НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАБЕЗПЕЧЕННЯ ПІДТРИМКИ ІНФРАСТРУКТУРИ СИСТЕМ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ДАНИХ В УМОВАХ ЗБОЇВ ЕНЕРГОПОСТАЧАННЯ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека»
Пшеничний Євгеній Анатолійович

Керівник: к.т.н., доцент
Бойко Віктор Дмитрович

Рецензент: к.т.н., доцент
Чепурна Олена Євгенівна

Одеса –2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет **кібербезпеки та інформаційних технологій**

Кафедра **кібербезпеки**

Галузь знань: **12 Інформаційні технології**

Спеціальність: **125 Кібербезпека**

Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Пшеничному Євгенію Анатолійовичу

1. Тема роботи: «Забезпечення підтримки інфраструктури систем кібербезпеки та захисту даних в умовах збоїв енергопостачання»

Керівник роботи: к.т.н, доцент Ганна Валеріївна Ахмаметьєва

затверджені наказом НУ ОЮА від «__» _____ 20___ року № _____

2. Строк подання здобувачем роботи «__» _____ 20___ рік

3. Дата видачі завдання«__» _____ 20___ рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

У сучасному світі, де інформація стає все більш цінним активом, питання кібербезпеки та захисту даних набуває особливої актуальності. Особливо гостро ці питання стоять в умовах перебоїв з електропостачанням, які можуть виникати внаслідок бойових дій, природних явищ або інших надзвичайних ситуацій.

Перебої в електропостачанні можуть мати значний вплив на інфраструктуру систем кібербезпеки та захисту даних: відключення електроенергії може призвести до зупинки серверів, мережевого обладнання та систем зберігання даних. Це може призвести до втрати даних, порушення роботи інформаційних систем та інших критичних послуг. Зловмисники можуть використовувати перебої з електропостачанням для здійснення кібератак. Наприклад, вони можуть розпочати DDoS-атаки або спробувати проникнути в системи, коли ті знесилені. Відсутність електроенергії може ускладнити або зробити неможливим реагування на кібератаки. Це може призвести до того, що зловмисникам вдасться завдати більшої шкоди.

Важливо також зазначити, що кібербезпека та захист даних - це не просто технічні питання. Це також питання культури та управління ризиками. Тому для того, щоб ефективно вирішувати ці проблеми, необхідний комплексний підхід, який буде включати в себе як технічні, так і організаційні заходи.

Цілю є створення системи моніторингу та управління енергетичною інфраструктурою інформаційно комунікаційних систем в умовах можливих збоїв в енергопостачанні, яка буде надавати користувачам інформацію про стан батареї, таку як заряд та час до розрядження, щоб своєчасно приймати рішення щодо своєчасного відключення ІКС, та додаткову можливість віддалено поновити роботу.

Для досягнення поставленої цілі потрібно буде виконати наступні задачі :

Огляд літературних джерел з проблем блекаутів, та їх впливу на проблеми кібербезпеки.

Вибір інструментальних засобів для побудови системи моніторингу та управління енергетичною інфраструктурою інформаційно комунікаційних систем в умовах можливих збоїв в енергопостачанні.

Планування роботи, структури, розгортання на налаштування системи моніторингу та управління енергетичною інфраструктурою інформаційно комунікаційних систем

Побудова та тестування системи моніторингу та управління енергетичною інфраструктурою інформаційно комунікаційних систем

Об'єктом цього дослідження є інфраструктурні аспекти систем кібербезпеки.

Предметом є моніторинг та управління інфраструктурою системи енергозабезпечення кібербезпеки в умовах збоїв енергопостачання.

1 РОЛЬ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

1.1 Блекаути як кіберзагроза

У сучасному світі майже всі види діяльності - економічна, наукова, корпоративне управління та особисте життя - нерозривно пов'язані з використанням технологій. Технології уможливлюють комунікацію, обмін інформацією, вирішення проблем, швидкість та ефективність повсякденної роботи. Технології стали не лише інструментом для досягнення цілей, але й невід'ємною частиною нашого повсякденного життя, впливаючи на те, як ми працюємо, відпочиваємо та взаємодіємо з іншими людьми.

Технологічний прогрес став важливим фактором розвитку суспільства та створення нових можливостей для інноваційних розробок у різних сферах життя. Однак разом із залежність від цифрових технологій створює ризики.

Одним із головних ризиків останнім часом для інфраструктури ІКС є перебої в постачанні електроенергії. Масштабні перебої називають "блекаутами", що означає масове відключення електроенергії.

Блекаут може бути плановим (віялові відключення за графіком) або раптовим (відключення внаслідок стихійних лих або технічних збоїв). Найбільшу загрозу становлять позапланові вимкнення, оскільки в цьому випадку системи часто не встигають штатно відреагувати і коректно завершити роботу.

Блекаути можуть бути спричинені різними причинами, як-от стихійні лиха, технічні збої, людські помилки, кібератаки та бойові дії..

