовуваного обладнання, що призводить до економії часу, коштів і площі, необхідних для створення центру обробки даних.

Кластеризація. Установка програм зв'язків між декількома серверами з метою їх об'єднання для координації роботи та перерозподілу навантажень.

Масштабування. Передбачення можливості збільшення потужності ЦОД за рахунок додавання нових модулів або поступового збільшення продуктивності наявного обладнання.

Резервування. Створення умов для безперебійної роботи ЦОД за допомогою перерозподілу функцій між окремими підсистемами.

1.1.2 Завдання ЦОД

Першочерговим завданням дата-центрів є створення сприятливих і захищених умов для доступу конкретної компанії до власних даних і їх закриття від сторонніх користувачів.

Досягнення основної мети забезпечується за допомогою:

- зберігання та аналізу великих обсягів інформації;
- забезпечення безпеки і безвідмовності високотехнологічних систем;
- забезпечення максимальної доступності даних;
- об'єднання окремих складових IT-систем.

1.1.3 Умови організації ЦОД

Створення дата-центру зазвичай передбачає виділення окремого відділу в конкретній компанії, якщо відповідні послуги не надаються ззовні на комерційних умовах.

Приміщення, де знаходиться ЦОД має розташовуватися в безпосередній близькості від зовнішніх транспортних і електричних мереж. В обов'язковому порядку дотримуються найжорстокіші нормативи по площі приміщення, навантажувальної спроможності його перекриттів, особливостям електроживлення і кондиціонування.

1.1.4 Основні етапи створення ЦОД:

- планування (розробка технічного завдання та плану реалізації);
- узгодження обраної концепції і її адаптація до реальних умов експлуатації дата-центру;
- безпосередня реалізація проекту;
- експлуатація центру обробки даних;
- модернізація дата-центру.

Будівництво безпечного і надійного ЦОД можливо тільки при дотриманні вимог і нормативів, які стосуються характеристик приміщення, де буде розташовуватися обладнання. Від фактичного стану майданчика залежить не тільки належне функціонування ЦОД, а й вартість його облаштування.

1.1.5 Типи ЦОД

За розміром ЦОД бувають:

- великі, що займають окремі будівлі, створенні для забезпечення найліпших умов розміщення. Часто мають власні канали зв’язку, до яких і під’єднуються сервери;
- модульні, що збираються з блоків;
- середні, зазвичай розміщуються в орендованих приміщеннях, канал зв’язку беруть у постачальників;
- малі, часто займають невелике, мінімально пристосоване приміщення.

Обладнання, як правило, низької якості. Спектр послуг невеликий.

- контейнерні – стійки з обладнанням розміщені у контейнерах. Перевагою є те, що такі ЦОД мобільні.

За призначення ЦОД поділяють на типи:

- корпоративні. Використовуються звичайними та інтернет-компаніями для зберігання власної актуальної інформації, і забезпечення функціонування віртуальних сервісів;

- комерційні. Орієнтовані на зберігання і обробку даних сторонніх користувачів у цілях підвищення ефективності щоденної економічної діяльності.

1.1.6 Склад ЦОД

Компоненти, з яких складається ЦОД, можна поділити на три основні групи:

- технічні компоненти. До них відносять: серверний комплекс, системи зберігання і резервного копіювання даних, мережева інфраструктура, системи інженерної експлуатації і безпеки дата-центра;

- програмне забезпечення. До них належать: операційні системи серверів, робочих станцій, програмне забезпечення баз даних, засоби адміністрування серверів і робочих станцій, резервного копіювання, кластеризації і інвентаризації, програми пристроїв зберігання даних, браузери і поштові клієнти;

- організаційне середовище. Воно забезпечує функціональність процесів пов’язаних с наданням IT- послуг.

1.2 Вимоги та рекомендації для організації серверної кімнати

До приміщення ставляться специфічні рекомендації, наприклад:

- у серверній потрібно підтримувати надлишковий тиск повітря по відношенню до прилеглих приміщень;

- при створенні серверної кімнати доцільно забезпечити резервування електроживлення, наприклад за допомогою підключення дизель-генератора;

- рівень підлоги в серверній повинен бути не менше, ніж на 10 см вище, ніж в сусідніх приміщеннях;

- також необхідно використання незалежних систем IP моніторингу серверних, що включають в себе датчики температури і вологості, кабельні або прості датчики витоку води, датчики струму і напруги, лічильники електричної потужності, датчики повітряного потоку і диму.

1.2.1 Основні вимоги

- рекомендована ASHRAE температура в приміщенні 18 - 27 ° С, для цього необхідно кондиціонування повітря;

- вологість повітря в серверній повинна бути в межах від 20% до 80% без конденсації вологи; швидкість зміни вологості 6% в годину;

- запиленість не повинна перевищувати 0,75 мг / м³ {СН 512-78};

- тиск в серверній повинен перевищувати тиск в сусідніх приміщеннях. Рекомендується перевищення тиску не менше 14.7 Па.;

- рівень освітлення має становити не менше 500 лк, виміряному на висоті 1 метр в горизонтальній площині;

- рівень електромагнітного випромінювання не повинен перевищувати 3 В/м в усіх діапазонах частот;

- для певних видів обладнання необхідно обмежити вібрацію.

1.2.2 Вимоги до електричного забезпечення

- 2 планки розеток підключених на різні вводи для кожної стійки;

- стабільність електроживлення повинна забезпечуватися ДБЖ підключеними по схемі On-Line;

- для групової прокладки з урахуванням обсягу горючого завантаження в приміщеннях, оснащених комп'ютерною та мікропроцесорної технікою повинні застосовуватися кабелі з маркуванням нг-HF – які не поширюють горіння при груповій прокладці і не виділяють корозійно-активних газоподібних продуктів при горінні і тлінні.

1.2.3 Норми пожежної безпеки

Приміщення повинно бути обладнане охоронно-пожежною сигналізацією. Серверне приміщення площею понад 24 м² має бути обладнано системою газового пожежогасіння. Серверна (основна і резервна) і телекомунікаційна обладнуються автоматичними установками газового пожежогасіння (АУГП), згідно з вимогами норм. АУГП передбачається для приміщень, де розташовується обладнання управління ІТТ (серверна, центр управління, процесинговий центр). Вогнегасячою речовиною повинен бути газ, який має український сертифікат. Використання фреону 114В2 (тетрафтордіброметан) і порошкових вогнегасників в цих приміщеннях категорично заборонено.

1.3 Стандарти інфраструктури

В даний час існує два стандарти, що визначають принципи побудови інфраструктури центрів обробки даних - це розроблений в США стандарт TIA / EIA-942 і європейський стандарт EN 50173-5. Обидва стандарти містять багато подібних положень, але сфера дії американського стандарту набагато ширше, адже він визначає не тільки особливості організації кабельної проводки. Номер європейського стандарту говорить про те, що він належить до групи кабельних стандартів, а число після дефіса вказує на застосування у відповідних приміщеннях. Так європейський стандарт, в основному визначає кабельні рішення для центрів обробки даних (рис.1.1, 1.2).

Американський стандарт розглядає структуру в цілому і містить не тільки загальні керівництва по організації кабельної інфраструктури, встановлення монтажної арматури і визначення місць для укладання кабелю. У ньому також приділено увагу проектуванню мережі, організації доступу, правилам розміщення центру обробки даних, архітектурним особливостям приміщень, організації електроживлення, освітлення, кліматичних умов, забезпечення безперебійної

роботи обладнання, пожежної безпеки та захисту від вологи. Важливою складовою стандарту є вимога забезпечення високої експлуатаційної готовності обладнання в центрі обробки даних, необхідного для обслуговування запитів, які надходять від великого числа користувачів.

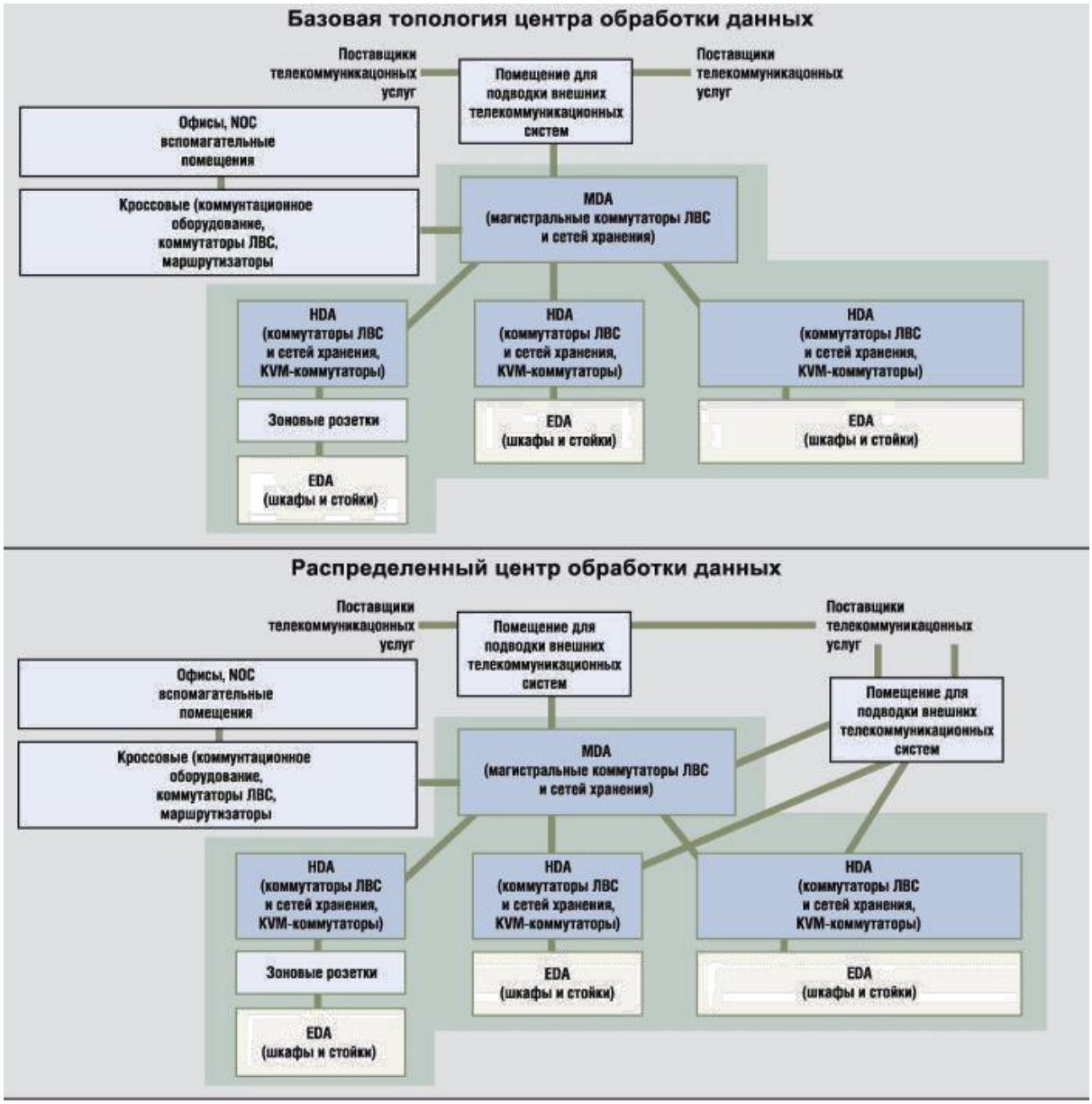


Рисунок 1.1 - Базова топологія центра обробки даних

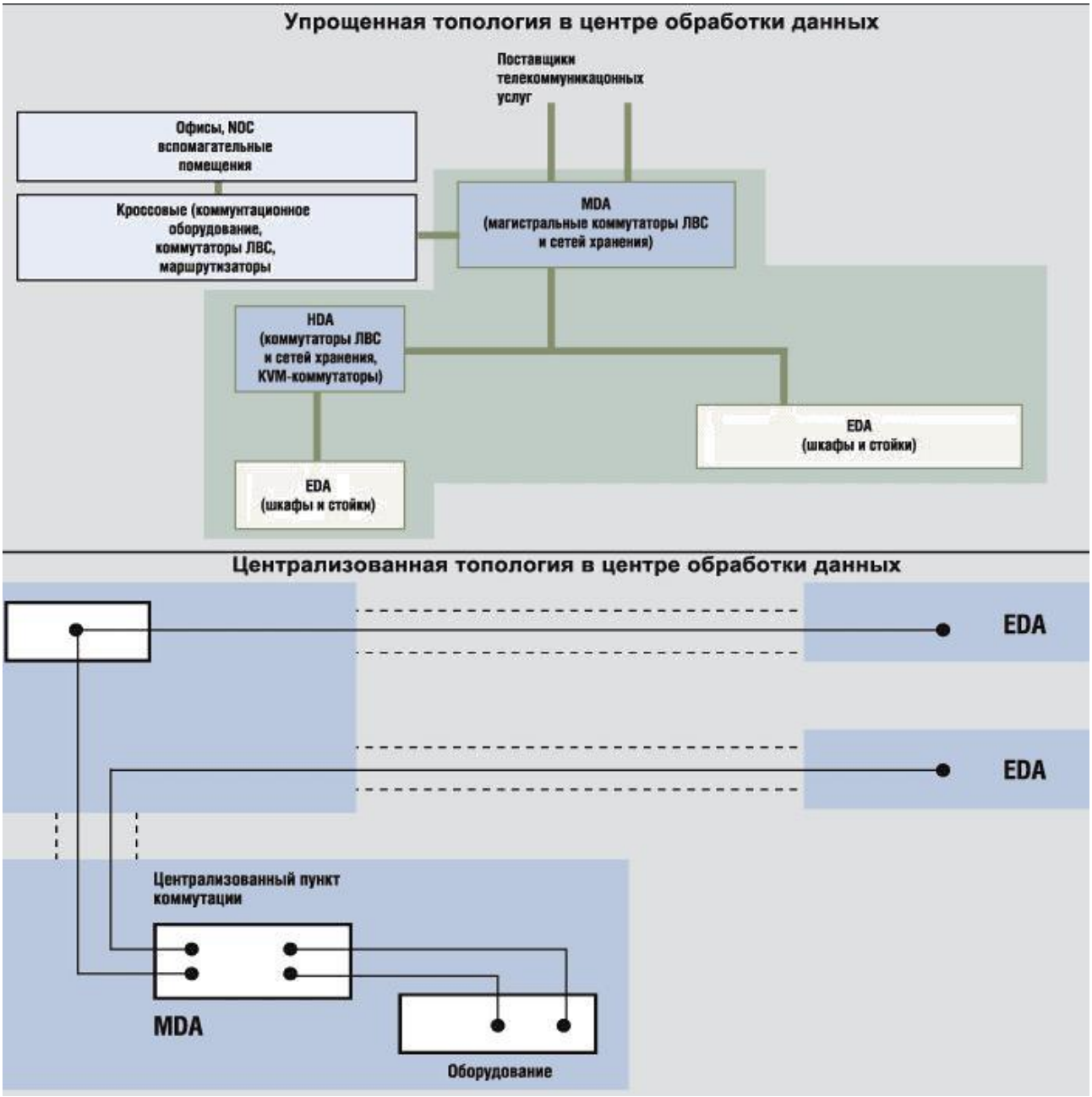


Рисунок 1.2 - Спрощена топологія в центрі обробки даних

У зв'язку з таким широким охопленням проблематики, пов'язаної з реалізацією інфраструктури ЦОД, далі буде розглядатися в основному американський стандарт.

Американський стандарт визначає вимоги і основні правила для проектування і реалізації центрів обробки даних і комп'ютерних приміщень (серверних залів). Своєрідною "відправною точкою" дії стандарту є початок

проектних робіт, що передують будівництву або реконструкції будівлі. Тільки на цьому етапі можна в повній мірі оцінити всі архітектурні особливості приміщень центру обробки даних і забезпечити взаємодію всіх технічних систем. Тому керуватися стандартом повинні в першу чергу проектувальники, так як їм доводиться планувати взаємозв'язок архітектури будівлі, його технічних систем і кабельної інфраструктури з урахуванням функціонування великої кількості комп'ютерного обладнання з високою щільністю компоновки.

1.4 Перелік основних елементів

Американський стандарт передбачає обов'язкове виділення спеціалізованих приміщень і організацію робочих зон. Зокрема, це приміщення для підводки зовнішніх телекомунікаційних систем, комп'ютерного обладнання, телекомунікаційного обладнання і приміщення для інженерних систем, наприклад, електрощитові, виробничі приміщення систем кондиціонування і вентиляції і т.і.

Для моніторингу та управління центром даних (особливо центром, який забезпечує виконання відповідальних завдань) організовується центр поточного управління мережею. Його функціонування полягає у визначенні несправностей і розробці дій, що виключають такі наслідки, як можливий простой комп'ютерного обладнання. У центрі поточного управління мережею розміщуються технічні засоби, які, зокрема, здійснюють моніторинг теплового режиму, відстежують зупинки і збоїв в роботі обладнання з подальшою діагностикою модулів і блоків, які вийшли з ладу. Крім приміщень для установки комп'ютерного обладнання, в будівлі центру обробки даних можуть виділятися приміщення для розміщення офісних і допоміжних служб, таких як центри обслуговування клієнтів або служби підготовки введення даних. До числа таких приміщень відносяться комутаційні пункти горизонтальної проводки для офісних і допоміжних служб.

1.5 Області комутації

У приміщенні для комп'ютерного обладнання виділяються області основної розводки (ООР), горизонтальної розводки (ОГР), зонової розводки (ОЗР) і область розводки обладнання (ОРО).

В європейському стандарті використовуються інші назви елементів кабельної інфраструктури. Зовнішні телекомунікаційні сервіси підводяться до зовнішнього інтерфейсу мережі, який з'єднується з основним центром комутації за допомогою підсистеми мережевого доступу. У зоновій підсистемі здійснюється розводка до розеток обладнання або безпосередньо, або через підключення локальних розподільчих пунктів.

Розташування приміщень і зон визначається розмірами центру обробки даних, а також можливостями установки додаткового обладнання та переходу на більш досконалі комунікаційні технології.

У приміщеннях для підводки зовнішніх телекомунікаційних систем розташовуються інтерфейси, що з'єднують структуровану кабельну систему центру обробки даних з магістралями групи будівель, а також з кабельним обладнанням постачальників телекомунікаційних послуг. Це може бути окреме приміщення (стандарт рекомендує виділяти окреме приміщення з міркувань безпеки), але допускається і об'єднання з приміщенням для комп'ютерного обладнання. В загальному приміщенні обладнання, що забезпечує введення зовнішніх телекомунікаційних сервісів, консолідується в області основної розводки.

У центрі обробки даних може налічуватися кілька приміщень для підводки зовнішніх телекомунікаційних систем, що дозволяє дотримуватися обмеження довжини ліній зв'язку, а також реалізовувати обслуговування різних підрозділів.