Джерелом, що викликало блекаут, може бути стихійне лихо. Найбільш широко обговорюваним у літературі відключенням електроенергії є блекаут, що стався в серпні 2003-го року в енергосистемах США і Канади, який торкнувся 50 мільйонів осіб і призвів до втрат у розмірі 6 мільярдів доларів[1]. У [2] описується два послідовних великих відключення електроенергії в енергосистемі Індії 30 і 31 липня 2012 року, що сталося через неправильну

роботу реле, спричинену неправильними налаштуваннями (прихованою відмовою) на тлі серйозних перебоїв у подачі енергії. Ці блекаути торкнулися 620 мільйонів осіб і на 2022-й рік є найбільшими з коли-небудь зареєстрованих із погляду кількості постраждалих людей.

За даними Північноамериканської ради з надійності електропостачання (NERC) за 1984-2006 роки , частота великих відключень електроенергії у Сполучених Штатах не зменшилась із плином часу, що спостерігається статистично значуще збільшення частоти відключень у години пік, а також наприкінці літа та в середині зими (хоча це й не пов'язано з ураганами)[3]. Ризик майже постійний протягом року і існує сильна статистична підтримка раніше спостережуваної степеневої статистичної залежності між розміром і частотою відключень.

Ці тенденції зберігаються навіть після врахування зростання попиту і чисельності населення, а також після виключення невеликих подій, дані щодо яких можуть бути спотворені через нерівномірне звітування. Однією з важливих складових є необхідність моніторингу стану системи енергопостачання, або джерел безперебійного живлення (далі ДБЖ), які підключені до системи.

У світлі ситуації, що склалася, що можна зробити, щоб запобігти подібним катастрофам у майбутньому, модернізувати і поліпшити енергетичну інфраструктуру, зробивши її більш стійкою до відключень і несприятливих погодних умов.

Перебої з електрикою можуть мати каскадні наслідки, спричиняючи проблеми з водопостачанням, транспортом і комунікаціями. Люди, які користуються медичним обладнанням, що працює від електрики, піддаються величезному ризику під час відключення електроенергії. Економічні наслідки відключення електрики можуть бути значними, оскільки вони можуть призвести до закриття підприємств і втрати робочих місць.

Відключення електроенергії створює ідеальні умови для

кіберзловмисників для використання вразливостей. Це відбувається тому, що системи безпеки та інструменти моніторингу, які потребують безперервного живлення, стають тимчасово неефективними. Головну проблему для кібербезпеки робить не відсутність електропостачання, а те що системи мають послаблення тому не можуть працювати на повну потужність внаслідок чого швидкість виявлення вторгнень буде знижена. Ризик виходить за рамки безпосереднього збою. Під час відключення електроенергії затримка з виявленням вторгнень дає зловмисникам більше часу для доступу до конфіденційної інформації, встановлення шкідливого програмного забезпечення або програм-вимагачів, а також для підготовки майбутніх атак.

Перебої в електропостачанні можуть мати значний вплив на інфраструктуру систем кібербезпеки та захисту даних: відключення електроенергії може призвести до зупинки серверів, мережевого обладнання та систем зберігання даних. Це може призвести до втрати даних, порушення роботи інформаційних систем та інших критичних послуг. Зловмисники можуть використовувати перебої з електропостачанням для здійснення кібератак. Наприклад, вони можуть розпочати DDoS-атаки або спробувати проникнути в системи коли відсутнє живлення. Відсутність електроенергії може ускладнити або зробити неможливим реагування на кібератаки. Це може призвести до того, що зловмисникам вдасться завдати більшої шкоди.

Таким чином, відключення електроенергії не лише порушує нормальний спосіб життя, але також створює серйозні загрози для кібербезпеки, і для запобігання таким ситуаціям потрібна комплексна стратегія. Ця вразливість особливо актуальна для секторів критичної інфраструктури, де порушення безпеки даних може мати величезні наслідки для критично важливих послуг, систем зв'язку та національної безпеки[4].

1.2 Проблеми кібербезпеки які створює блекаут

Досвід безперебійної роботи інформаційно-комунікаційних мереж часто

призводить до того, що багато різних служб - у тому числі служби, що забезпечують інфраструктуру кібербезпеки так чи інакше використовують їх, як частину своєї інфраструктури, при цьому не приділяючи належної уваги стійкості до збоїв в енергопостачанні.

Керівник Utility Bidder підкреслив, що відключення електроенергії порушують не тільки постачання електроенергії, але й можуть стати причиною кібератак та серйозною загрозою для кібербезпеки. [5].

При цьому часто ігнорується відразу кілька факторів, що створюють ризики, а саме:

- загальна зношеність інфраструктури, що визначає наростання кількості збоїв у системах енергопостачання;
- подорожчання енергоносіїв, що опосередковано уповільнює чи відкладає модернізацію технічних систем;
- низьку практичну підготовленість технічного персоналу та невміння планувати та прогнозувати дії для екстрених ситуацій - наприклад, далеко не кожен технічний фахівець має уявлення про те, що різні моделі дизельних генераторів мають різні граничні терміни функціонування, після яких їм потрібна перерва та технічне обслуговування;

Досвід блекаутів зими 2023 року говорить про те, що системи кібербезпеки та системи інформаційно-комунікаційних мереж загалом вимагають додаткових заходів та технічних засобів, що дозволяють мінімізувати збитки від відключень електроенергії. Практика показала, що найбільшою проблемою є неможливість управління та контролю енергетичної складової інфраструктури дистанційно, що часто ускладнювалася запровадженням комендантської години, що додатково ізолювало технічний персонал.