Область основної розводки (ООР) – це місце розміщення основного комутаційного центру кабельної системи ЦОД. ООР є найбільш підходящим місцем для установки маршрутизаторів і комутаторів ядра локальної

обчислювальної мережі центру даних і мережі зберігання. Крім того, в цю область можуть інтегруватися розподільні пункти горизонтальної розводки, що обслуговують обладнання в безпосередній близькості від ООР.

Області горизонтальної розводки (ОГР) ви виділяються для реалізації розподільних пунктів горизонтальної підсистеми, кабельні лінії якої доходять до області розводки обладнання. Тому ОГР розглядається як місце розміщення комутаторів локальної обчислювальної мережі та мережі зберігання, а також KVM-комутаторів (що дозволяють управляти декількома серверами за допомогою одного комплекту "клавіатура-відео-миша"), які обслуговують обладнання в відповідних областях розводки обладнання (ОРО).

Додаткові комутаційні центри зонового кабельного обладнання, яким відповідають області зонової розводки, - це необов'язкові елементи. Вони розміщуються між ОГР і ОРО, там, де необхідно часто проводити реконфігурацію кабельного обладнання, або ж використовуються як засіб забезпечення додаткової гнучкості в горизонтальних рішеннях. Горизонтальні кабелі, які підходять до області зонової розводки, обжимають в зоновій розетці або точці консолідації. Подальша розводка здійснюється за допомогою комутаційних шнурів.

В області зонової розводки не рекомендується встановлювати активне обладнання, за винятком рішень по організації електроживлення на витій парі.

В області розводки обладнання здійснюються мережеві підключення, необхідні для комп'ютерного обладнання. Розетки ОРО рекомендується реалізовувати за допомогою комутаційних панелей, які розміщуються в стійках з обладнанням.

Допускаються додаткові з'єднання між ОГР (в тому числі з метою резервування) або з'єднання з кабельним обладнанням приміщень для підводки зовнішніх телекомунікаційних систем (коли виділяється кілька таких приміщень).

1.6 Рівні надійності

Щоб підтримувати надійність роботи центрів обробки даних, в американському стандарті специфікуються рівні експлуатаційної готовності і перераховуються заходи, що забезпечують функціонування обладнання ЦОД з урахуванням характеристик того чи іншого рівня.

Стандарт виробляє атестацію центрів обробки даних відповідно з чотирма визначеними рівнями. Чим більше номер рівня, тим вище експлуатаційна готовність. Класифікація за рівнями дає проектувальникам можливість визначати, які рішення слід застосовувати в тому чи іншому випадку. Крім того, вона дозволяє швидко і ефективно оцінювати роботу центру обробки даних, що може знадобитися споживачеві послуг хостингу.

Для кожного рівня наводяться детальні рекомендації, що визначають особливості архітектурного проекту, а також рекомендації щодо функціонування інженерних систем.

Класифікація за рівнями розглядає можливість збереження працездатності при наявності хоча б одного виходу з ладу в якомусь з інфраструктурних рішень. Проект, в якому можливе проведення планових робіт з технічного обслуговування без порушення роботи системи, визначається як допускаючий одночасну експлуатацію і технічне обслуговування. Це обслуговування передбачає виконання заздалегідь запланованих робіт, процедури проведення яких чітко визначені: різні перевірки, налаштування, регламентні роботи, тестування систем і компонентів, що входять до них.

Відмінності між рівнями визначаються величиною експлуатаційної готовності. Так, для центрів обробки даних першого рівня величина експлуатаційної готовності повинна бути не менше 99,671%, що відповідає максимально-допустимій сумарній тривалості простоїв 28 годин 48 хвилин. Це базовий рівень працездатності центру обробки даних. В такому ЦОД може встановлюватися джерело безперебійного електроживлення і навіть аварійний

генератор, але разом з тим використовується єдиний канал підведення електроживлення і єдиний канал розподілу охолоджуючого повітря.

Проведення регламентних або ремонтних робіт вимагає повного виведення з експлуатації всієї інфраструктури. Тому позаштатні ситуації є причиною досить тривалих простоїв.

Рівень з резервуванням компонентів (рівень II) допускає тривалість простою не більше 22 годин за рік (експлуатаційна готовність - 99,741%). Причини простоїв - ті ж, що і для попереднього рівня, - нештатні ситуації і планові перерви на технічне обслуговування. Також вразливим місцем є активні підводи комунікацій (по одному на систему). Резервування здійснюється за схемою N + 1.

Центри обробки даних, що обслуговуються одночасно рівня III допускають проведення будь-яких запланованих дій з технічного обслуговування без переривання роботи комп'ютерного обладнання. Річний простій на цьому рівні не повинен перевищувати 1 годину 36 хвилин (експлуатаційна готовність -99,982%). У таких ЦОД реалізується кілька каналів підведення комунікацій і здійснюється резервування всіх кабельних ліній.

Стійкі до несправностей центри обробки даних четвертого рівня забезпечують 99,995% експлуатаційної готовності і допускають простої протягом всього 25 хвилин за рік. Функціональні можливості інфраструктури ЦОД рівня IV дозволяють зберігати працездатність при найнесприятливіших обставин, що супроводжують нештатну ситуацію. Такі рішення передбачають наявність в кожній системі декількох активних каналів або навіть резервування типу “system+system”.

Інфраструктура центру даних IV рівня є оптимальним робочим середовищем для реалізації високонадійних IT-рішень, таких як кластерні обчислювальні системи, системи зберігання та відмовостійкі комп'ютерні мережі.

1.7 Переваги ЦОД

Унікальні можливості ЦОД гарантують ефективність і безперебійність роботи будь-якої організації, допомагаючи вирішувати більшість проблем, властивих будь-якому виду бізнесу.

Багатокомпонентні системи забезпечують:

- високу надійність зберігання інформації по цілком обґрунтованій вартості;
- значну економію коштів за рахунок варіативного вибору послуг і можливостей, що особливо актуально при реалізації нових IT-проектів;
- скорочення витрат на оренду приміщень, сервісне обслуговування обладнання та оплату електрики;
- створення умови для безперебійної роботи і взаємодії головного офісу і мережі філій;
- можливість організації резервного офісу в разі потреби.

1.8 Дослідження процесу моніторингу і диспетчеризації

Сучасні центри обробки даних (ЦОД) дозволяють працювати з великим потоком інформації, організовувати централізоване зберігання даних, збільшувати надійність всієї інформаційної інфраструктури і забезпечувати зв'язок між центром обробки даних і користувачами.

Неправильна організація центрів обробки даних і економія на системах життєзабезпечення - системах вентиляції, кондиціонування, пожежогасіння, контролю доступу та відеоспостереження - може стати причиною поганих наслідків. При виході з ладу центр обробки даних може заблокувати доступ до інформації, а в найгіршому випадку відбудеться її безповоротна втрата.

Система контролю мікроклімату має забезпечувати в серверному приміщенні заданий рівень вологості і температури, необхідний для нормального функціонування активного обладнання незалежно від пори року, і має бути розрахована на цілодобову безперервну роботу. Для забезпечення надійності вищевказаної системи і для попередження виникнення аварійних ситуацій використовується система моніторингу мікроклімату. Система моніторингу повинна виконувати наступні функції:

- контролювати температуру і вологість в серверному приміщенні;
- зберігати значення параметрів мікроклімату;
- подавати сигнал аварії при перевищенні встановлених значень параметрів мікроклімату в приміщенні;
- повідомляти користувачам про виникнення аварійних ситуацій через Інтернет і засоби мобільного зв'язку.

Серверна - серце інформаційної системи підприємства. Для підтримки коректної роботи комунікацій потрібен контроль не тільки software складової серверів, їх грамотне налаштування, але і якісне і своєчасне обслуговування. Найбільш типовими завданнями моніторингу серверних кімнат є: моніторинг клімату і навколишнього середовища при роботі комп'ютерного обладнання, моніторинг доступу в приміщення і наявності руху в серверній кімнаті, моніторинг наявності електроживлення. Система моніторингу повинна постійно відслідковувати ці параметри і повідомляти черговий персонал у разі необхідності. Для більшості компаній потрібно підтримувати безперебійну роботу серверів в режимі 24/7.

Сучасні бізнес-процеси може забезпечити тільки безвідмовно працююче обладнання. Безпека і безперебійність виробничого процесу багато в чому визначаються безперервним контролем за технологічними параметрами. Відсутність контролю веде до відмов і простоїв дорогого обладнання, що в свою чергу призводить до збитків компанії. Своєчасне діагностування несправностей, засобами дистанційного керування технологічного обладнання, знижує вартість ремонту даного обладнання і мінімізує час введення резерву в експлуатацію.

1.8.1 Моніторинг кімнати

Моніторинг кімнати включає в себе підтримку температури в межах 18 ° - 27 ° С. Рівень вологості від 40% до 60%.

Моніторинг серверної або ЦОД - це моніторинг навколишнього середовища в кімнаті, тобто рівні вологості і температури. Датчики температури і вологості зазвичай встановлюють:

- в потенційно "гарячих" зонах усередині серверної або ЦОД;

- біля кондиціонерів, щоб випередити поломку цих систем.

Коли в серверній є кілька кондиціонерів, поломка одного кондиціонера буде спочатку компенсуватися іншими, запобігши повну поломку охолоджуючої системи через перевантаження. Рекомендується встановити датчики температури / повітряного потоку біля кожного кондиціонера, щоб заздалегідь визначити поломку.

Моніторинг вологості так само важливий, як і моніторинг температури, але його часто випускають з виду. Відносна вологість в серверних і ЦОД повинна бути між 40% і 60%. Занадто сухе повітря призведе до накопичення статичної електрики в системах, а надто вологе - викличе корозію, яка почне повільно руйнувати ваше обладнання та призведе до його постійних поломок.

Використання холодних коридорів всередині ЦОД може привести до підвищеної температури повітря поза коридорів. Температура повітря 37 ° С не є чимось незвичайним в таких умовах, це дозволяє істотно зменшити вартість електроенергії. Однак, це також означає, що моніторинг температури має найбільше значення, оскільки поломка кондиціонера швидше відіб'ється на доступності і терміні служби систем (навантаження на вентилятор, перегрів процесора, тощо).

Високі температури в кімнаті можуть також позначитися на обладнанні, не встановленому в стійках .

При використанні гарячих коридорів необхідно стежити за температурою по всій кімнаті, щоб переконатися, що в кожну стійку потрапляє досить холодного повітря. У цьому випадку можна покластися на датчики температури,

встановлені в стійках, на додаток до датчиків температури і вологості біля кожного кондиціонера.

Система охолодження і система опалення повинні управлятися уніфікованим пристроєм, яке дозволяло б зчитувати дані з датчиків температури, вологості і передавати команди управління системам опалення або системам охолодження, згідно налаштувань граничних значень.

Система охолодження повинна бути досить надійною, щоб безперебійно працювати протягом довгого часу і підтримувати необхідний рівень температури і вологості повітря. Крім того, в зимову пору року під час дії негативних температур обладнанню в серверній кімнаті також може знадобитися охолодження. Також може знадобитися опалення. Для вмикання / вимикання опалювальної системи потрібна система управління, яка зможе управляти обігрівачем, ґрунтуючись на даних датчиків температури і вологості.

Показник вологості також є важливим в роботі обчислювального обладнання. Для підтримки оптимальної вологості повітря необхідно вибирати відповідний кондиціонер або використовувати додатково осушувач повітря. Деякі сучасні спліт-системи дозволяють знизити температуру, здійснити постійний приплив очищеного повітря, але не дозволяють підтримувати його оптимальну вологість. Варто уникати використання подібних спліт-систем в серверних приміщеннях. Як правило, в приміщенні встановлюється один кондиціонер, що з точки зору забезпечення нормального температурного режиму недостатньо: в разі раптового виходу з ладу кондиціонера можливий перегрів обладнання і, як наслідок, його вихід з ладу. Тому рекомендується встановлювати як мінімум два кондиціонери. Потужність кожного кондиціонера окремо була б достатньою для створення необхідних кліматичних умов в серверній кімнаті. Також,
використовуючи сучасні системи моніторингу клімату в серверній, можливе налаштування почергової роботи кондиціонерів для збільшення терміну служби і можливості безвідмовної роботи. Використовуючи функції почергової роботи кондиціонерів, можливе проведення профілактичних робіт з кондиціонерами, що

в кінцевому підсумку збільшить ресурс кондиціонерів і убезпечить обладнання від небажаних підвищень температури і виходу з ладу обладнання.

Диспетчеризація - це процес централізованого моніторингу і дистанційного керування, з використанням оперативної передачі інформації між об'єктами диспетчеризації і пунктом управління. Впровадження систем диспетчерського контролю дозволяє підвищити техніко-економічні показники за рахунок контролю і підвищити ефективність роботи обладнання, а також безпеку персоналу.

1.8.2 Важливість моніторингу центра обробки даних Так чи інакше, всі IT-процеси проходять через серверну кімнату. Неполадки в серверній впливають на всю компанію - наслідки непередбачувані. Моніторинг допомагає швидко виявити помилки і захистити IT-інфраструктуру від можливих збоїв.

Сервери - ключові елементи IT-інфраструктури компанії. Відмова сервера може позначитися на роботі всієї компанії: простої в роботі, відсутність доступу до даних. Це відіб'ється на якості роботи бізнес-підрозділів. Програмне забезпечення та ключові сервіси будуть недоступні. Серверна кімната вимагає надійного захисту: від пожежі і руйнування, від злому і несанкціонованого доступу.

Сервери чутливі до перепадів температури, вологості і перебоїв з електроживленням. Тому серверні приміщення вимагають постійного моніторингу. Конфіденційні дані необхідно захищати. Для цього потрібні чіткі правила доступу в серверну кімнату. Запобігти несанкціонованому використанню даних можна за допомогою контролю доступу та системи запису подій.

Системи моніторингу допомагають захистити обладнання серверної кімнати від перепадів температури і вологості. За допомогою датчиків ви відстежуєте доступність серверів та іншого обладнання в приміщенні і контролюєте мікроклімат: температуру, вологість, швидкість потоку повітря.

Важливо отримувати миттєві повідомлення про зміни серверної кімнати, щоб відразу ж зреагувати на ті чи інші зміни.

Ці запобіжні заходи дадуть позитивні результати. Клієнти і партнери будуть спокійні, усвідомлюючи, що все під контролем.

1.9 Висновки до розділу

Дата-центр, або центр обробки даних (ЦОД), – це комплекс потужних серверів, дискових сховищ і технічних рішень, спрямованих на автоматизацію і безперебійну роботу комерційних процесів.

ЦОД включає в себе такі компоненти: технічні компоненти, програмне забезпечення і організаційне середовище. У даному розділі було визначено необхідність моніторингу центру обробки даних. Технічні компоненти ЦОД надзвичайно важливі у IT-інфраструктурі компанії, тому не можна допускати того, щоб вони вийшли з ладу.

Було розглянуто принцип роботи і завдання ЦОД, основні етапи створення, вимоги та рекомендації для організації серверної кімнати. Наведено основні переваги центру обробки даних. Розглянуто і проаналізовано рівні надійності центрів обробки даних.

2 АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ТА ВИБІР НАЙКРАЩИХ ВАРІАНТІВ ДЛЯ СИСТЕМИ МОНІТОРИНГУ І ДИСПЕТЧЕРИЗАЦІЇ

2.1 Вибір устаткування системи моніторингу

Основними вимогами до устаткування автоматизованої системи диспетчеризації та управління (АСДУ) ЦОД є:

- єдина система диспетчеризації повинна дозволяти своєчасно усувати несправності та забезпечувати гнучкість і ефективність експлуатації обладнання ЦОД;

- система диспетчеризації та автоматизації інженерних систем ЦОД повинна будуватися за модульним принципом і мати можливість гнучкого доповнення для обробки сигналів різних типів без перестроювання всієї системи, мати можливість підключення нових зон, областей контролю і управління в систему диспетчеризації з виходом на РМА диспетчера. А також мати резерв кабельних розводок і центрального устаткування для підключення додаткових контролерів;

- моніторинг параметрів інженерних систем ЦОД повинен проводитися на основі наявних засобів внутрішнього моніторингу зазначених систем.

Для моніторингу інженерних систем ЦОД використовуються вільно-програмовані контролери. Підключення модулів введення/виведення по шині дозволяє набирати потрібну кількість точок введення/виведення відповідно до вимог по автоматизації систем ЦОД.

Додаткові функції контролера:

- управління маршрутизацією тривожних повідомлень в мережі. Три рівня функціональності тривожних повідомлень різних пріоритетів. Надійне відстеження і контроль передачі тривожних повідомлень;

- тимчасові програми;

- побудова трендів;

- можливість віддаленого управління;

- захист доступу до мережі з індивідуальними профілями і рівнями доступу для користувачів.

Контролери забезпечують можливість реалізації та обробки системних і прикладних функцій. Крім вільно-запрограмованих функцій контролю, контролер включає зручні функції управління тривожними повідомленнями з маршрутизацією їх по всій мережі.

Збір даних стану інженерних систем ЦОД проводиться в станції диспетчеризації в системі диспетчеризації і управління, і забезпечує наступні можливості:

- можливість здійснювати комунікацію з контролерами (станціями автоматизації);
- отримувати і відображати інформацію про стан контролерів (станція автоматизації);
- отримувати і виводити інформацію про точки даних контролерів;
- керувати правами доступу для різних груп користувачів системи диспетчеризації;
- задавати групи маршрутизації, одержувачів аварійних повідомлень і розкладу активізації того чи іншого одержувача;
- розсилати аварійні повідомлення згідно з таблицею маршрутів.

У той же час передбачається взаємодія елементів диспетчеризації з системою відеоспостереження для контролю виконуваних робіт з інженерними системами.

АСДУ може складатися з наступних підсистем:

- підсистема моніторингу та управління інженерних систем об'єкта;
- підсистема моніторингу протікання;
- підсистема моніторингу стану телекомунікаційних шаф;
- підсистема газоаналізу;
- підсистема технологічного відеоспостереження;
- підсистема збору, обробки та зберігання інформації;
- підсистема синхронізації часу.

Основними підсистемами системи моніторингу ЦОД є:

- моніторинг контролю доступу до серверних шаф;
- моніторинг навколишнього середовища в приміщенні ЦОД.

2.2 Вибір контролеру

Після тривалого аналізу ринку контролерів вибір звузився до двох виробників: ИТР і NetPing. Зрівняємо обидва для вибору оптимального контролеру для системи диспетчеризації.

2.2.1 Контролер ИТР «Импульс 112»

Це контролер моніторингу, який дозволяє забезпечити цілодобове спостереження за мережами, обладнанням, інженерними об'єктами. До контролера можна підключати аналогові датчики. Сам контролер приєднується до мережі за допомогою як USB модему, так і Ethernet підключення. Контролер може працювати в двох основних режимах: мережевому і локальному. Контролер легкий в налаштуванні завдяки вбудованому веб-інтерфейсу.

Має змогу підключити 4 датчики, напруга живлення 12 В, має веб-інтерфейс.

Вартість 4251, 68 грн.

2.2.2 Пристрій UniPing server solution v3 / SMS

Пристрій віддаленого моніторингу датчиків по мережі Ethernet/Internet. Дозволяє віддалено отримувати інформацію про стан датчиків і повідомлення про спрацювання датчиків.

Має:

- Ethernet 100 мбіт/с порт;
- можливість підключення по WiFi;
- вбудований GSM модем для SMS-повідомлень про спрацювання датчиків;
- 8 IO ліній для підключення датчиків або управління зовнішніми пристроями;
- резервне безперебійне живлення;
- вбудований web-сервер для конфігурації і управління пристроєм через браузер.

У деяких випадках може автоматично вжити необхідних заходів для відновлення оптимальних умов роботи обладнання. Наприклад, при перевищенні рівня температури включити резервний кондиціонер.

Зазвичай використовується для:

- моніторингу фізичних умов роботи комп'ютерного обладнання та обмеження доступу до ящиків з обладнанням, повідомлення відповідальних осіб про позаштатні ситуації (e-mail, SMS-повідомлення, локальні повідомлення);

- віддаленого управління кондиціонерами, системами вентиляції, і системами підтримки мікроклімату. Підключені датчики дозволяють відстежувати поточну ситуацію, а віддалене управління розетками 220 В дозволяє включити необхідну систему без фізичної присутності на об'єкті, в тому числі і в автоматичному режимі.

Датчики які можна підключити (рис. 2.1):

- датчики температури;

- датчик наявності електроживлення, датчик відкриття/закриття дверей;

- датчик протікання води;

- датчик наявності диму;

- датчик удару;

- датчик розбиття скла;

- датчик вологості повітря.

Вбудований супервізор живлення захищає пристрій від перебоїв при скачках напруги. Доступ до web-інтерфейсу пристрою захищений обраним користувачем логіном і паролем. Для того, щоб потрапити на web інтерфейс пристрою, потрібно авторизуватись. Крім того, можна обмежити доступ пристрою, залишивши можливість доступу тільки з певної IP-підмережі.

Протокол SNMP широко використовується в системах збору інформації про мережеве обладнання. Пристрій підтримує команди управління і отримання інформації від датчиків по SNMP протоколу. Пристрій легко інтегрується із системами моніторингу мережі Zabbix, PRTG Network Monitor, OpenNMS, Nagios,

Cacti, The Dude, Monit та їм подібних, які отримують інформацію про стан датчиків, підключених до пристрою по протоколу SNMP.

Рисунок 2.1- Датчики відстеження різноманітних ситуацій

Протокол Syslog разом зі спеціальним ПО на сервері можна використовувати для того, щоб збирати текстові журнали (логи) роботи різних пристроїв в мережі, в тому числі і пристроїв NetPing. Це може бути дуже корисно для збору і аналізу статистики.

Пристрій підтримує управління розетками та отримання інформації від датчиків за допомогою спеціальних HTTP команд. Ці команди дозволяють управляти пристроєм за будь-якої розробленої користувачем web-сторінки, в тому числі і з будь-якого мобільного додатку.

Всі події (ввімкнення і вимкнення пристроїв, інформація з датчиків) зберігаються в незалежній пам'яті. Інформація збережеться навіть при перебої в постачанні електроенергії.

Для того, щоб команди могли бути виконані в строго певний час (модуль «Розклад»), дуже важливо, щоб годинник на пристрої не збивався. Мітки часу використовуються також для записів журналу. У пристрої є як власний вбудований незалежний годинник, так і можливість автоматичної синхронізації з зовнішнім сервером часу по протоколу NTP.

Вартість 8242,26 грн.

Враховуючи усі переваги пристрою моніторингу NetPing, а найголовніше те, що до нього можна підключити 8 датчиків і організувати процес сповіщення про критичні зміни у фізичному стані серверного приміщення вибір зупинився на ньому.

2.2.3 Підбір датчиків

Датчик температури – 500 грн.

Датчик вологості – 1410 грн.

Датчик протікання – 566 грн.

Датчик диму – 426 грн.

Датчик відкриття/закриття дверей – 161 грн.

Загальна сума системи моніторингу 11305,26 грн.

2.3 Порівняльний аналіз різних варіантів (типів) сповіщення

Мобільний телефон вже давно став невід'ємною частиною нашого життя, при чому, як в побуті, так і на роботі (більшість виробничих питань вирішуються по мобільному телефону, багато фірм повністю відмовилися від стаціонарного телефонного зв'язку через дешевизну та доступність мобільного). За даними Всесвітньої організації охорони здоров'я мобільними телефонами користуються 6,9 мільярдів чоловік, що практично дорівнює населенню Землі. За допомогою мобільного телефону можна завжди залишатися на зв’язку. Тому у процесі сповіщення займає головну роль.

2.3.1 Електронна пошта

Електронну пошту прийнято називати "email" що є скороченням від "electronic mail". Email - це система, яка використовується для створення, відправлення/отримання і зберігання даних в цифровому форматі по комп'ютерній мережі. Раніше система електронної пошти була заснована на простому протоколі передачі пошти (SMTP). Сьогоднішні технології електронної

пошти використовують «store-and-forward» модель (тобто передача даних з проміжним зберіганням). У цій моделі користувачі відправляють і отримують інформацію на свої комп'ютери.

Існує ряд переваг використання поштового сервісу:

- *простота у використанні*. Поштовий сервіс допомагає керувати нашими контактами, дозволяє нам швидко відправляти листи, допомагає підтримувати наші розсилки та історію і надає досить місця для зберігання. Електронний лист можна відправити з будь-якого комп'ютера з доступом в Інтернет;

- *швидкість*. Лист може бути доставлено миттєво і практично в будь-яку точку земної кулі. Ви можете надіслати повідомлення одночасно декільком користувачам; таким чином, поштовий сервіс економить масу часу;

- *зберігання даних*. Постачальники послуг електронної пошти пропонують своїм клієнтам / користувачам достатньо місця для зберігання листів. Також, процес сортування та організації листів, по темі або за іншими критеріями;

- *легко розставляти пріоритети*. Листи приходять з позначками.

Таким чином, стає легко розподілити їх і ігнорувати ті, які є небажаними. Таким чином, користувачі можуть легко сортувати і фільтрувати пошту в своїй поштовій скриньці.

Хоча у служби електронної пошти, є багато переваг, вона також має певні обмеження і недоліки:

- *спам*. Листи, які використовуються для відправки несанкціонованих повідомлень і небажаної реклами, що створюють незручності називаються спамом. Перевірка і видалення небажаних листів може споживати багато часу користувача. Як правило, спам-це обман, що практикується при відправці листів. Частка спаму у світовому поштовому трафіку складає близько 60-80%;

- *злом*. Акт порушення комп'ютерної безпеки називається зломом. При цій формі порушення безпеки, електронні листи перехоплюються зловмисниками. Лист, перш ніж він буде доставлений одержувачу, "проходить" між серверами,

розташованими в різних частинах світу; тому облікові записи електронної пошти уразливі для злому професійними хакерами;

- *не підходить для бізнесу*. Важливі документи можуть довго залишатися непоміченими серед великої кількості листів, які накопичуються в папці "вхідні". Таким чином, термінові листи, а особливо ті, які вимагають негайного розгляду не можуть бути легко керовані за допомогою електронної пошти;

- *віруси*. Віруси - це комп'ютерні програми, які мають потенціал для нанесення шкоди комп'ютерним системам. Віруси, як відомо, можуть копіювати самі себе і далі інфікувати всю суміжну комп'ютерну систему;

- *переповнена поштова скринька*. Поштова скринька, має тенденцію переповняться через певний проміжок часу. Такого роду інформаційне перевантаження часто відштовхує користувачів від використання послуг електронної пошти;

- *регулярна перевірка поштової скриньки*. Для того, щоб залишатися в курсі подій, потрібно регулярно перевіряти ваш обліковий запис електронної пошти. Якщо людина, через напружений розпорядок дня, не перевіряє поштову скриньку, вона може втратити деякі важливі і термінові повідомлення.

2.3.2 SMS повідомлення

SMS була створена в кінці 1980-х років в роботі з цифровою технологією GSM (глобальна система мобільного зв'язку), яка є засновницею для більшості сучасних стільникових телефонів.

Переваги SMS перед Email: SMS не вимагає роботи на вашому комп'ютері і не потребує доступу до інтернету, миттєве повідомлення про нові SMS.

Недоліки SMS:

- SMS платні. Деякі компанії беруть плату не тільки за вихідні, а й за вхідні

- доставка повідомлень не гарантується. Ви можете припускати, що сповістили потрібних людей, а вони можуть не отримати Ваші SMS або отримати з великим запізненням. У періоди високого навантаження, це може зайняти від декількох хвилин до декількох годин;

- SMS використовується лише для надсилання текстових повідомлень. SMS не підтримує передачу фотографій, відео або музичних файлів.

2.3.3 Месенджер

Месенджер – це служба безкоштовного миттєвого обміну повідомленнями через інтернет. З появою месенджерів SMS повідомлення і голосові дзвінки стали відходити на другий план, так як за них необхідно платити. Різниця у використанні месенджерів і електронної пошти в тому, що обмін повідомленнями відбувається в реальному часі. При відправлені повідомлення по Email воно зберігається у поштовій скриньці на сервері. Для того, щоб отримати повідомлення, отримувач повинен сам перевірити свою поштову скриньку і забрати їх. У смартфонах зв'язок між користувачами утримується постійно і відправлене повідомлення одразу передається отримувачу.

Тож для того, щоб отримувати миттєві повідомлення найкращим вибором буде використання месенджеру. Так як на сьогодні існує декілька варіантів різних месенджерів, необхідно обрати найбільш відповідний для задоволення процесу моніторингу і диспетчеризації.

2.4 Аналіз популярних месенджерів і визначення найбільш підходящого для створення боту зі сповіщенням

В Україні найбільш популярними вважаються три месенджери: Viber (з часткою 87%), Telegram (40%) і WhatsApp (31%). Розглянемо кожен більш детально.

2.4.1 Viber

Рік створення: 2010. Кількість користувачів: 900 000 000.

Функціонал.

На базі програми користувачі можуть:

- здійснювати умовно безкоштовні телефонні дзвінки і відеодзвінки між користувачами месенджера;

- заходити в сервіс з комп'ютера;

- створювати групові чати до 200 чоловік;

- відправляти один одному необмежену кількість повідомлень, фотографій, документів, презентацій, аудіо- та відеофайлів;

- дзвонити за мінімальними тарифами на міські і мобільні номери по всьому світу (сервіс Viber Out);

- підписуватися на публічні чати;

- здійснювати грошові перекази.

Переваги:

- простий і зрозумілий інтерфейс;

- велика кількість емодзі, стікерів і фонів для чату;

- відсутність офіційної реклами;

- наявність власної ігрової платформи;

- можливість спілкування в тематичних відкритих чатах.

Недоліки:

- час від часу виникають проблеми з безпекою;

- довге завантаження ігор;

- багато спаму.

Viber для бізнесу.

Цей популярний месенджер також максимально ефективний в малому і середньому бізнесі, але його успішно використовують і великі бренди. Наприклад, для підвищення лояльності і впізнаваності бренди розробляють корпоративні стікери спеціально для Viber. Великі компанії, такі як Fanta і Sprite, музичний агрегатор ELLO, журнал MAXIM створили публічні чати, на які можуть підписатися всі бажаючі. Крім того, Viber становить конкуренцію Skype за тарифами для міжнародних телефонних комунікацій с клієнтами.

2.4.2 Whatsapp

Рік створення: 2009. Кількість користувачів: 1 500 000 000.

WhatsApp Messenger - універсальний додаток для смартфонів, що працює на всіх мобільних платформах. Програма сканує телефонну книгу і додає в список контактів тих, хто вже працює з месенджером WhatsApp.

Функціонал.

На базі програми користувачі можуть:

- умовно безкоштовно обмінюватися повідомленнями і дзвонити;
- синхронізувати месенджер з комп'ютером;
- створювати групові чати до 256 осіб;
- відправляти необмежену кількість текстових і голосових повідомлень, фотографій, документів, аудіо- та відеофайлів, місць розташування, історії чатів;
- не використовувати пін-код і логін, так як додаток інтегрується з існуючою адресною книгою;
- мати доступ до повідомлень, які були доставлені, коли додаток був офлайн.

Переваги:

- швидкість;
- простота;
- популярність.

Недоліки:

- немає ігрової платформи;
- час від часу виникають проблеми з безпекою;
- при відправленні якість медіафайлів знижується.

WhatsApp для бізнесу

WhatsApp активніше застосовується в малому і середньому бізнесі. Мессенджер зручний для використання як в рамках внутрішньої комунікації компанії (для корпоративних чатів), так і за її межами. Через додаток можна надавати клієнтську підтримку користувачів і просувати продукти бренду. Згідно з дослідженнями, потенційні клієнти на 40% активніше взаємодіють з компаніями через мобільний месенджер WhatsApp в порівнянні з дзвінками. Людям простіше відправити коротке миттєве повідомлення, ніж дзвонити в довідкову службу, яка

часто перевантажена через велику кількість вхідних. У свою чергу маркетологи можуть відправляти через рекламні ролики, інформувати про появу нового товару / послуги і вести комунікації з ЦА.

2.4.3 Telegram

Рік створення: 2013. Кількість користувачів: 200 000 000.

Telegram — месенджер, який дозволяє обмінюватися текстовими, аудіо- і відеофайлами, а також безкоштовно телефонувати іншим користувачам програми.

Переваги:

- безпека;
- відсутність реклами;
- секретні чати і повідомлення, що самовидаляються;
- створення і підтримка розумних ботів;
- швидкість і простота;
- наявність своєї бази стікерів;
- швидкий пошук за повідомленнями і таймер для їх видалення;
- шифровка повідомлень;
- просунутий редактор фото;
- автоматична синхронізація між пристроями.

Недоліки:

- періодичні збої в роботі через великі навантажень на сервер;
- відсутність можливості відеодзвінків;

Telegram для бізнесу

Функціонал Telegram може бути ефективний для всіх видів бізнесу. Мессенджер має високу конфіденційність і можливість здійснення банківських операцій - все це може бути активно використано компаніями фінансової сфери. Клієнтському сервісу месенджер забезпечить оперативну передачу інформації. Також Telegram буде корисний для великого бізнесу з великим документообігом і масивними базами даних, так як програма має можливість зберігання великих обсягів інформації на хмарних сервісах.

Відмітна риса Telegram, що має величезний потенціал для використання в сфері бізнесу, - підтримка розумних ботів. Це акаунти, які автоматично обробляють повідомлення і відповідають на них. Функціонал ботів практично не обмежений, вони можуть здійснювати як прості, так і складні операції: від показу актуальних новин до замовлення обіду в найближчому кафе за все в пару кликів і управління «розумним будинком».

За допомогою спеціального API сторонні розробники можуть створювати «ботів», спеціальні акаунти, керовані програмами. Типові боти відповідають на спеціальні команди в персональних і групових чатах, також вони можуть здійснювати пошук в інтернеті або виконувати інші завдання, застосовуються задля розваг або в бізнесі.

*Особливості, унікальні для Telegram***.** Першочергово Telegram претендував на популярність, пропонуючи користувачам повне шифрування. Хоч сьогодні це характерно для багатьох платформ обміну повідомленнями, Telegram досі є найкращим вибором для тих, хто серйозно ставиться до конфіденційності. Користувачі Telegram можуть на свій вибір зробити так, щоб секретні повідомлення зникли через встановлений час і можуть заборонити знімки екрана розмов. Жодна опція не доступна на WhatsApp.

На додаток до цього, Telegram має перевагу перед WhatsApp в тому, що підтримує наклейки. Оскільки спілкування з кожним днем стає все більш наочним, підтримка наклейок Telegram є привабливою для деяких користувачів. Ще одна унікальна особливість Telegram - це канали. У каналі може публікувати повідомлення лише певний набір користувачів (всі інші читають), він може слугувати корисним та безпосереднім медіа-каналом для видавців чи творців контенту.

Якщо ви надсилаєте друзям багато файлів, ви можете вибрати Telegram серед інших програм для обміну повідомленнями. Вся активність Telegram зберігається в хмарі, тому якщо ви надіслали вкладення одному контакту, ви можете легко надіслати його іншому без необхідності повторного завантаження.

Нарешті, Telegram пропонує кілька варіантів налаштувань, які WhatsApp не підтримує. Користувачі можуть легко змінювати телефонні номери у своєму обліковому записі прямо з меню налаштувань, і коли вони це зроблять, усі їхні контакти (крім тих, кого вони заблокували) автоматично зареєструють цей новий номер. Багатомовні користувачі можуть обирати мову додатку для обміну повідомленнями, що відрізняється від мови їх телефону, WhatsApp не дозволяє цього.

Telegram ідеально підходить для тих, кому потрібно багато пам’яті, щоб зберігати файли, мультимедійні повідомлення, підвищену конфіденційність та доступ до функцій каналів. Оскільки WhatsApp ще не випустив користувальницький інтерфейс чат-ботів, Telegram є кращою платформою для розробників ботів.

У Telegram можна закріпити у вибраних до 5 чатів і визначати пріоритет повідомлень (низький, середній, високий, терміновий). Якщо встановити максимальний пріоритет, то повідомлення будуть приходити навіть у режимі «Не турбувати».

Перевага WhatsApp залишається лише у кількості користувачів, - 1,5 мільярди активних користувачів у місяць проти 200 мільйонів у Telegram.

Ознайомившись з інформацією щодо кожного месенджеру і виходячи з даних у таблицях 2.1 і 2.2 можна зробити такі висновки: враховуючи швидкість відправки повідомлення, високу надійність і відмовостійкість, миттєву хмарну синхронізацію, динамічне завантаження вмісту, простоту і багатоплановість у створенні ботів для розроблення боту моніторингу було обрано месенджер Telegram.

Для зв’язки Telegram bot і Web інтерфейсу NetPing потрібен спеціальний сервіс.