Частою була ситуація, коли системному адміністратору доводилося гадати про причини збою в системі – це блекаут чи просто помилка у програмному забезпеченні? Особливо складною була ситуація у разі, якщо доводилося

підтримувати парк розподілених у просторі серверів.

Проблему енергетичної інфраструктури можна розв'язувати кількома шляхами - зокрема впровадженням джерел безперебійного живлення, резервуванням і розподілом комп'ютерних систем (у разі часткового блекауту система може переключити навантаження на незачеплені блекаутом сегменти).

Додатковими засобами запобігання непередбачуваним відключенням електроенергії з метою визначення того, наскільки поширеною є проблема перебоїв, викликаних негативними природними явищами або наслідками навмисного руйнування енергетичної інфраструктури. У багатьох країнах, особливо в Європі та США, є компанії, які надають послуги, щоб запобігти таким ситуаціям. Вони надають послуги від генераторів до виділених ліній електропередачі. Але через високу вартість ці послуги часто недоступні для малих підприємств.

Наприклад, компанія "HomeGuide" у Сполучених Штатах пропонує різноманітні послуги для дому, такі як проведення нових ліній електропостачання за такими цінами[6]:

- Проведення підземних ліній коштує від $10 до $25 за фут.
- Проведення повітряних ліній коштує від 5 до 15 доларів за фут.
- Проведення повітряних ліній становить від $42,000 до $79,000 за милю.

При цьому, всі перераховані заходи вимагають впровадження додаткових систем управління та моніторингу.

1.3 Необхідність моніторингу та управління енергетичною інфраструктурою

Все вищеперелічене передбачає необхідність підвищеної уваги до систем управління інфраструктурою інформаційно-комунікаційних мереж, як до важливої складової кібернетичної безпеки.

Однією з проблем є також різний ступінь зношеності комп'ютерного парку та енергетичної інфраструктури. У різних компаніях організаціях може бути

різне обладнання, яке невідомо наскільки активно використовувалося, яких навантажень воно зазнавало. Це може призводити до нерівномірного розподілу навантаження на енергетичну мережу і незбалансованості споживання ресурсів. Унаслідок цього спрогнозувати приблизний час автономної роботи майже не можливо оскільки на це впливає не один параметр який залежить для чого використовується ІКС, якщо це сервер до час роботи буде один а якщо це звичайний офісний персональний комп'ютер (далі ПК) то час роботи буде інший, додатково потрібно додати те що дистанційно перевірити стан енергосистеми може виклики проблеми якщо збій в енергосистеми стався неочікувано. Найбільшою проблемою під час блекаутів є відключення SIEM[7]. SIEM– це рішення, що допомагає організаціям виявляти, аналізувати й усувати загрози безпеці. Іншими словами це окремий ПК котрий відповідає за аналіз мережі та допомагає швидке відреагувати на кібератаки, оскільки він окремо існує виключно для підвищення рівня безпеки в ІКС. Внаслідок чого при блекауті та відключені SIEM або апаратної частини може бути використано для кібератаки.

З урахуванням зазначеного вище, впровадження додаткового резервування енергосистеми та підтримання працездатності систем кібербезпеки потребує не лише суто технологічних заходів (гаряче та холодне резервування, дублювання проблемних систем, використання дизель-генераторів та джерел безперебійного живлення), а й систем моніторингу та управління енергетичною інфраструктурою.

У компаніях великого масштабу ці питання, як правило, вирішуються впровадженням відповідного відділу технічної підтримки, або вже вирішені на рівні наявних відділів. У компаніях середнього та малого масштабу цьому питанню донедавна не приділяли достатньо уваги. Тому проста мінімальна система моніторингу та управління енергетичною інфраструктурою може істотно підвищити стійкість такої компанії і, як наслідок, збільшити її кібербезпеку.

Складовими мінімальної системи можуть бути:

- система моніторингу стану електромережі;
- система моніторингу джерел безперебійного живлення,
- система моніторингу стану живлення серверів та робочих станцій (за даними їх сенсорних систем);
- система дистанційного увімкнення відключеного обладнання при подачі електроенергії (зокрема зручною є технологія Wake-On-LAN);

Як показує практика, такі заходи, реалізовані з урахуванням можливості доступу до самих серверних систем (у найпростішому випадку - за протоколом ssh), дозволять вчасно вжити заходів штатного реагування на відключення світла:

- контролювати стан машинного парку;
- контролювати ступінь зношеності систем резервного живлення;
- задіяти альтернативні варіанти роботи при відключенні живлення;
- штатно відключати "безнадійні" чи некритичні системи, що дозволить уникнути втрати даних;
- при відновленні живлення запускати всі відключені системи, контролюючи при цьому стан системи резервування.

Таким чином було проаналізовано роль енергетичної інфраструктури в забезпеченні кібербезпеки. На основі огляду літератури було сформульовано основну проблему, яку необхідно вирішити в цій роботі.

Роботу буде присвячено побудові ефективної системи управління та моніторингу інфраструктури кібербезпеки та захисту даних в умовах вимкнення електроенергії, маючи на увазі простоту використання та ефективність для звичайних користувачів і малих підприємств та бізнесів. Для цього слід розробити систему моніторингу та управління інформаційно-комунікаційними мережами в умовах планових або раптових блекаутів.