Таблиця 2.1 – Робота з ботами

Особливість	Telegram	Viber	WhatsApp
Основна концепція	Інтеграція месенджера з будь якими сервісами, виконання найрізноманітніших задач в межах Telegram	Чат боти для оптимізації бізнесу та підтримки користувачів при взаємодії з публічними акаунтами	
Реалізація	Особливі Telegram-акаунти без номерів телефону, що контролюються програмами та відповідають чи звертаються до користувачів в рамках можливостей Bot API та фантазії розробників Особливі Telegram-акаунти без	інтерфейс Viber API відповідають користувачам, надаючи зокрема різноманітні бізнес пропозиції та пов’язану інформацію інтерфейс Viber API	Не підтримуються
Обмеження на створення	Майже відсутніконтролюються програмами та	Є певні вимоги до ботів користувачам, надаючи	
Підтримувані типи вмісту	Всі (що підтримуються Telegram) зокрема місцезнаходження та номер	Текст, Зображення, відео контакт, URL, каруселі, графічний зміст, а також місцезнаходження	
Комунікація через вбудований режим	Підтримується (відправка запитів і отримання результатів відповіді)	Обмежена реалізація через розширення	
Додавання ботів до інших чатів	Підтримується (до груп / каналів)	Не підтримується	
Варіанти використання	Отримання новин, інформації повідомлень, покупка товарів і послуг, створення нових інструментів, ігор, соціальних сервісів, оптимізація користувацького досвіду (IV попередній перегляд посилань), навчання, автоматизація, зворотній зв'язок, авторизація та безліч іншого	Отримання інформації, реклами, новин, зв'язок з публічним акаунтом, підтримка	

Таблиця 2.2 – Основні характеристики

Особливість	Telegram	Viber	WhatsApp
Швидкість відправки повідомлень	150 мілісекунд	900 мілісекунд	550 мілісекунд
Обсяг трафіку для відправки повідомлення	Мінімальний	середній	середній
Відмовостійкість та надійність	Висока	середня	середня
Вид синхронізації	Хмарна і миттєва	І первинний пристрій(смартфон\ планшет) і кілька вторинних (планшети\комп'юте-ри), які синхронізуються з первинним пристроєм	І смартфон і 1 пов'язаний з ним комп'ютер
Завантаження вмісту	Динамічне в режимі реального часу, на вимогу	Одноразова доставка з сервера	Одноразова доставка з сервера

2.5 Zapier

Zapier - це платформа, яка з'єднує попарно сервіси, програми та додатки. Користувач вибирає два сервіси, які повинні взаємодіяти і задає умови для їх взаємодії.

Таких взаємодій може бути безліч і називаються вони "Zap". Найпростіший "Zap" складається з двох кроків:

- Trigger, який запускає процес;

- Action - дія, яку потрібно виконати в такому випадку.

Для передачі даних послідовність додатків наступна: Trigger (звідки брати дані) -> Action (куди їх передавати), (рис.2. 1).

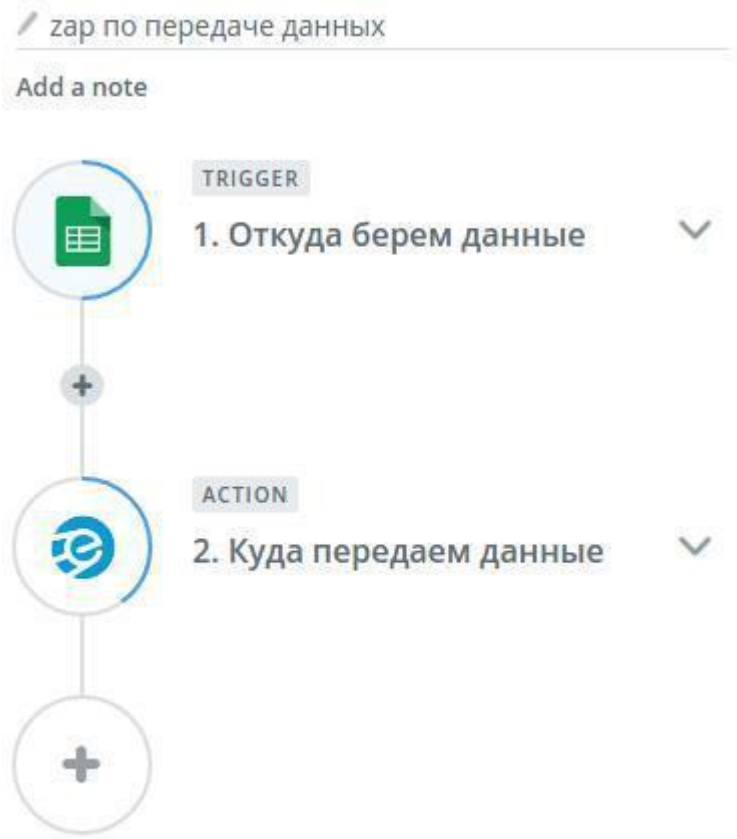


Рисунок 2.1 - Послідовність передачі даних додатків

Для роботи з Zapier не потрібні навички програмування.

2.6 Методи взаємодії з ботом

Telegram дозволяє встановлювати свої сертифікати https, що дозволяє не купувати дорогий сертифікат.

Для взаємодії з користувачем в Telegram використовуються два принципово різних способи.

Перший – **getUpdates**. Цей метод використовується для отримання оновлень через long polling. Відповідь повертається у вигляді масиву об'єктів Update. У даного способу оновлень є маса недоліків. Необхідність самостійно запитувати з сервера список повідомлень користувачів, що не дуже зручно. Для

цього необхідно запитувати кожні n секунд з сервера телеграма дані. Це ресурсозатратно і не раціонально.

Другий – **setWebHook.** Існує ще один спосіб отримання повідомлень від бота. Це використання WebHook. Ідея полягає в тому, що сервер сам буде надсилати нам повідомлення користувача, а ми будемо вирішувати, що з ними робити. Кожен раз при отриманні оновлення на цю адресу буде відправлений HTTPS POST з серіалізованим в JSON об'єктом Update. В основному ми будемо працювати з об'єктом Message, який, відповідно, отримаємо з Update.

2.7 Webhooks

Webhooks - це один із способів того, як програми можуть надсилати автоматизовані повідомлення чи інформацію іншим програмам. Саме так PayPal повідомляє вашому банківському додатку, коли хтось перераховує кошти на вашу картку.

Це простий спосіб для того, щоб ваші онлайн-акаунти могли "спілкуватися" між собою і отримувати повідомлення автоматично, коли трапляється щось нове. Вам потрібно знати, як користуватися Webhooks, якщо ви хочете автоматично пересилати дані з однієї програми в іншу.

Є два способи спілкування ваших додатків один з одним для обміну інформацією: polling та Webhooks. Polling - це як стукати у двері вашого друга і запитати, чи є у них цукор. Webhooks - це наче хтось кидає мішок із цукром у ваш будинок, коли ви його купуєте.

Webhooks - це автоматизовані повідомлення, що надсилаються з додатків, коли щось відбувається. Вони мають повідомлення і надсилаються за унікальною URL-адресою - по суті, номером телефону або адресою програми.

Вони дуже схожі на SMS-сповіщення. Скажімо, ваш банк надсилає вам SMS, коли ви робите нову покупку. Ви вже сказали банку свій номер телефону,

щоб вони знали, куди надіслати повідомлення. Вони набирають текст "Ви щойно витратили 100 гривень у АТБ" і надсилають їх на ваш номер телефону +380xxxxxxxxx. Щось сталося у вашому банку, і ви отримали повідомлення про це. Webhooks працює по тому ж принципу.

Найпростіший спосіб надсилання даних до Webhooks за URL-адресою - це HTTP GET-запит. Буквально це означає додати дані до URL-адреси та пропінгувати адресу (або ввести її в адресний рядок браузера). Так само ви можете відкрити сайт zapier.com, ваші програми можуть надсилати повідомлення один одному, позначаючи додатковий текст із позначкою питання в кінці адреси веб-сайту.

Згадайте, коли вам доводилось перевіряти електронну пошту, щоб побачити чи з’явились нові повідомлення. Завдяки Webhooks можна уникнути цієї проблеми. Вам більше не потрібно буде перевіряти чи з’явилась нова інформація. Натомість, коли щось відбудеться, вони видадуть вам повідомлення про це і не будуть витрачати час на перевірку і очікування.

Використання Webhooks в будь-якому додатку із Zapier. У вас є програма, яка може надсилати або отримувати дані за допомогою Webhooks, і ви хочете підключити її до іншого додатку, який не працює з Webhooks. В такому випадку може допомогти Zapier. Маючи понад тисячу підключених додатків, є великий шанс, що додаток, який ви хочете використовувати, працює із Zapier. Після цього Zapier зможе обробляти частину Webhooks, щоб з'єднати обидві програми. Скажімо, у вас є програма, яка може обмінюватися даними з URL-адресою Webhooks. Щоб підключити її до інших додатків, потрібно зробити новий Zap - те, що ми називаємо автоматизованими робочими процесами програми Zapier - і вибрати додаток Webhooks у Zapier як тригерний додаток. Вибрати Catch Hook, який може отримати запит GET, POST або PUT від іншого додатка. Zapier надасть вам унікальну URL-адресу Webhooks - скопіюйте її, а потім додайте її до поля URL-адреси Webhooks програми у своїх налаштуваннях.

Тепер ви можете використовувати Webhooks в іншому додатку. Виберіть action app - додаток, до якого потрібно надіслати дані. Ви побачите поля форми

для додавання даних у цю програму. Натисніть на кнопку «+» праворуч, щоб вибрати дані з Webhooks, які ви хочете надіслати іншому додатку. Перевірте і ввімкніть Zap, і наступного разу, коли додаток тригера надішле дані у Webhooks, Zapier автоматично додасть його до вибраного додатку дій.

Нарешті, вставте URL Webhooks з програми, в яку ви хочете отримати дані, у поле URL у налаштуваннях Webhooks Zapier. Ви можете вибрати спосіб серіалізації даних. Потім Zapier автоматично надсилатиме всі дані з тригерного додатку до Webhooks, або ви можете встановити конкретні змінні даних із полів Дані.

Увімкніть Zap, і коли що-небюудь нове трапиться у вашому тригерному додатку, Zapier скопіює дані та надішле їх у URL-адресу Webhooks іншого вашого додатка.

2.8 Висновки до розділу

У даному розділі було розглянуто існуючі засоби моніторингу. Обрано найбільш відповідні компоненти для системи диспетчеризації і сповіщення. В якості контролеру було обрано пристрій uniping server solution v3/sms, до нього можна підключити 8 датчиків і організувати процес повідомлення про критичні зміни у фізичному стані серверного приміщення.

Серед типів сповіщення було обрано месенджер, так як він забезпечує миттєве, на відміну від електронної пошти, і безкоштовне, на відміну від SMS, сповіщення у режимі реального часу.

Серед месенджерів вибір зупинився на Telegram. Це найбільш захищенний, надійний і відмовостійкий месенджер з найшвидшою відправкою повідомлень і хмарною синхронізацією. Він підтримує можливість створення і використання ботів. У Telegram можна закріпити у вибраних до 5 чатів, тому бот моніторингу завжди буде перед очима при відкритті месенджеру. Завдяки можливості вибрати

максимальний пріоритет повідомлень сповіщення про зміни стану серверного приміщення будуть приходити навіть у режимі «Не турбувати».

3 РОЗРОБКА TELEGRAM БОТУ ДЛЯ МОНІТОРИНГУ ПОТОЧНОГО СТАНУ СЕРВЕРНОЇ КІМНАТИ

3.1 Отримання інформації про спрацювання датчиків, підключених до системи моніторингу за запитом

На віртуальній машині Oracle VM VirtualBox, встановлено OS Ubuntu 18.04, інтерпретатор мови програмування Python. Встановимо менеджер пакетів pip:

```
kate@kate-VirtualBox:~$ sudo apt install python3-pip
```

3.1.1Реєстрація нового бота

Для створення нових ботів існує спеціальний *Telegram bot @BotFather*. Додати цей bot в месенджері досить просто. У пошуку додатка вводимо назву бота, після чого відкриється вікно взаємодії з ним. У вікні присутня кнопка «Розпочати», якщо встановлена українська локалізація. Необхідно її натиснути, тоді активується режим діалогу. Увесь процес створення нового бота буде здійснюватися за допомогою спілкування з *@BotFather*. Ініціюємо діалог і запитуємо список доступних команд (рис. 3.1):

Вигадуємо ім'я, пишемо його і відправляємо. Якщо ім'я не зайнято, то bot створюється, і буде запропоновано створити користувача. Користувач може бути з будь-яким іменем, але повинен закінчуватися на bot. У нашому прикладі ім'я бота і користувача - network_monitoring_bot (рис.3.3).

Після реєстрації імені основна частина створення бота закінчена. У цьому повідомленні буде надано token (1), необхідний, щоб отримати доступ до API Telegram, який знадобиться пізніше.

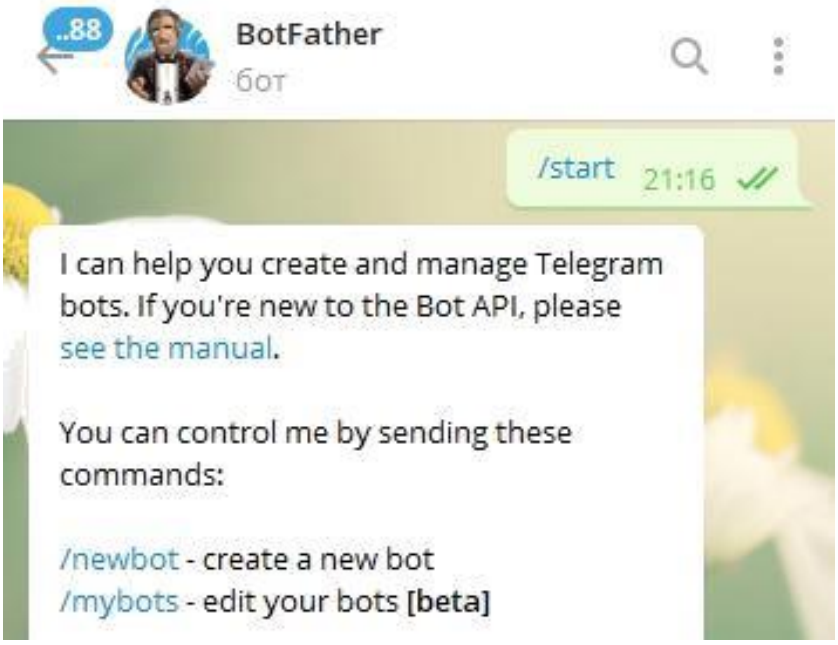


Рисунок 3.1 – Діалогове вікно: список доступних команд

Створюємо bot (рис. 3.2):

Рисунок 3.2 – Створення bot

Додатково ще можна вказати перелік підтримуваних функцій, який буде виводитися в діалоговому вікні, коли вводиться символ «/». Для цього потрібно виконати наступні дії (рис.3.4).

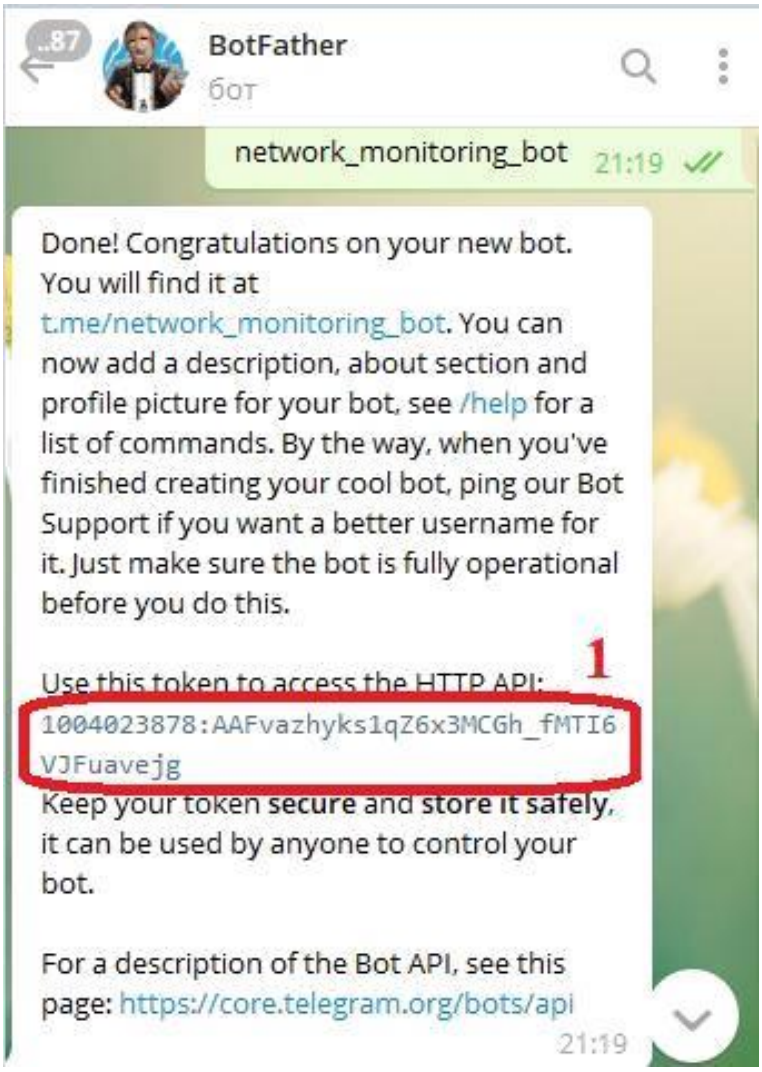


Рисунок 3.3 – Діалогове вікно: присвоєння ім’я боту

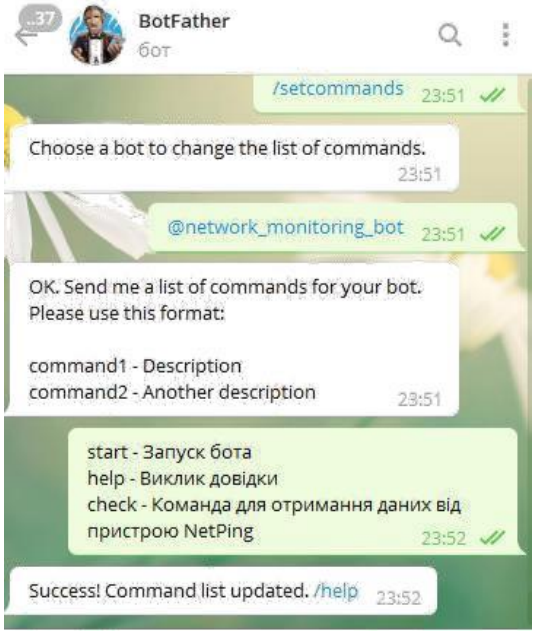


Рисунок 3.4 – Діалогове вікно: перелік підтримуваних функцій

3.1.2 Програмування бота

Тепер необхідно запрограмувати @network_monitoring_bot. Виконувати ми це будемо через представлений API «Телеграм» за допомогою програми на мові програмування Python. Усі роботи виконуються в терміналі Linux.

Спочатку встановимо необхідні пакети за допомогою наступних команд:

```
kate@kate-VirtualBox:~$ pip3 install pyTelegramBotAPI
```

```
kate@kate-VirtualBox:~$ pip3 install requests
```

```
kate@kate-VirtualBox:~$ nano conf_bot.py
```

Потім створюємо файл конфігурації бота з наступним змістом, рис. 3.5.