2 РОЗРОБЛЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕЛЕКТРОННО ІНФОРМАЦІЙНИМИ СИСТЕМАМИ

2.1 Вибір інструментальних засобів

Основною метою цього розділу роботи є вибір інструментальних засобів для розробки та тестування програми для забезпечення надійної підтримки інфраструктури кібербезпеки та захисту даних під час відключень електроенергії у вигляді програми котра дозволить будь який людині переглянути стан ДБЖ на веб-платформі та додатково для системного адміністратора увімкнути сервер/ПК дистанційно.

В якості мови програмування розглядалися 3 мови програмування: Python, C++, Java . Основні критерії для вибору мови для написання програми були такі :

- швидкість самої програми,
- можливість модифікації,
- простота у розумні структури коду,
- невелике навантаження на систему,
- підтримку на різних операційних системах
- хороша взаємодія із залізом персонального комп'ютера.

Якщо ознайомлюватись із специфікаціями кожної мови програмування то можна прийти до таких висновків що C++ - це потужна, компільована мова програмування з високою продуктивністю та широким спектром можливостей. Вона зазвичай використовується для розробки швидких програм, включаючи операційні системи, вбудовані системи, ігри та додатки з високими вимогами до продуктивності. C++ має строгу типізацію та можливості ручного керування пам'яттю, що робить його більш вимогливим для вивчення, але водночас надає більшу контроль над програмою. Мова є низькорівневою в наслідок чого має дуже велику швидкість виконання запитів програми, але в одно час, сам код стає дуже складно модифікувати внаслідок чого при переписувані коду або додавання іншого функціоналу потрібно зважувати додаткові параметри. Також більш

складна взаємодія із різними мовами програмування. А серед плюсів можна виділити не тільки велику швидкість та повний контроль над програмою але й повний доступ до системи та заліза, що робить дані отримані для програми більш точними [8].

Java - це об'єктно-орієнтована, мультиплатформенна мова програмування, розроблена для створення надійних та масштабованих програм. Вона відома своєю портативністю, оскільки програми, написані на Java, можуть виконуватися на різних операційних системах без модифікацій. Java широко використовується для веб-розробки, мобільних додатків (зокрема на платформі Android), корпоративного програмування та багатьох інших областей. Порівнюючи із Python та C++ Java може виглядати більш привабливим інструментом, але серед цього є один великий недолік: для роботи програм на Java постійно запускається віртуальне оточення (JVM) через що навантаження без оптимізації буде дуже велике. Хоча Java все одно буде запускати код будь де та із одним результатом але якщо те як сама програма буде працювати та чи буде вона на різному залізі однаково далеко не факт [9].

Python - це високорівнева, інтерпретована мова програмування, яка активно використовується для розробки різноманітних програм. Вона відома своєю простотою та легкістю в освоєнні, що робить її популярним вибором для початківців. Python має широкий спектр застосувань, включаючи веб-розробку, обробку даних, штучний інтелект, наукові дослідження та інше. Вона має велику кількість бібліотек у широкому спектрі, які допоможуть уникнути зайвого коду, та спростять написання програм. Також через велику кількість бібліотек програми написані на мові Python можна запустити на майже будь якій системі, а також взаємодія коду реалізована на гарному рівні із іншими мовами програмування, мовами розмітки наприклад HTML та мовою структурованих запитів SQL та різними її підвидами. Багато плюсів має Python але через природу високо рівневої мови програмування він має повільну швидкість роботи, але це

при великому обсязі коду або складання коду із декількох файлів, у деяких випадках допомагають вбудовані бібліотеки чи стороні котрі спрямовані на пришвидшення роботи коду на Python, але у них також є свої обмеження внаслідок яких швидкість коду при повній оптимізації буде меншою ніж антологічний по своєму код але на низькорівневій мові програмування. [10]

Проаналізувавши варіанти, для виконання цієї роботи було обрано мову програмування Python через свою простоту у використані, універсальність, можливість модифікацій, слабке навантаження на залізо нашого персонального комп’ютеру, брати до уваги те що програмі не потрібно швидко працювати а навпаки стабільна робота на різних пристроях та системах. Тому вибір пав на цю мову програмування.

Python має широкий набір бібліотек та інструментальних засобів, що значно спрощують розробку. Для цієї роботи було обрано використання таких бібліотек і фреймворків.

psutil Це бібліотека для отримання інформації про систему та ресурси комп'ютера. Вона надає функції для отримання інформації про процеси, систему управління енергією, мережу, пам'ять та інші ресурси. У вашому коді вона використовується для отримання інформації про батарею, таку як рівень заряду, час до розрядження тощо. [11]

time Це вбудована бібліотека Python, яка надає функції для роботи з часом. У вашому коді вона використовується для створення затримки між перевірками статусу батареї. [12]

socket Це вбудована бібліотека Python для мережевого програмування. Вона надає можливість створення мережевих з'єднань і виконання різноманітних мережевих операцій. [13]

threading Це вбудована бібліотека Python для роботи з потоками. Вона дозволяє створювати та керувати потоками виконання програми. У вашому коді потенційно можна використати потоки для виконання операцій у фоновому