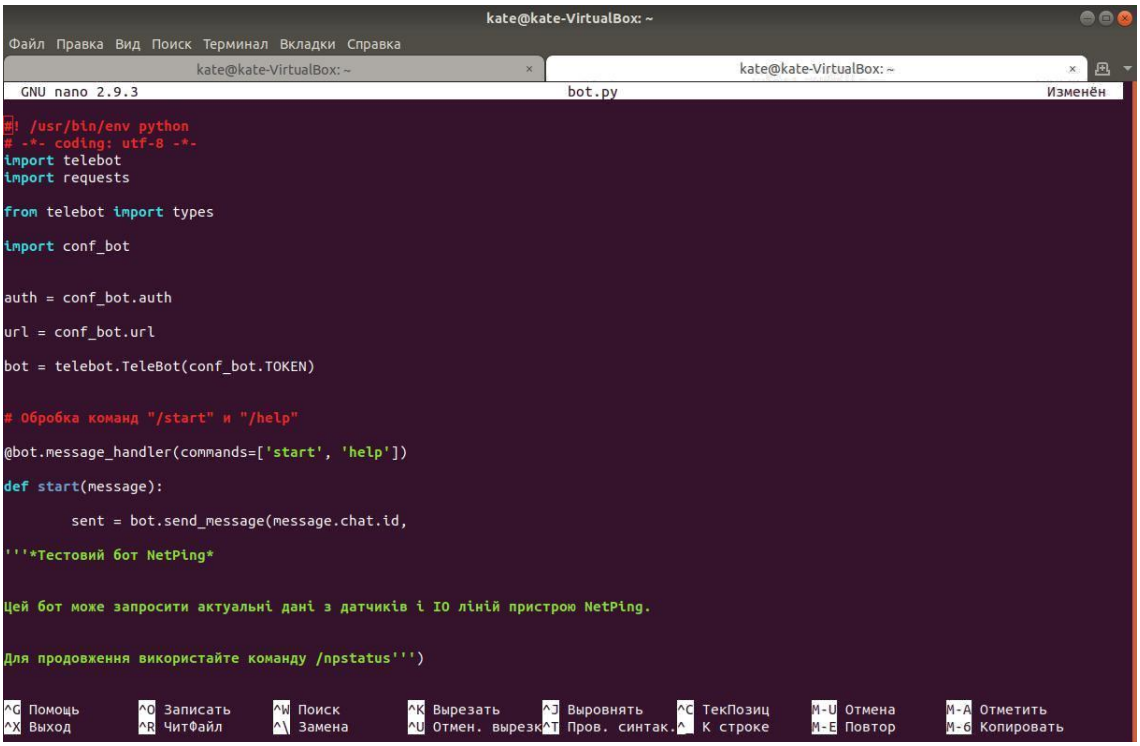


Рисунок 3.5 - Файл конфігурації бота

Далі створюємо основний файл нашого бота (рис.3.6).

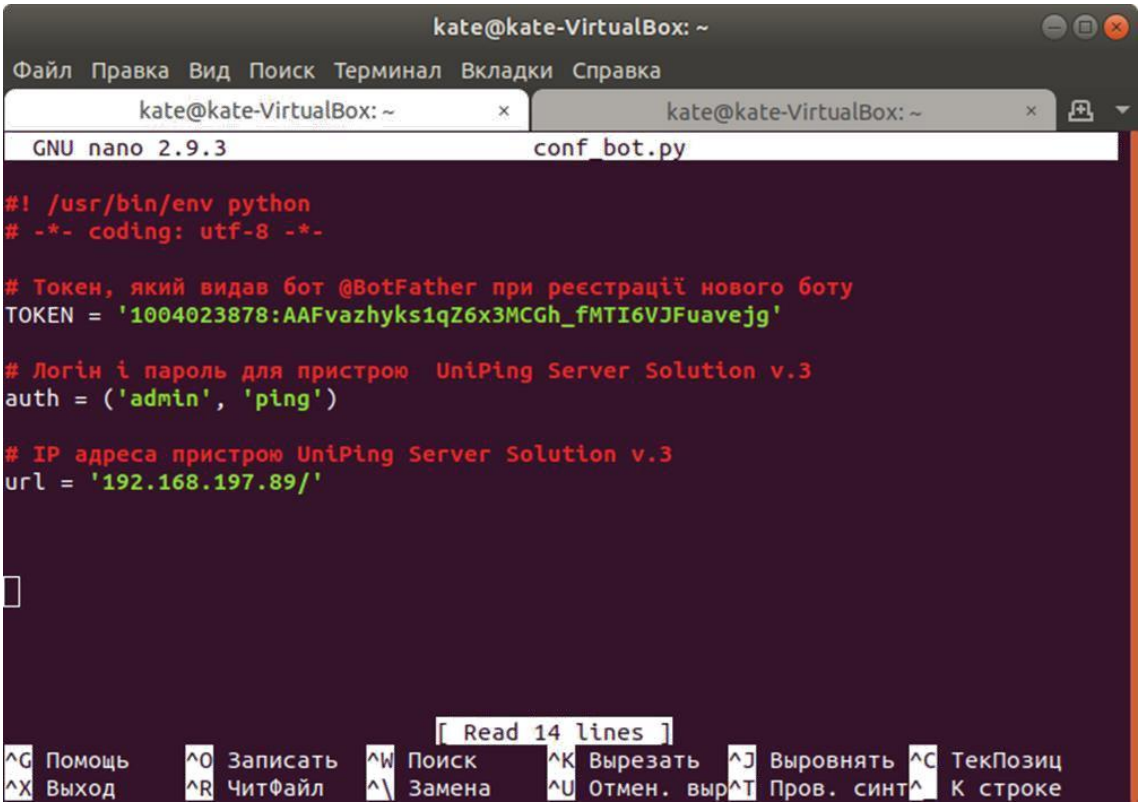


Рисунок 3.6 - Основний файл бота

Тепер запускаємо створений файл на виконання. Якщо в терміналі Ubuntu нічого не виводиться, і термінал виглядає «завислим» - значить, все зроблено правильно, і @network_monitoring_bot працює.

3.1.3 Робота з ботом

Не закриваючи термінал відкриваємо @network_monitoring_bot в Telegrami, запускаємо бота кнопкою «Розпочати», рис. 3.7:

Отримуємо вітальне повідомлення з описом бота і можливих команд, рис.3.8.

Далі пишемо боту команду «/check» і отримуємо запрошення вибрати параметр, який нас цікавить, рис. 3.9.

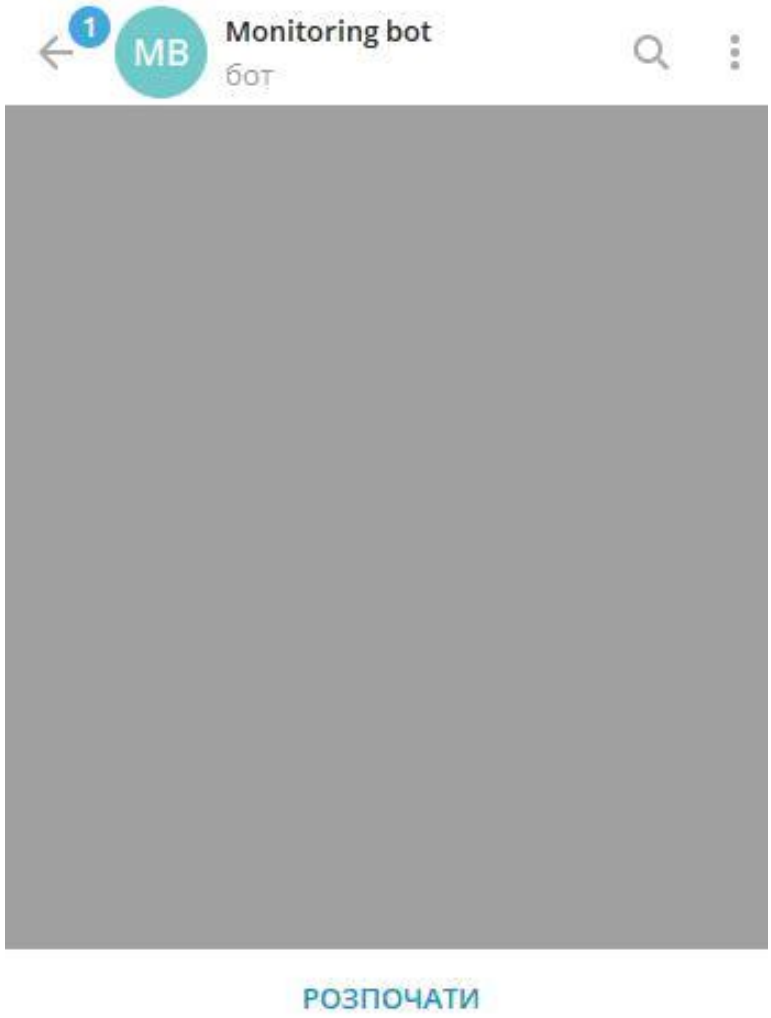


Рисунок 3.7 - Запуск бота

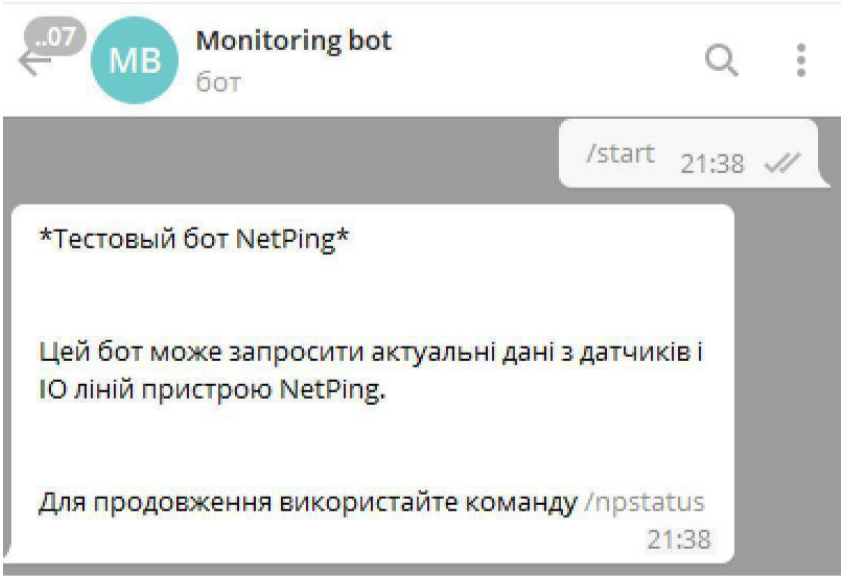


Рисунок 3.8 – Діалогове вікно з описом бота і можливих команд

Рисунок 3.9 – Вибір параметрів боту

Натискаємо на потрібну нам кнопку і отримуємо дані від датчиків або IO ліній пристрою моніторингу (рис. 3.10). Для прикладу була натиснута кнопка «Температура»:

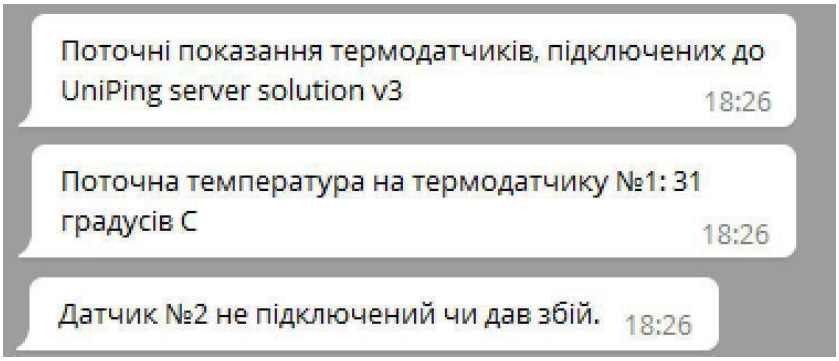


Рисунок 3.10 - Отримання даних від датчиків

В результаті перерахованих вище дій ми отримаємо бот для месенджера Telegram, який може в будь-який час і в будь-якому місці (при наявності доступу до мережі Інтернет) опитати пристрій моніторингу і отримати дані про стан датчиків.

3.2 Налаштування автоматичного отримання інформації про спрацювання датчиків

Отримання інформації від системи моніторингу за запитом реалізовано. Далі створимо отримання інформації в «Telegram» в автоматичному режимі з використанням сервісу «Zapier».

3.2.1 Реєстрація та налаштування нового бота

На першому етапі створимо новий bot. Процедура аналогічна створенню першого бота (рис.3.11). Ім'я нового бота @Monitoring_and_notification_bot. Token нам знадобиться пізніше.

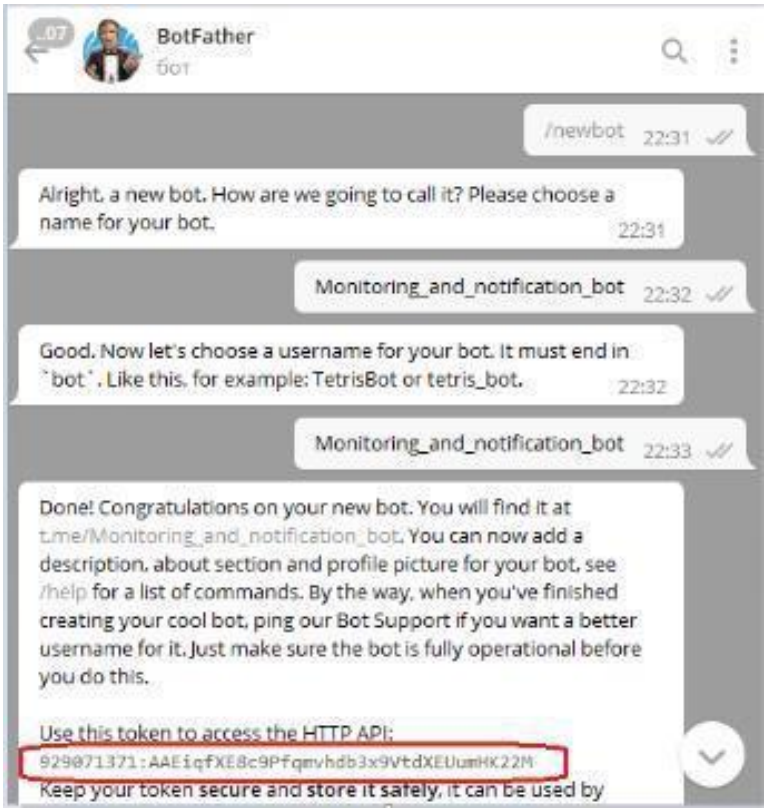


Рисунок 3.11 – Створення нового боту

Далі потрібно додати в Telegram службовий bot @ChatFuel, за допомогою якого ми додамо нашому новому боту розширений функціонал, який дозволить @Monitoring_and_notification_bot отримувати повідомлення з сервісу «Zapier».

Переходимо за посиланням з повідомлення бота @Chatfuel для встановлення @Monitoring_and_notification_bot надбудови «Chatfuel» (рис.3.12).

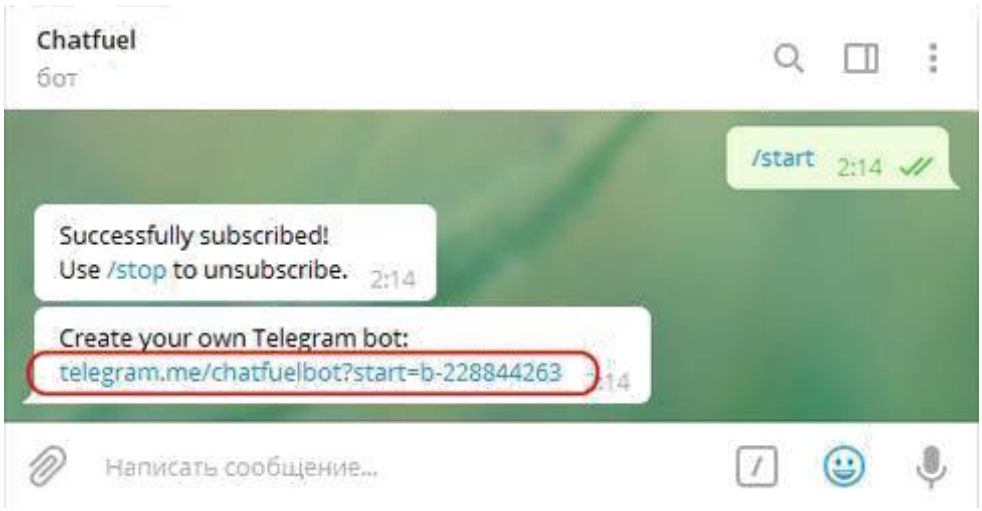


Рисунок 3.12 – Перехід за посиланням з повідомлення боту

Після переходу за посиланням натискаємо кнопку «Розпочати»: І натискаємо в меню, що з’явилося кнопку «Новий бот», рис. 3.13.

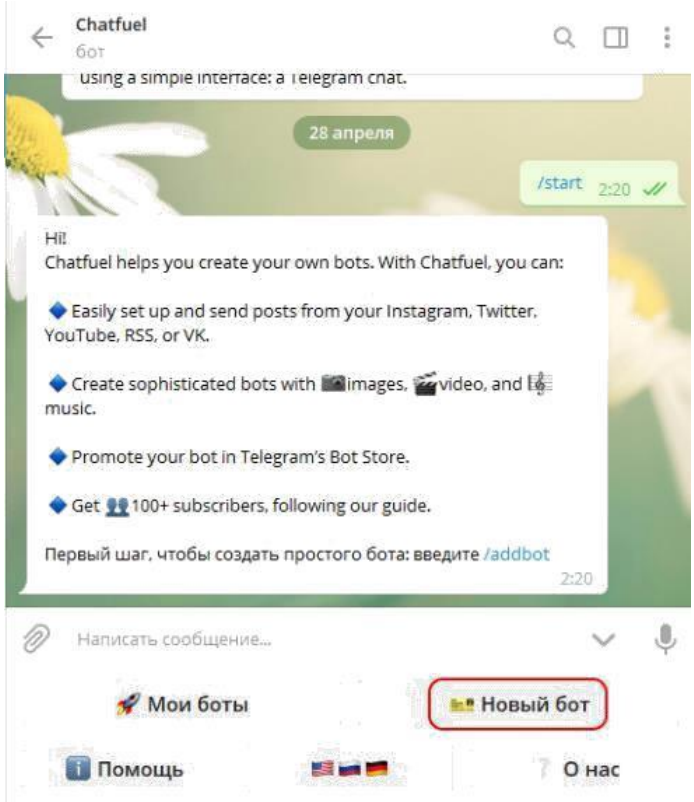


Рисунок 3.13 – Новий бот

Далі, в полі введення повідомлення вказуємо token, який ми отримали раніше при створенні @Monitoring_and_notification_bot.

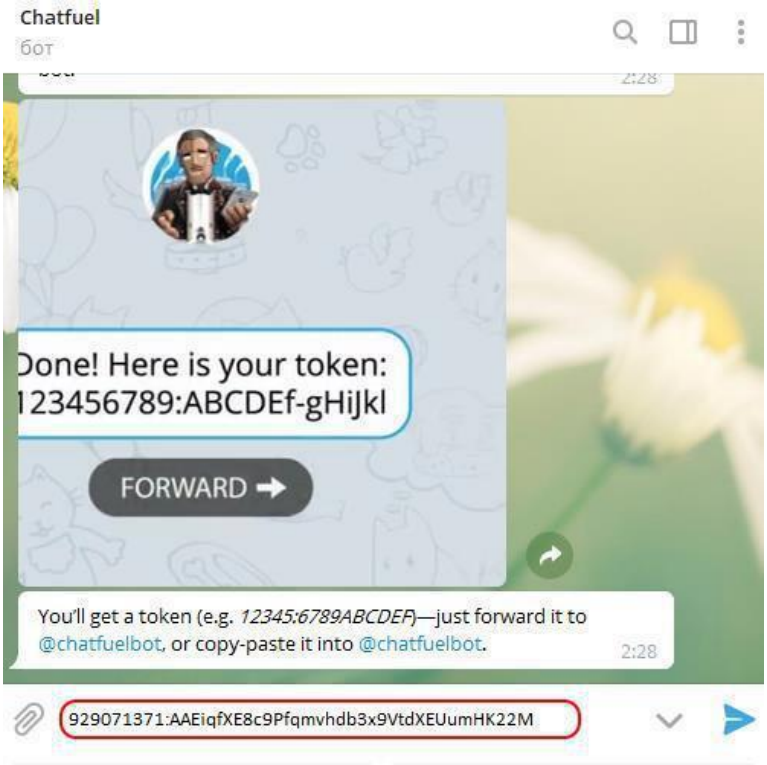


Рисунок 3.14 – Вікно введення повідомлення

Після введення значення token ми отримуємо повідомлення про успішну установку надбудови для нашого бота. Додаємо @Monitoring_and_notification_bot в контакт лист натисканням на посилання:

Рисунок 3.15 - Повідомлення про успішну установку надбудови для бота

Запускаємо його кнопкою «Розпочати». Потім переходимо в розділ управління, щоб створити унікальний ключ, необхідний для прив'язки @Monitoring_and_notification_bot до системи «Zapier», рис. 3.16.

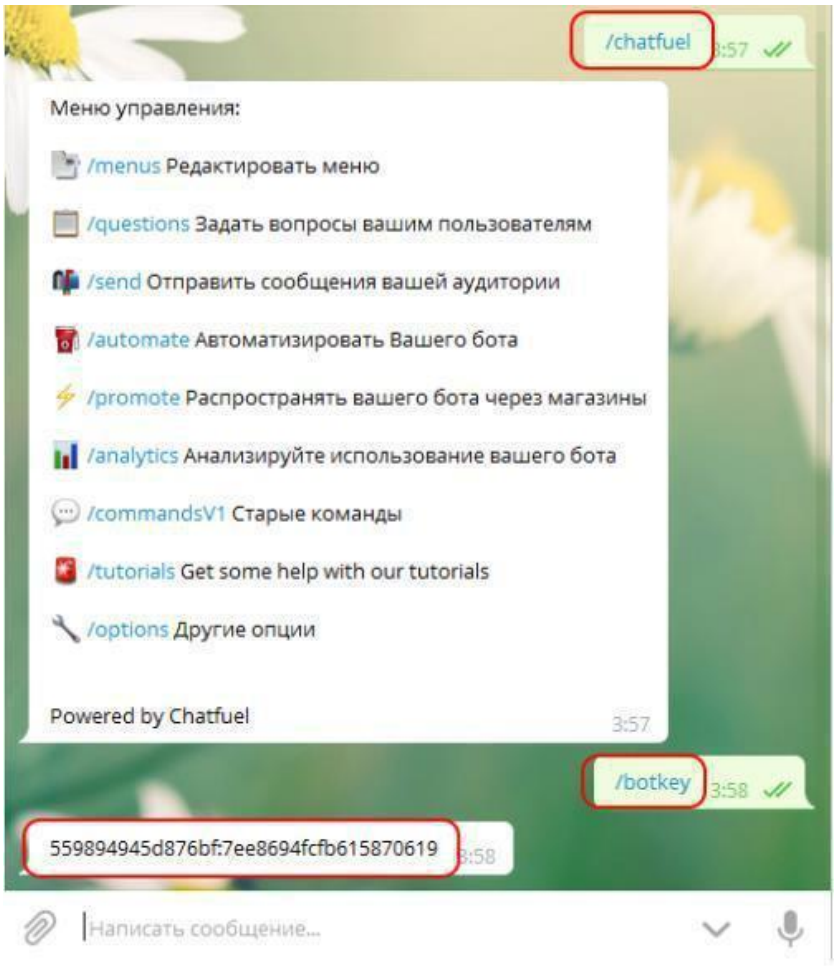


Рисунок 3. 16 – Створення унікального ключа

3.3 Налаштування Zapier

Далі переходимо на сайт zapier.com. Після реєстрації і авторизації ми можемо створити автоматичну дію, так званий «Zap», який буде відправляти повідомлення @Monitoring_and_notification_bot при реєстрації подій на пристрої моніторингу.

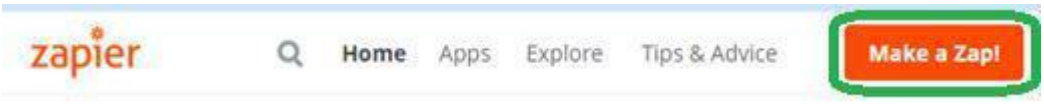


Рисунок 3.17 – Інформаційне вікно «Zapier»

Далі вибираємо Trigger App, при спрацьовуванні якого будуть виконуватися автоматичні дії (рис.3.18). Нам потрібно буде отримувати Webhook повідомлення від пристрою моніторингу при спрацюванні датчиків і зміні станів IO ліній.

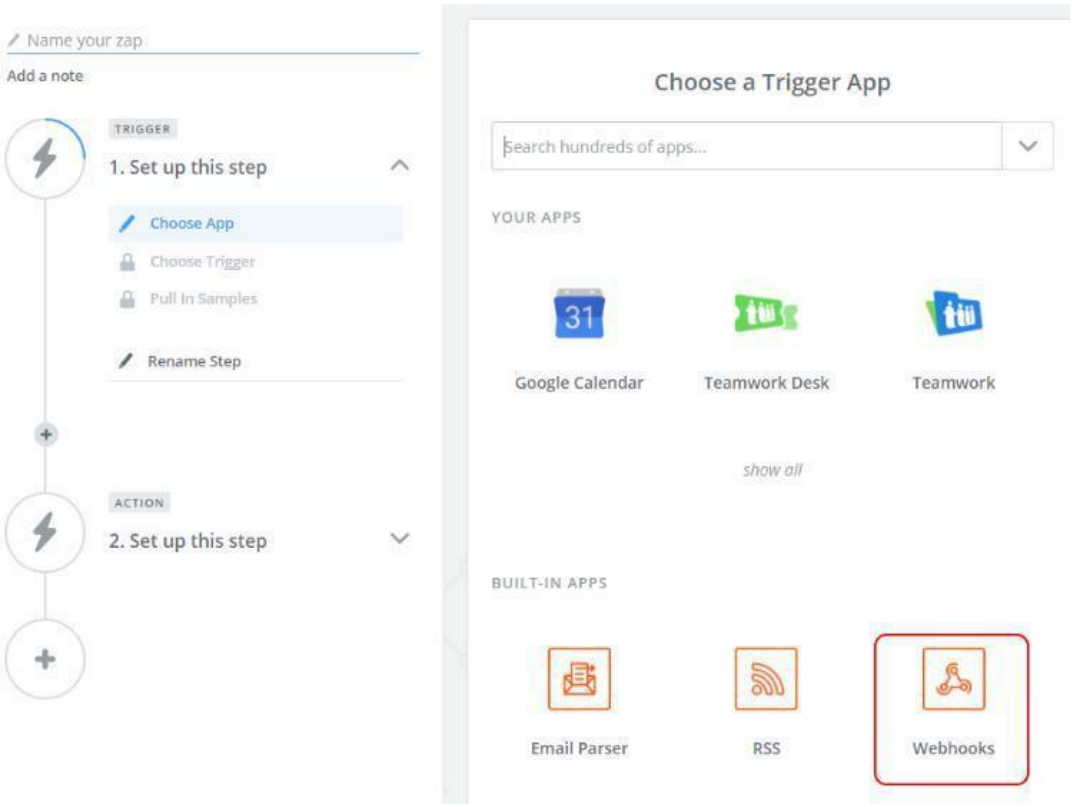


Рисунок 3.18 – Діалогове вікно

Далі вибираємо тип повідомлень, як на знімку екрану (рис. 3.19), і переходимо до наступного кроку налаштування.

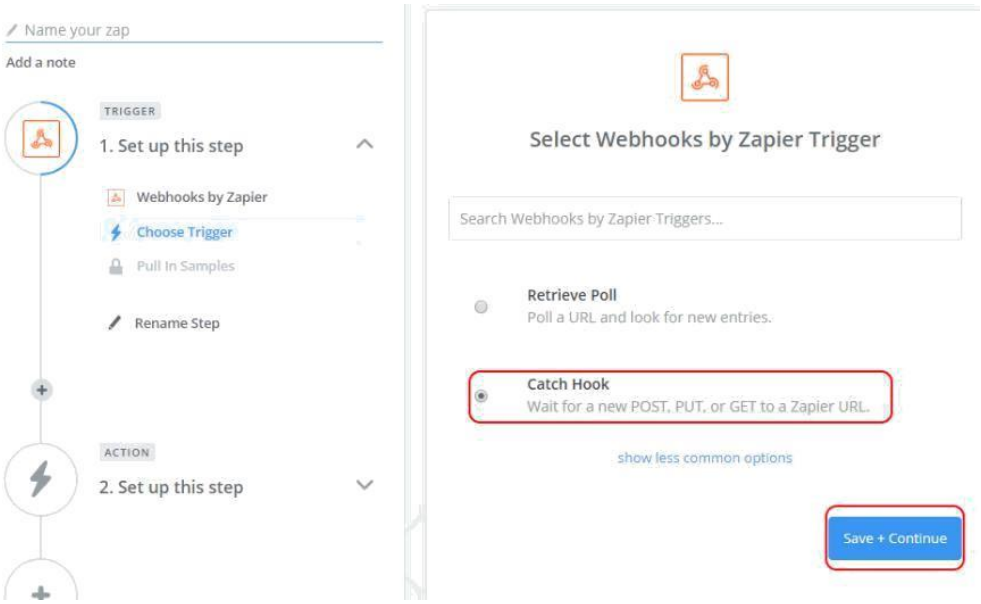


Рисунок 3.19 – Вікно вибору типу повідомлень

На наступному кроці все залишаємо за замовчуванням і продовжуємо налаштування, рис.3.20:

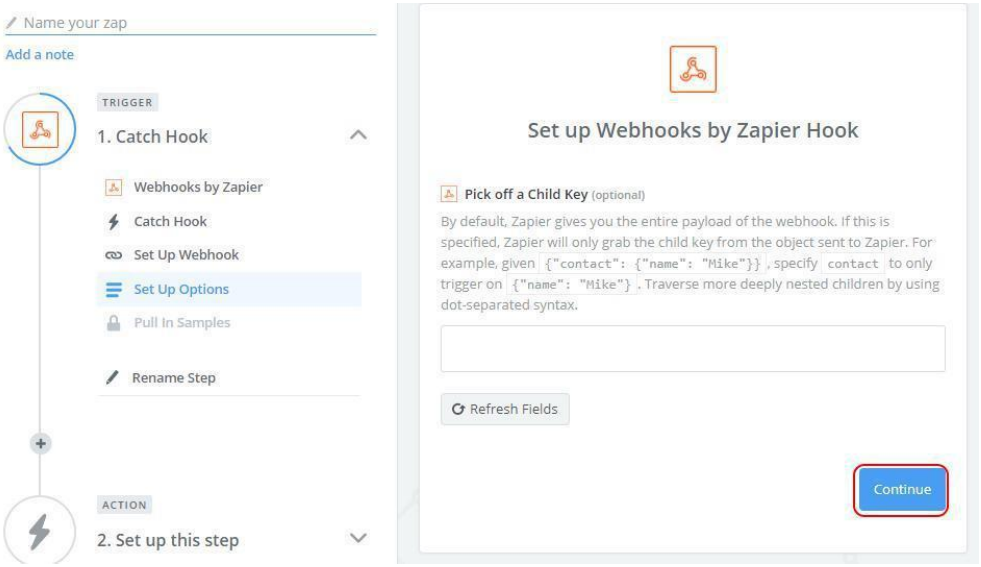


Рисунок 3.20 – Продовження налаштування

На наступному кроці буде створене унікальне посилання, по якому буде передаватися Webhook в «Zap» (рис.3.21). Натискаємо кнопку «Копіювати» в полі посилання:

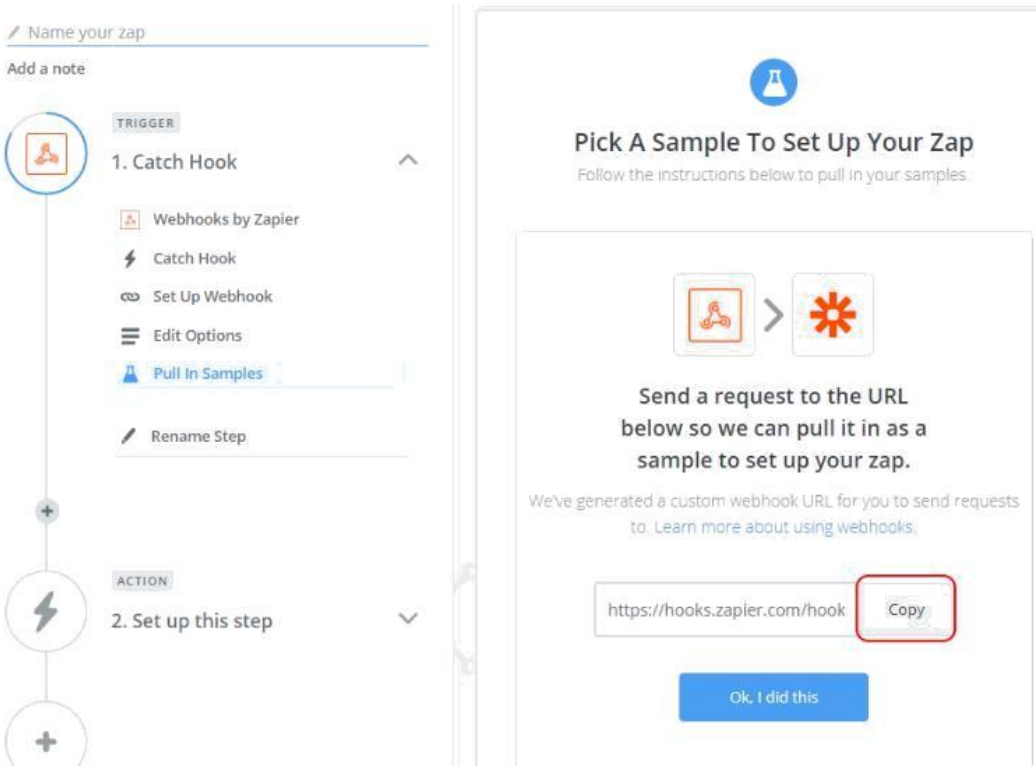


Рисунок 3.21 - Створення унікального посилання

Тепер перейдемо до web-інтерфейсу нашого пристрою моніторингу. Необхідно налаштувати повідомлення. Щоб створити повідомлення необхідно перейти у розділ «ПОВІДОМЛЕННЯ» і натиснути на рядок «натисніть сюди для додавання нових даних» (рис.3.22).

Рисунок 3.22 - Налаштування повідомлення

На цьому етапі створимо повідомлення про перевищення верхньої межі нормальної температури на датчику температури:

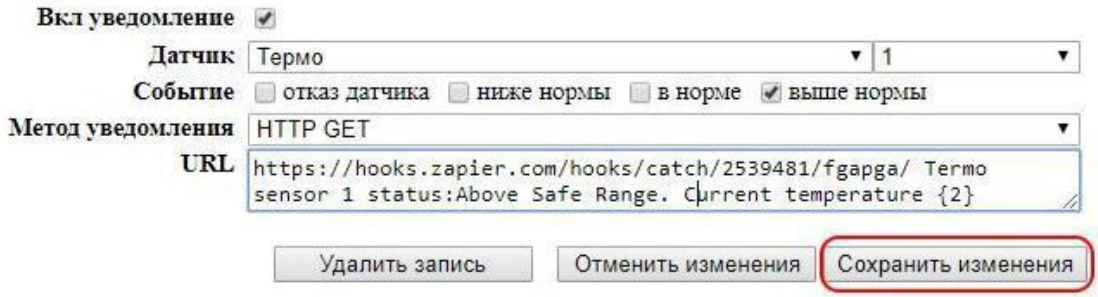


Рисунок 3.23 – Створення повідомлення

Для цього зазначимо наступні параметри:

- **Увімкнути повідомлення**;
- **Датчик** - вибираємо зі списку «Термо» і «1»;
- **Подія** - «Вище норми»;
- **Метод повідомлення** - вибираємо зі списку «HTTP GET»;

- **URL** - в цьому полі вказуємо унікальне посилання на «Zap», яке ми скопіювали раніше, і через пробіл пишемо повідомлення. На жаль, система «Zapier» не підтримує кирилицю.

Натискаємо «Зберегти зміни». Потім переходимо на сторінку «Термодатчики» і штучно викликаємо спрацьовування події «Температура вище норми», задавши верхню межу норми менше поточного значення температури на датчику (рис. 3.24).

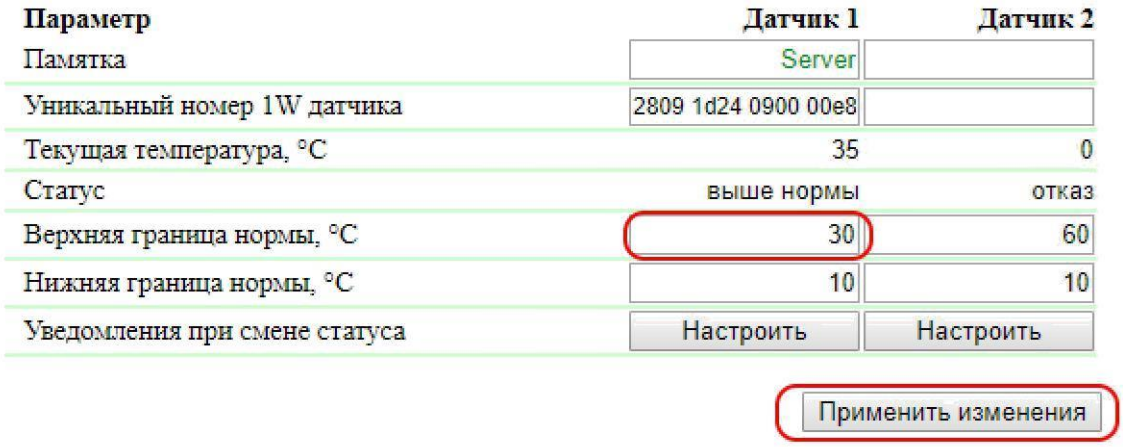


Рисунок 3.24 – Задання температурних показників

Натискаємо кнопку «Застосувати зміни», повертаємося до «Zapier» і натискаємо кнопку «Так, я зробив це», рисунок 3.25.