режимі. [14]

requests Це бібліотека Python для здійснення HTTP-запитів. Вона дозволяє виконувати HTTP-запити до веб-ресурсів, таких як отримання вмісту веб-сторінок, виконання запитів до веб-сервісів тощо. У вашому коді не використовується, але загалом ця бібліотека використовується для мережевої взаємодії з веб-ресурсами. [15]

sqlite3 Це вбудована бібліотека Python для роботи з базами даних SQLite. Вона надає можливість створювати, зчитувати, оновлювати та видаляти дані в базах даних SQLite з використанням мови SQL. У вашому коді вона використовується для збереження статусу батареї в базі даних. [16]

TKinter Це стандартна бібліотека для створення графічного інтерфейсу користувача (GUI) в мові програмування Python. Вона базується на бібліотеці Tk, яка є однією з найпоширеніших інтерфейсних бібліотек для створення GUI. Tkinter дозволяє легко створювати вікна, кнопки, поле введення та інші візуальні елементи, що дозволяє розробникам швидко створювати інтуїтивно зрозумілі та ефективні інтерфейси для своїх програм. [17]

flask це легковагий веб-фреймворк для мови програмування Python. Він дозволяє швидко створювати веб-додатки з мінімальними зусиллями, простотою використання та гнучкістю. [18]

Додатково для збереження та структуризації даних буде використовуватись база даних.

Як робочу СКБД було обрано SQLite.

SQLite - це легка, вбудована база даних, яка має кілька переваг над іншими системами керування базами даних (СКБД). SQLite не вимагає окремого сервера і може бути легко вбудована безпосередньо в додатки. Це робить її ідеальною для додатків, де важлива простота розгортання та ефективність також вона дуже ефективно використовує ресурси, що робить її ідеальною для пристроїв з обмеженими ресурсами. Крім того, SQLite підтримує багато поширених функцій

СУБД, таких як транзакції та індекси, і підтримується широким спектром операційних систем, що робить її універсальним і доступним рішенням для багатьох випадків використання.

Як інтерфейси керування було обрано використання CLI та GUI.

CLI - command line interface та має такі переваги - він забезпечує стабільну роботу, простий, дає змогу працювати дистанційно (наприклад через ssh).

GUI - graphics user interface дозволяє комфортну роботу та інтуїтивно зрозумілий користувачеві.

GUI у даній роботі буде створено за допомогою вбудованої бібліотеки TKinter.

Для реалізації функції моніторингу стану батареї або ДБЖ буде ви користуватись веб-фремворк FLASK [18] котрий дозволить виводити дані із бази даних у вигляді веб сторінки. Flask було обрано через базовий набір функцій для розробки веб-додатків. Він також має активну спільноту, яка розробляє розширення та допомагає вирішувати проблеми. Flask є одним із найпопулярніших виборів для створення веб-додатків в середовищі Python.

Оскільки програма повинна допомогти віддалено запустити потрібну машину буде додатково реалізована функцій Wake-On-LAN [19].

2.2 Функціонування системи

Роботу системи моніторингу та управління енергетичної інфраструктури можна поділити на 3 режими у котрому вона буде працювати.

1. *Штатний режим*: Відстежувати стан клієнтських машин (зокрема статус акумуляторних батарей і наявність або відсутність зовнішньої напруги), буде проводитись передача даних у якому стані зараз знаходиться машина. Здійснюється моніторинг за вивід інформації за допомогою flask / web, котрий закріплений за IP - адресою пристрою. На машинах інформація додатково збирається в базу даних для статистики та повного розуміння скільки витрачає енергії за певний час, машина при відсутності енергії. Що в свою чергу із

статистики можна буде зрозуміти чи потрібно замінити акумулятор або ДБЖ.

2. *Аварійний режим*: У разі вимкнення напруги і досягнення акумуляторами критичного рівня який користувач повинен визначити сам але мінімальним краще поставити 5%, щоб заряду вистелило для збереження всіх даних. Можна штатно вимкнути систему, уникнувши проблем деградації акумулятора та втрати його максимального об’єму унаслідок чого зменшиться час активної роботи.

3. *Режим відновлення*: Дає змогу ввімкнути відключені машини, використовуючи технологію Wake-On-LAN. Якщо немає інших джерел даних — для того щоб дізнатись ци заявилось електропостачання можна посилати перевірку ци з’явилась машина в мережні методом "пінгування" після спроби Wake-On-LAN "наосліп" кожні 10 чи 15 секунд. Якщо подивитись у майбутнє то дану функцію можна реалізувати постійним пінгуванням із затримкою.

У першу чергу перед написанням коду потрібно спланувати концепт програми та який функціонал потрібен бути у неї та для реалізації цих функцій знайти потрібну інформацію. Було прийняте рішення для більшої зручності оптимізувати програму поділивши її загалом на 3 частини та 2 додаткові файли.