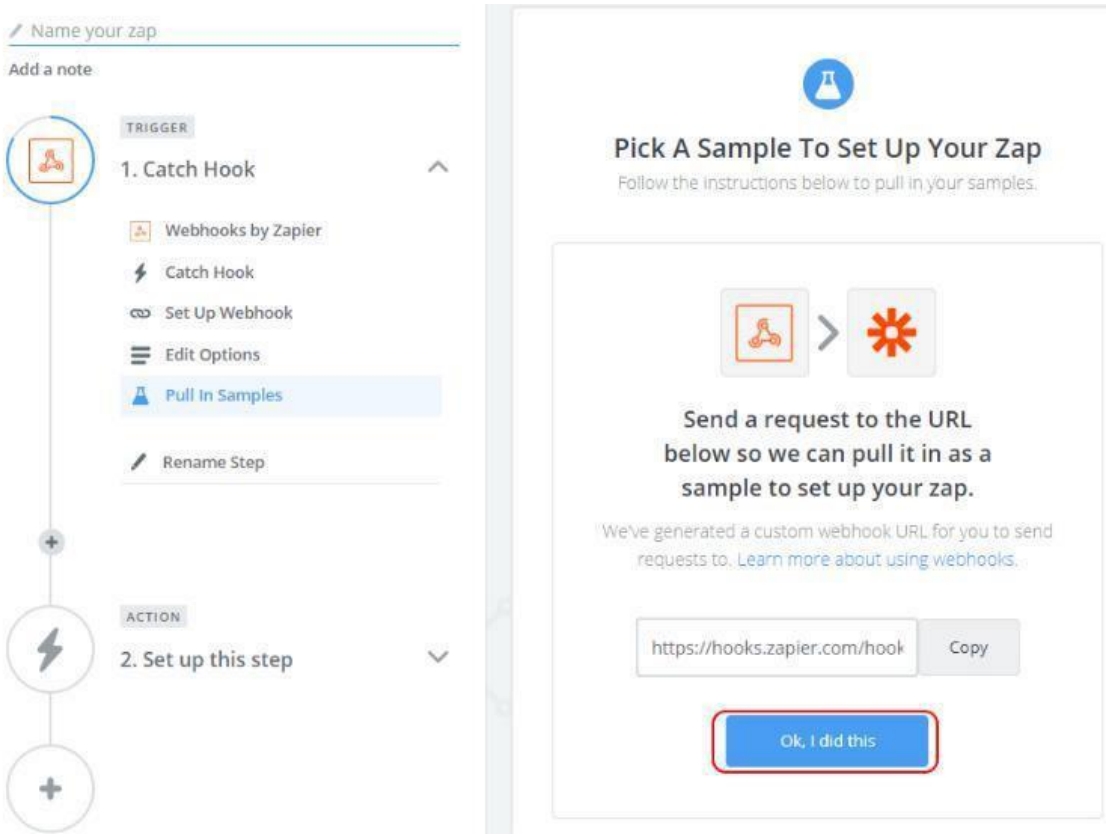


Рисунок 3.25 – Завершення змін

Якщо в налаштуваннях нашого пристрою моніторингу ми все зробили правильно, то на наступному кроці ми отримаємо вхідне повідомлення. На цьому налаштування Trigger завершено (рис. 3.26). Переходимо до налаштувань «Дії»:

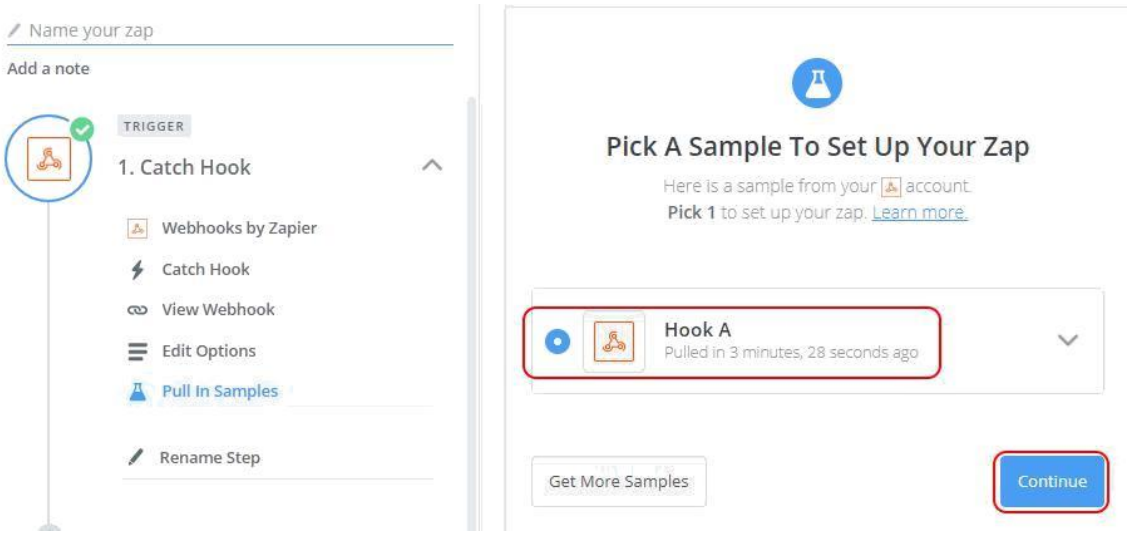


Рисунок 3.26 – Завершення налаштування Trigger

На наступному кроці вибираємо Action App (рис.3.27).

Рисунок 3.27 – Налаштування Action App

Далі вибираємо тип дії, яка буде виконана при спрацьовуванні Trigger App, зберігаємо і продовжуємо (рисунок 3.28).

На наступному кроці нам необхідно прив'язати аккаунт нашого @Monitoring_and_notification_bot до системи «Zapier». Для цього потрібно ввести ключ, який ми отримали раніше (рис.3.29).

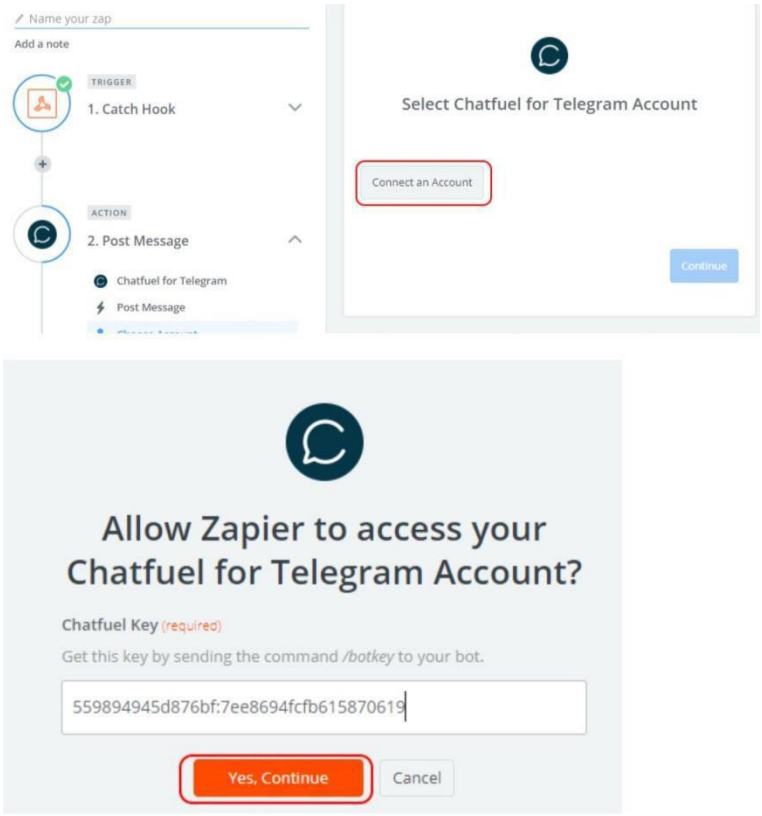


Рисунок 3.28 - Обрання типу дії, яка буде виконана при спрацьовуванні Trigger App

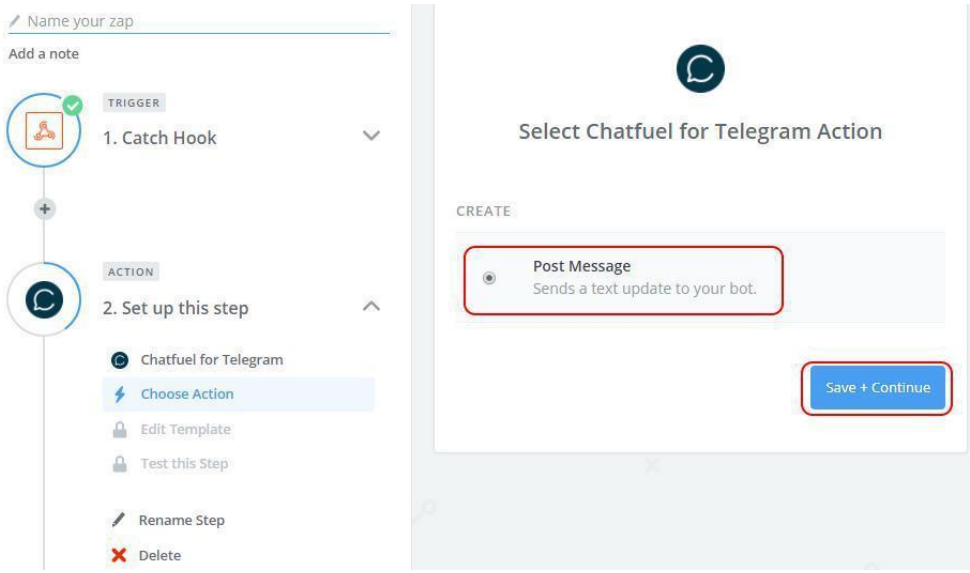


Рисунок 3.29 - Прив'язка аккаунта до системи «Zapier»

Підтверджуємо зміни. Потім система запропонує нам задати текст повідомлення, яке відправлятиметься @Monitoring_and_notification_bot. Вибираємо повне повідомлення і йдемо далі (рис. 3.30).

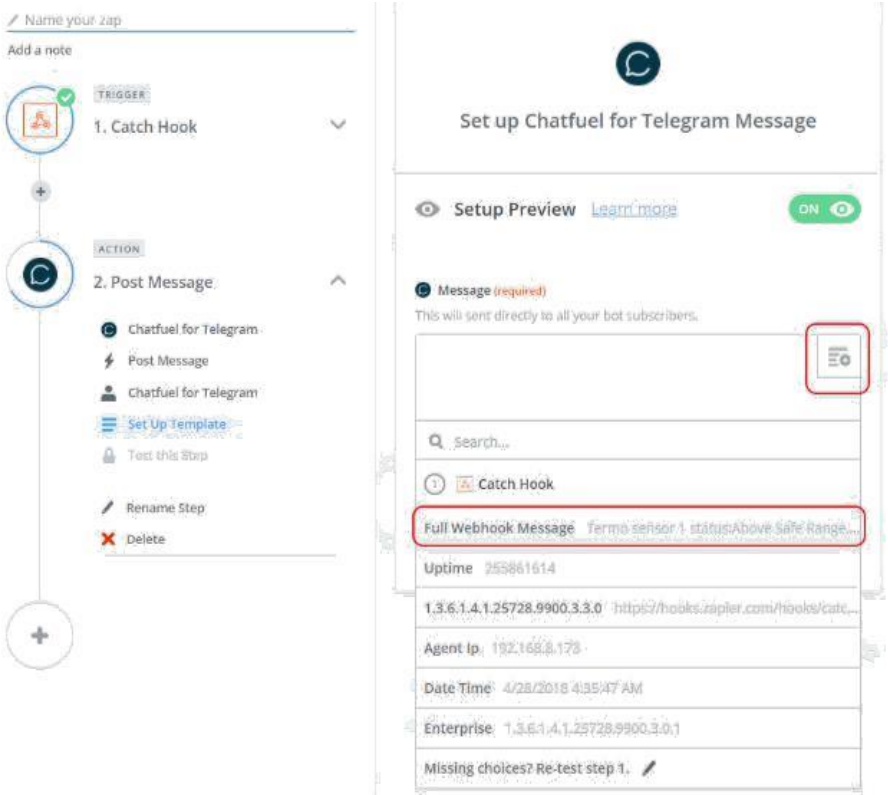


Рисунок 3.30 – Обрання типу повідомлень

На наступному кроці буде виконано тестування (рис.3.31).

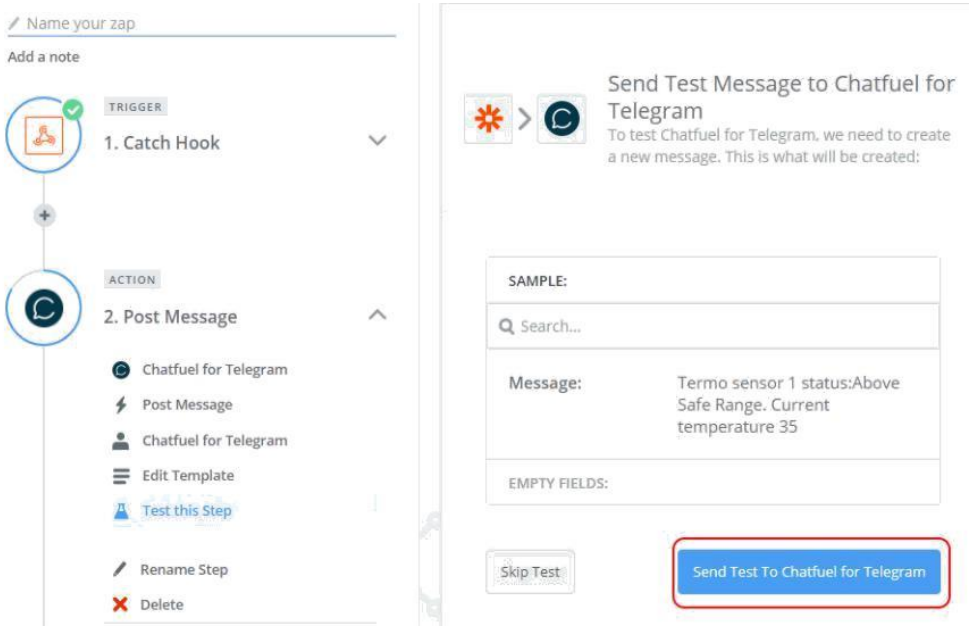


Рисунок 3.31 - Виконання тестування

І, якщо тестування виконано успішно, ми отримаємо повідомлення про це в системі «Zapier» і повідомлення в Telegram. На цьому завершуємо налаштування (рис.3.32).

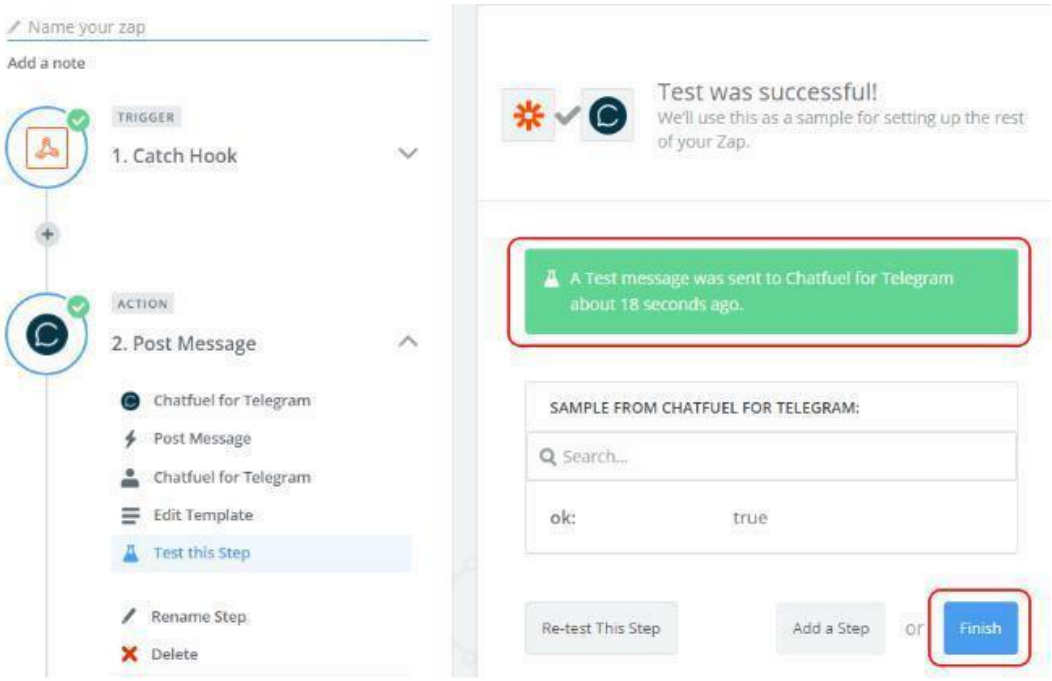


Рисунок 3.32 – Завершення тестування

Після цього нам буде запропоновано назвати наш «Zap» і запустити його на виконання. Напишемо ім'я в текстовому полі і переведемо перемикач виконання в положення «ввімкнено»(рис. 3.33).

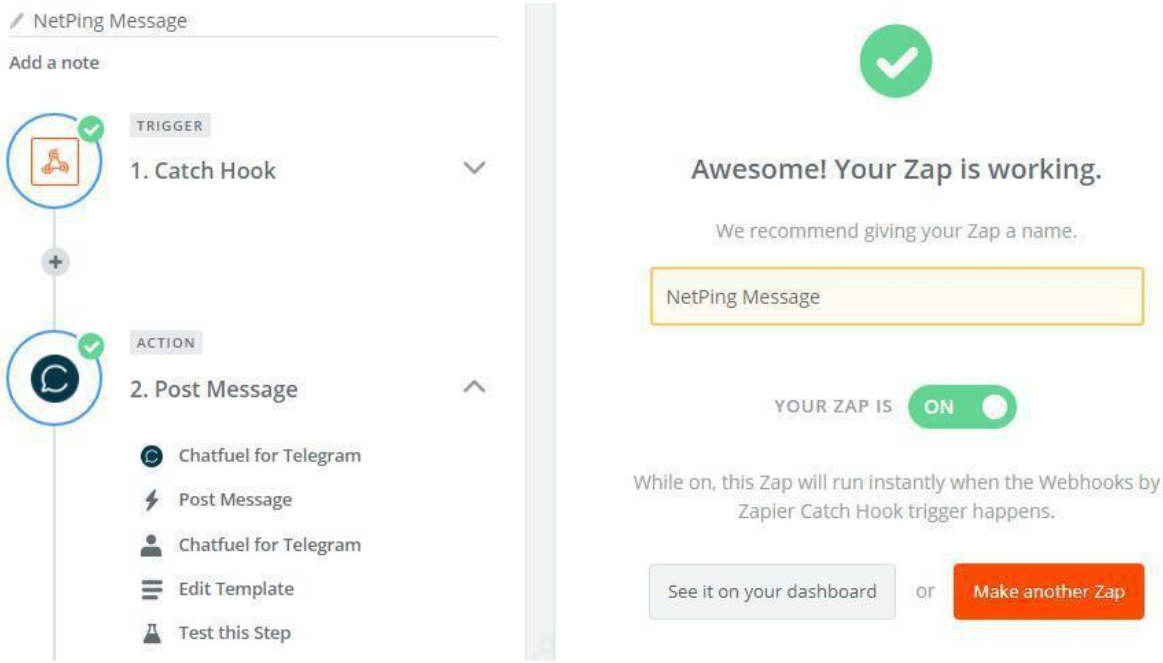


Рисунок 3.33 – Запит що до обрання ім’я

Після цього отримаємо повідомлення, що все працює. На цьому налаштування для передачі повідомлень від пристрою моніторингу в Telegram можна вважати закінченим.

Повернемося до веб-інтерфейсу пристрою моніторингу і додамо важливі повідомлення для моніторингу датчиків. Налаштування виконуються аналогічно налаштувань для датчика температури, які були описані вище. Після створення нових повідомлень на пристрої моніторингу якимось чином змінювати налаштування сервісу «Zapier» немає необхідності (рис.3.34). "Підхоплення" нових повідомлень відбудеться автоматично.

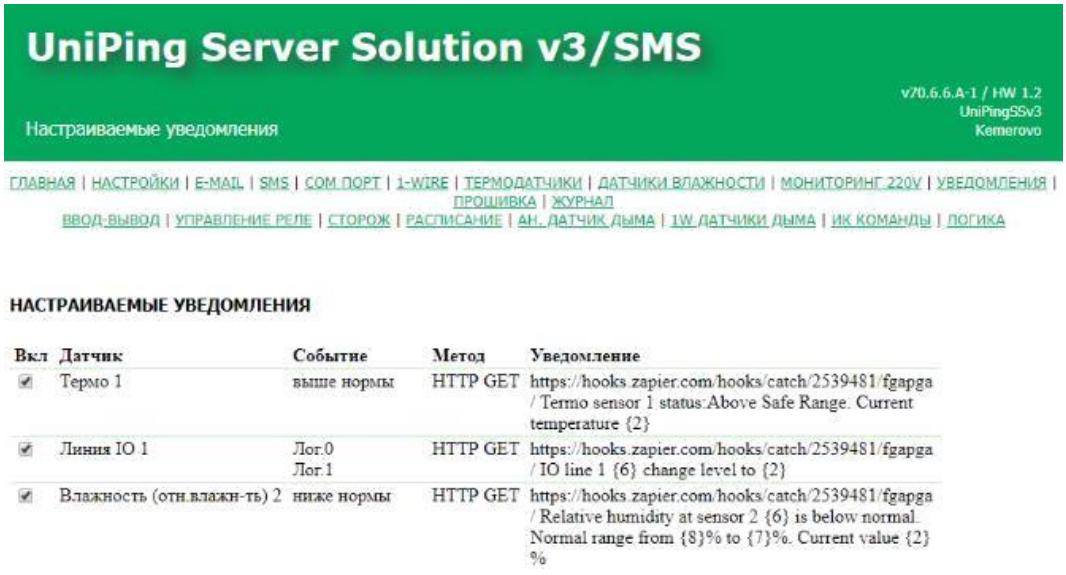


Рисунок 3.34 – Автоматичне оновлення нових повідомлень

В результаті всіх вищенаведених налаштувань в момент зміни статусу датчиків, підключених до нашого пристрою моніторингу, в Telegram надходять повідомлення, що наведені на рисунку 3.35.

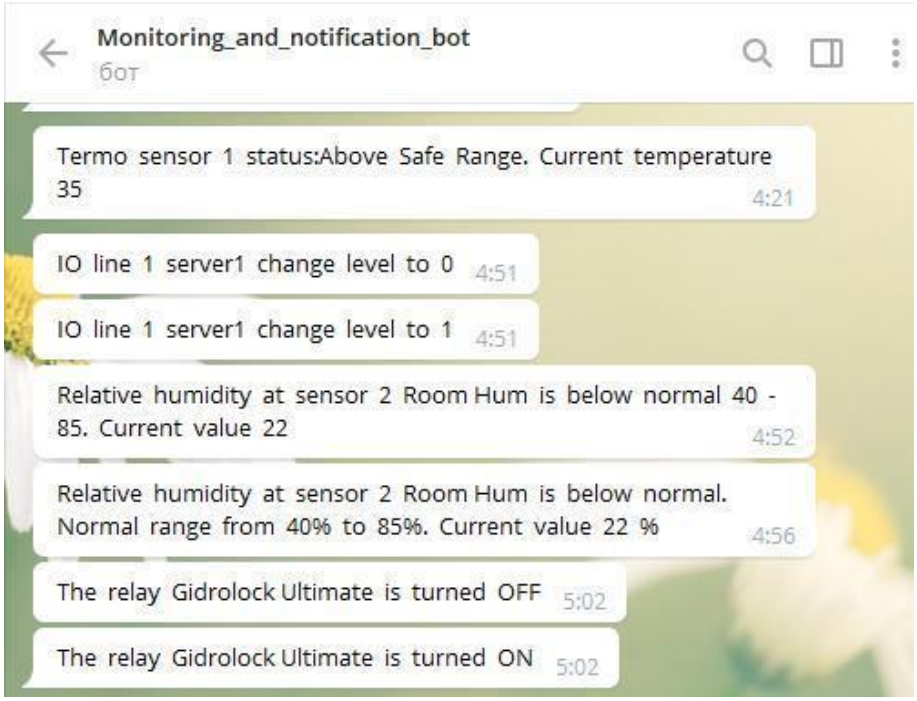


Рисунок 3.35 – Повідомлення, які надходять після всіх налаштувань

3.4 Висновки до розділу

У даному розділі було розроблено програму боту моніторингу фізичних умов серверного приміщення і боту автоматичного сповіщення про критичні перевищення заданих значень датчиків. Наведено повний опис всіх етапів розробки з додаванням ілюстрацій до кожного кроку розробки. Встановлено зв’язку сервісу

Telegram із Web інтерфейсом контролеру моніторингу. Продемонстровано роботу програми.

ВИСНОВКИ

У роботі було розроблено систему моніторингу центру обробки даних. Технічні компоненти ЦОД надзвичайно важливі у IT-інфраструктурі компанії, тому не можна допускати того, щоб вони вийшли з ладу.

Було розглянуто принцип роботи і завдання ЦОД, основні етапи створення, вимоги та рекомендації для організації серверної кімнати.

Наведено основні переваги центру обробки даних. Розглянуто і проаналізовано рівні надійності центрів обробки даних.

Також було розроблено програму боту моніторингу фізичних умов серверного приміщення і боту автоматичного сповіщення про критичні перевищення заданих значень датчиків. Наведено повний опис всіх етапів розробки додаванням ілюстрацій до кожного кроку розробки. Встановлено зв’язку сервісу Telegram із Web інтерфейсом контролеру моніторингу. Продемонстровано роботу програми.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЬ

1. https://jayxt.github.io/MessengerComparison/.
2. http://citforum.ru/gazeta/27/.
3. https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5 %D1%80%D0%BD%D0%B0%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BD%D0%B0%D1%82%D0%B0.
4. Центри обробки даних (Дата-центри) [Електронний ресурс]. Режим доступу: https://www.olly.ru/blog/centry-obrabotki-dannyh-data-centry/.
5. https://uk.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80 _%D0%B4%D0%B0%D0%BD%D0%B8%D1%85.
6. https://zapier.com/blog/what-are-webhooks/.
7. Оліфер В. Г. Комп'ютерні мережі. Принципи, технології, протоколи: / В. Г. Оліфер, Н. А.Оліфер. // Підручник для вузів. - 4-е изд. - СПб .: Пітер, 2010. - 944с .: ил.
8. Закер Крейг. Планування і підтримка мережевої інфраструктури Microsoft Windows Server 2003. Навчальний курс MCSE / Закер Крейг. // Пер. з англ М .: Видавничо-торговий дім «Російська Редакція», 2005. - 544с. : Ил.
9. Нортроп Т. Проектування мережевої інфраструктури Windows Server 2008. Навчальний курс Microsoft / Т. Нортроп, Дж. К. Макін; Пер. з англ. - М.: Видавництво «Російська Редакція», 2009. - 592с. : Ил.
10. Палмер М. Проектування і впровадження комп'ютерних мереж / М. Палмер, Р. Сінклер. - СПб.: БХВ-Петербург, 2004. - 752с .; мул.
11. Колісниченко Д.М. Бездротова мережа будинку і в офісі / Д.М. Колісниченко. - СПб .: БХВ-Петербург, 2009. - 480с .; мул.
12. Демидов М. Невидима павутина. Огляд технологій бездротового підключення до Інтернету / М. Демидов // HARD'n'SOFT. - 2010. - №8. - С.54-57
13. Ethernet - Вікіпедія [електронний ресурс]: режим доступу http://ru.wikipedia.org/wiki/Ethernet

14. Знайомтесь: Radio Ethernet і інші бездротові технології [електронний ресурс]: режим доступу http://www.iemag.ru/platforms/detail.php?ID=16509

15. Програма резервного копіювання, синхронізації папок і відновлення данихHandyBackup[електроннийресурс]:режимдоступу http://www.handybackup.ru/

16. Internet Security Software - Bitdefender Internet Security 2014 [Електронний ресурс]: режим доступу http://www.bitdefender.com/solutions/internet-security.html

17. Forefront Threat Management Gateway [електронний ресурс]: режим доступуhttp://technet.microsoft.com/en-us/forefront/ee807302

Принцип роботи системи

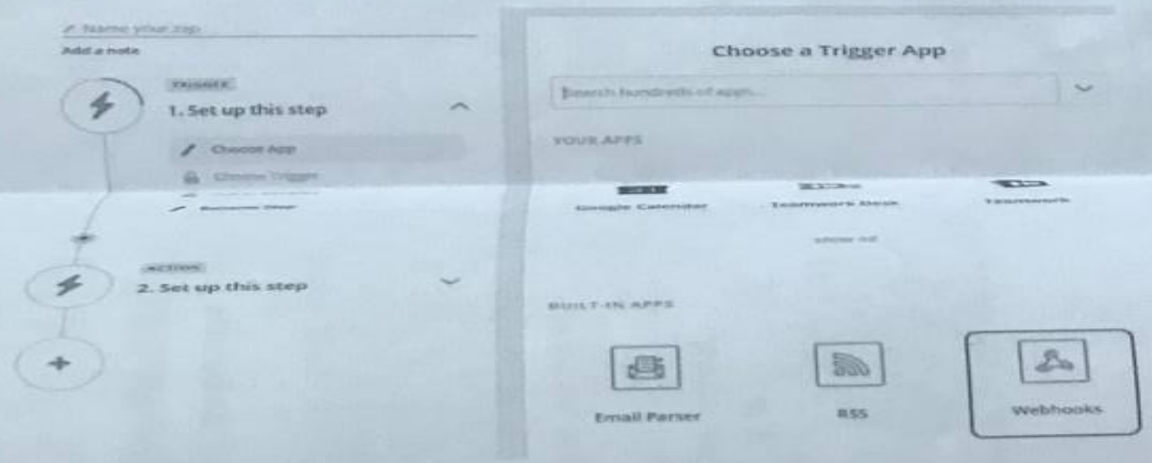
					13.02070849.00047 ПЛ1
Зам.	Лист.	№ докум.	Підп.	Дата	Розробка системи моніторингу комп'ютерної мережі
Розроб.		Білоусов В.В.			
Перев.		Ільяшенко М.Б.			
Т.контр.					Принцип роботи системи
Н.контр.		Зелік О.В.			
Затв.		Кудерметов Р.К.			

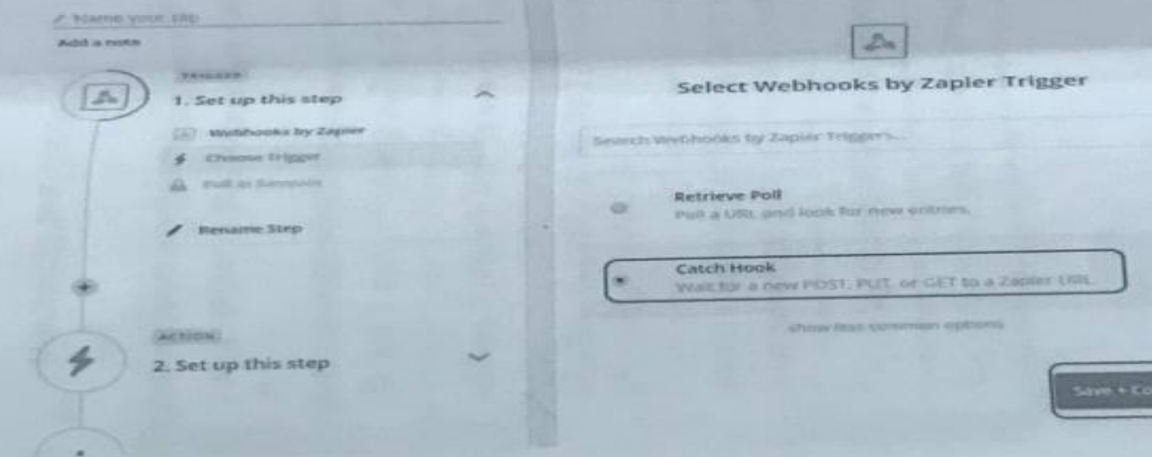
Лит. | Лист 1 | НУ «Запорізька КНТ-5

Особливість	Telegram	Viber	WhatsApp
Швидкість відправки повідомлень	≈ 150 мілісекунд	≈ 900 мілісекунд	≈ 550 мілісекунд
Обсяг трафіку для відправки повідомлення	Мінімальний	Середній	Середній
Відмовостійкість та надійність	Висока	Середня	Середня
Вид синхронізації	Хмарна і миттєва	1 первинний пристрій (смартфон / планшет) і кілька вторинних (планшети / комп'ютери), які синхронізуються з первинним пристроєм	1 смартфон і 1 пов'язаний з ним комп'ютер
Завантаження вмісту	Динамічне в режимі реального часу, на вимогу	Одноразова доставка з сервера	Одноразова доставка з сервера

Зам.	Лист	№ докум.	Підп.	Дата	13.02070849.00047 ПЛ2		
Розроб.		Білоусов В.В			Розробка системи моніторингу комп'ютерної мережі	Лит.	Маса
Перев.		Ільяшенко М.Б.				Лист 2	Лист
Т.контр.					Основні характеристики месенджерів	НУ «Запорізька політ КНТ-518сп	
Н.контр.		Зелік О.В.					
Затв.		Кудерметов Р.К.					

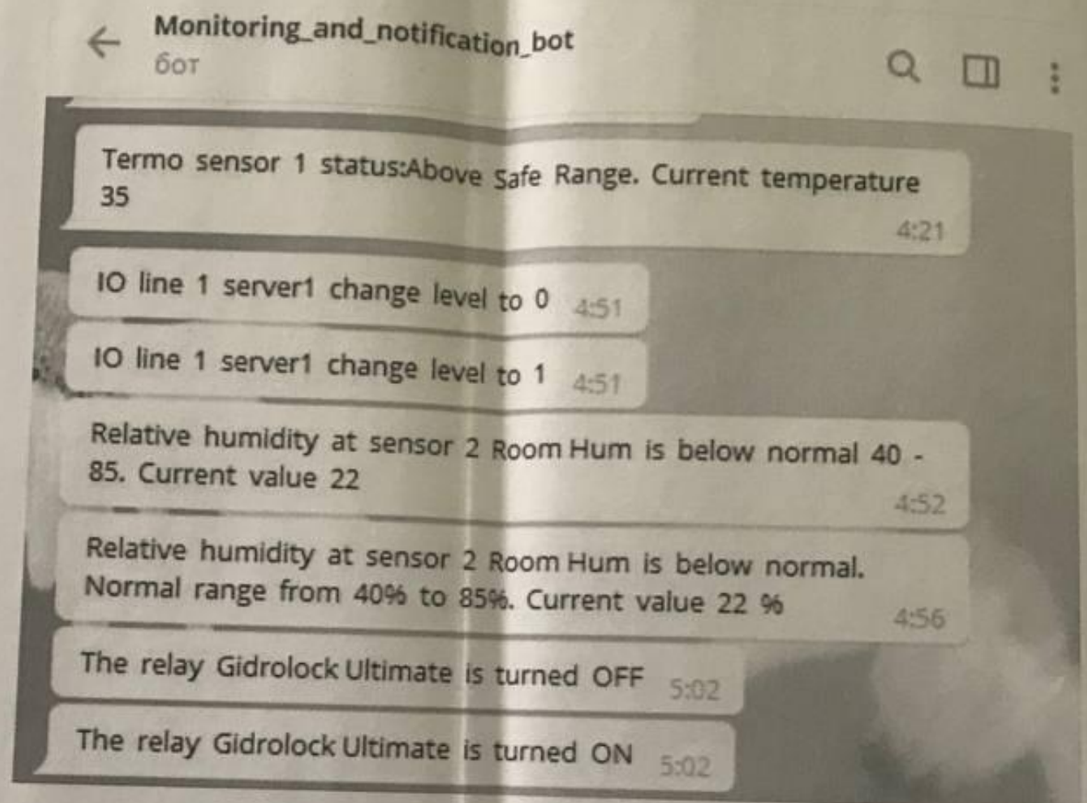
Налаштування Zapier





Зам.	Лист.	№ докум.	Підп.	Дата	13.02070849.00047 ПЛЗ			
Розроб.		Білоусов В.В			Розробка системи моніторингу комп'ютерної мережі	Літ.	Маса	Масшт.
Перев.		Ільяшенко М.Б.						
Т.контр.						Лист 2	Листів 4	
Н.контр.		Зелік О.Я.			Налаштування Zapier	НУ «Запорізька політехніка» КНТ-518сп		
Затв.								

Результати роботи



					13.02070849.00047 ПЛ4	
Зам.	Лист	№ докум.	Підп.	Дата		
Розроб.		Білоусов В.В			Розробка системи моніторингу комп'ютерної мережі	Літ. / Маса / Масшт.
Перев.		Ілляшенко М.Б.				Лист 4 / Листів 4
Т.контр.						
Н.контр.		Зелік О.В.			Результати роботи	НУ «Запорізька політехніка» КНТ-518сп
Затв.		Кулеметов Р.К.				