У рамках робочого фреймворка виділяється сервер моніторингу (робоче місце) і клієнтські частини, що являють собою комп'ютери, які моніторяться. Такими комп'ютерами можуть бути, зокрема, веб-сервери, сервери безпеки тощо. Брати за основний план функціонування системи буде мати вигляд який показано на Рисунок 2.1. Сервер котрий може відправити магічний пакет для увімкнення ПК, та самі “клієнти” котрі дають дані про стан акумулятора для сервера

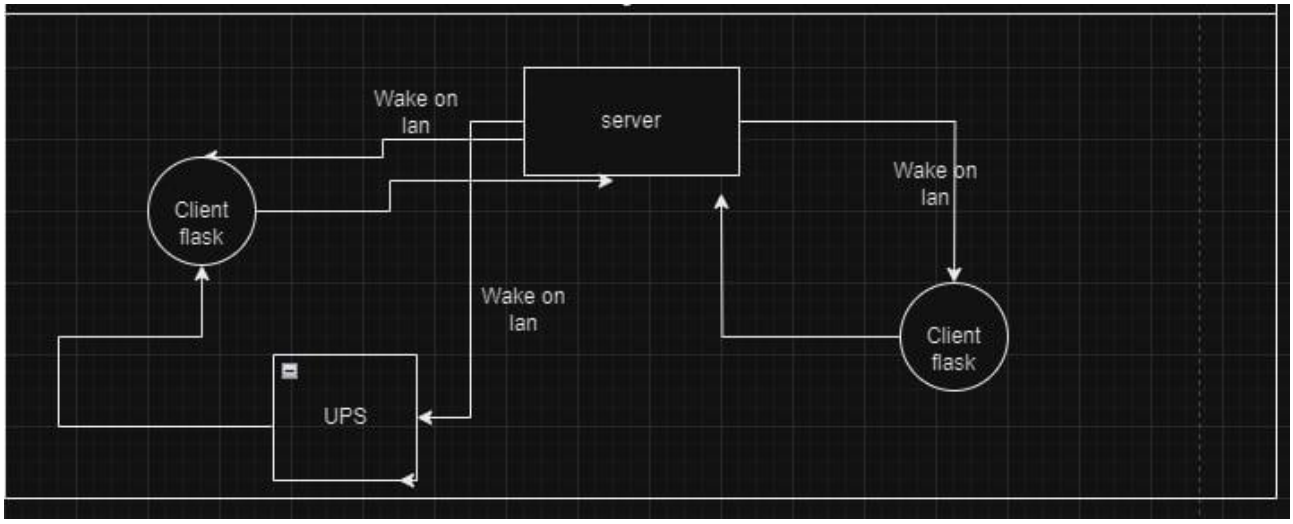


Рисунок 2.1 — Проста візуалізація роботи ПО

2.3 Розгорнення та налаштування системи

Перед тим як розгорнути систему потрібно упевнитись в тому що потрібні параметри були присвоєні та увімкнені. Для функціонування самої програми потрібно встановити Python не раніше версії 3.10 для коректної роботи та встановити потрібні бібліотеки. Для того щоб увімкнути можливість Wake-On-LAN потрібно зайти в налаштування Рисунок 2.2 після переходу до налаштувань, переходимо до пункту Мережа та Інтернет як на рисунку 2.3. На рисунку 2.4 показані додаткові налаштування мережі де потрібно обрати потрібний мережевий адаптер як показано на рисунку 2.5. У меню адаптера натиснути змінити додаткові налаштування адаптера рисунок 2.6. Рисунок 2.7 показує налаштування адаптера. Увімкнути функцію Wake on magic packet, як показано на Рисунок 2.8.

Не забудьте перевірити чи є у вашій мережевій картці така можливість оскільки дана функція працює тільки на мережеве з'єднання, тобто по витій парі, та тільки по ньому. Для людей у котрих система не Windows а створені на основі ядра Linux дані кроки не потрібні, вона там ввімкнена відразу.

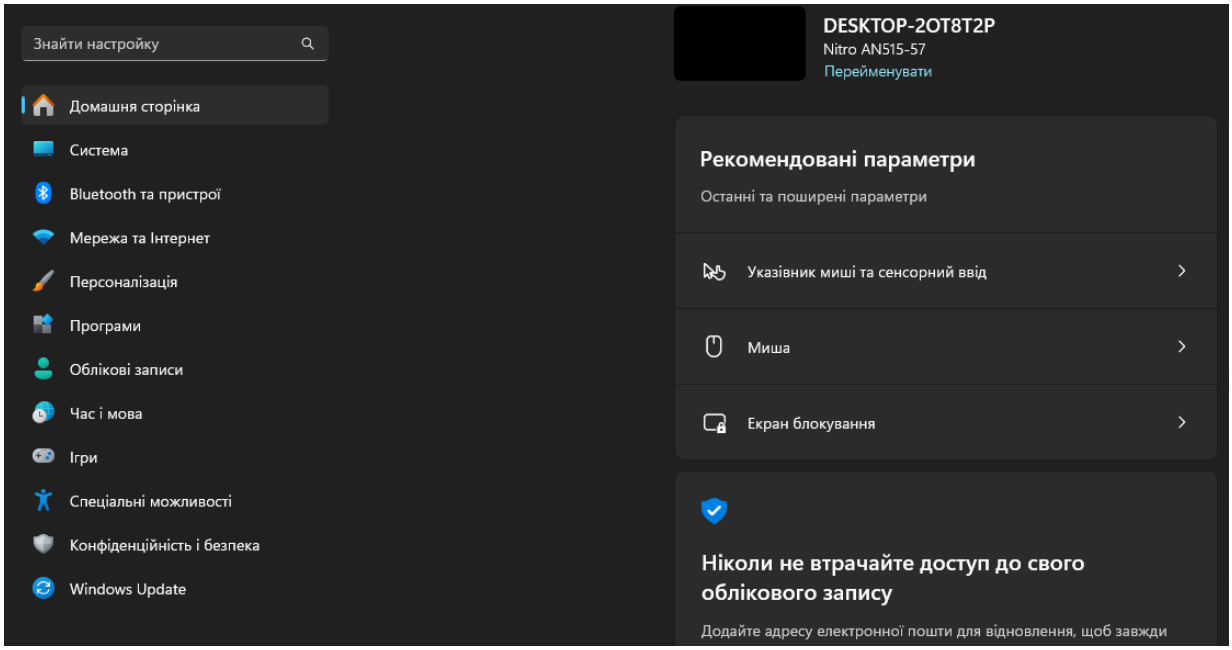


Рисунок 2.2 — Налаштування системи Windows

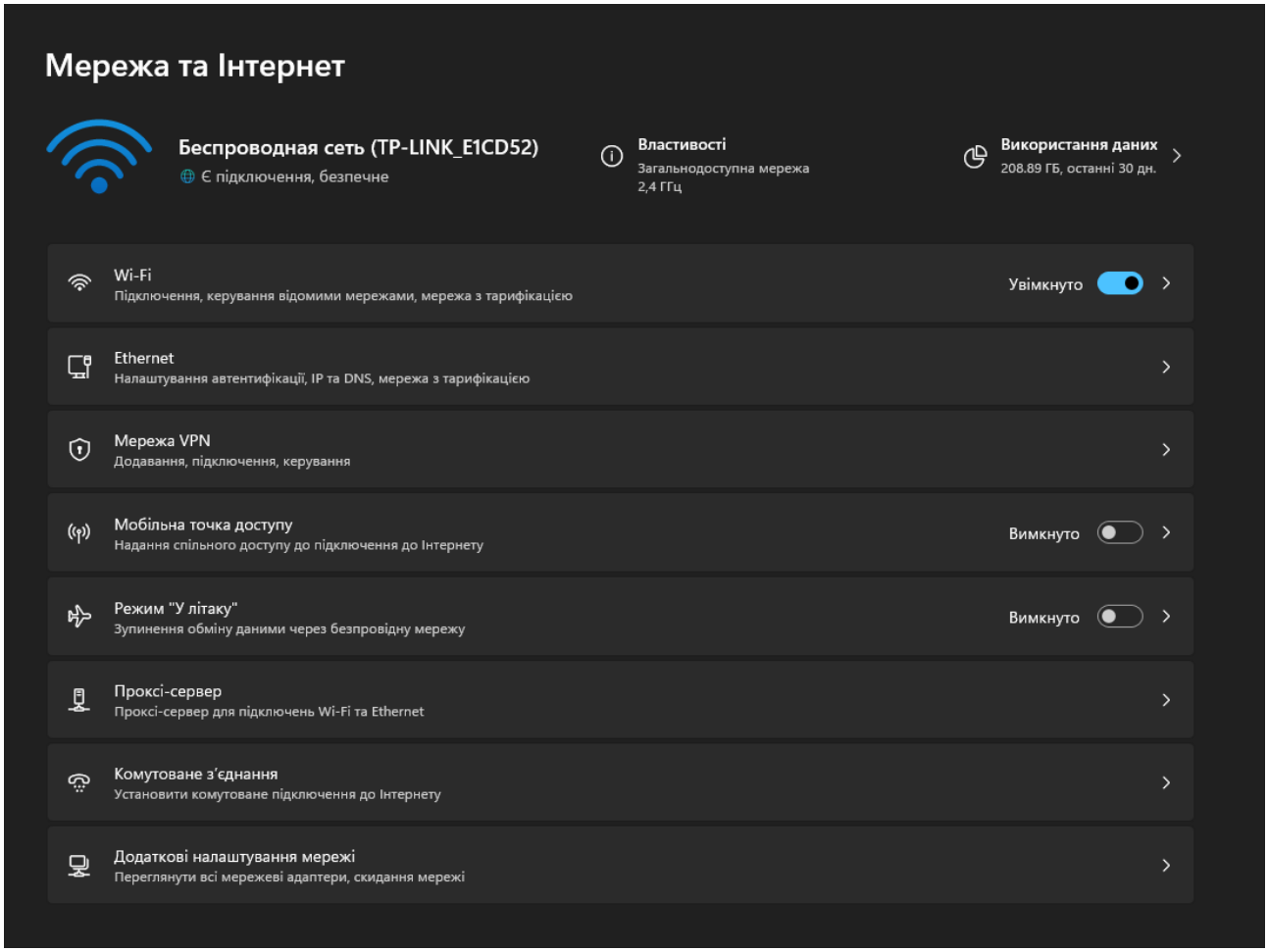


Рисунок 2.3 — Налаштування мережі

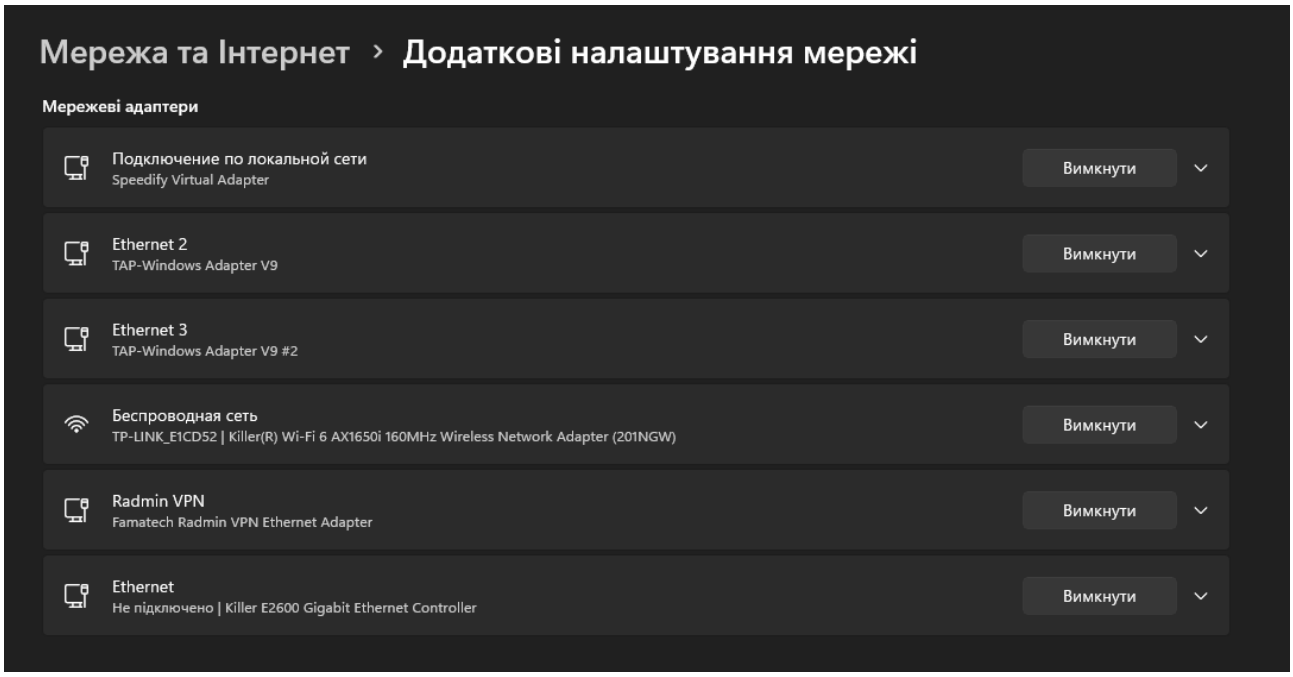


Рисунок 2.4 — Додаткові налаштування мережі

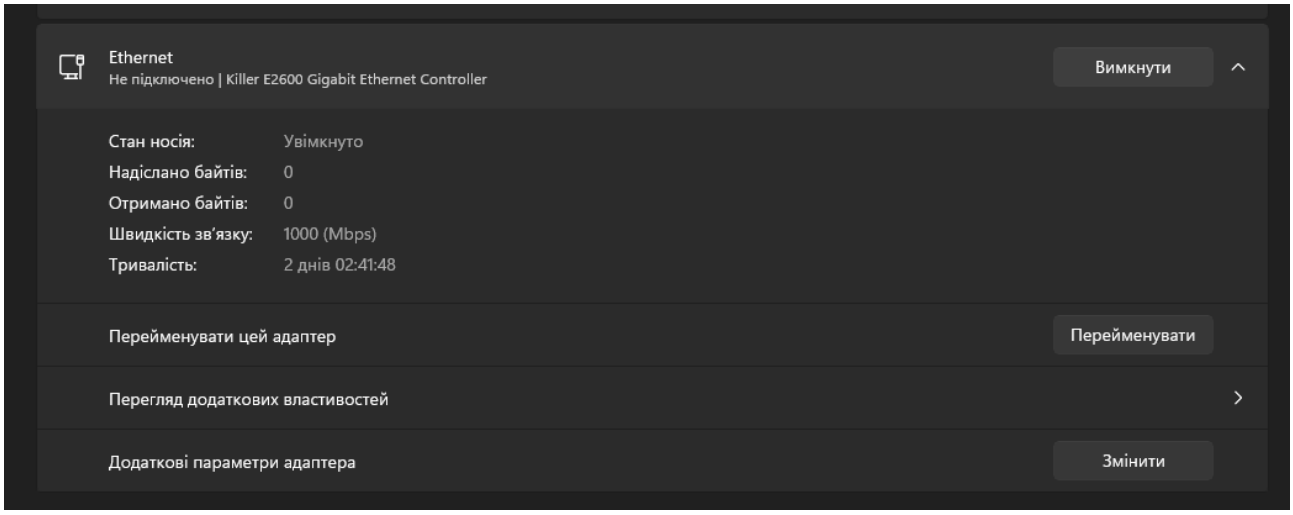


Рисунок 2.5 — Вибір мережевого адаптера

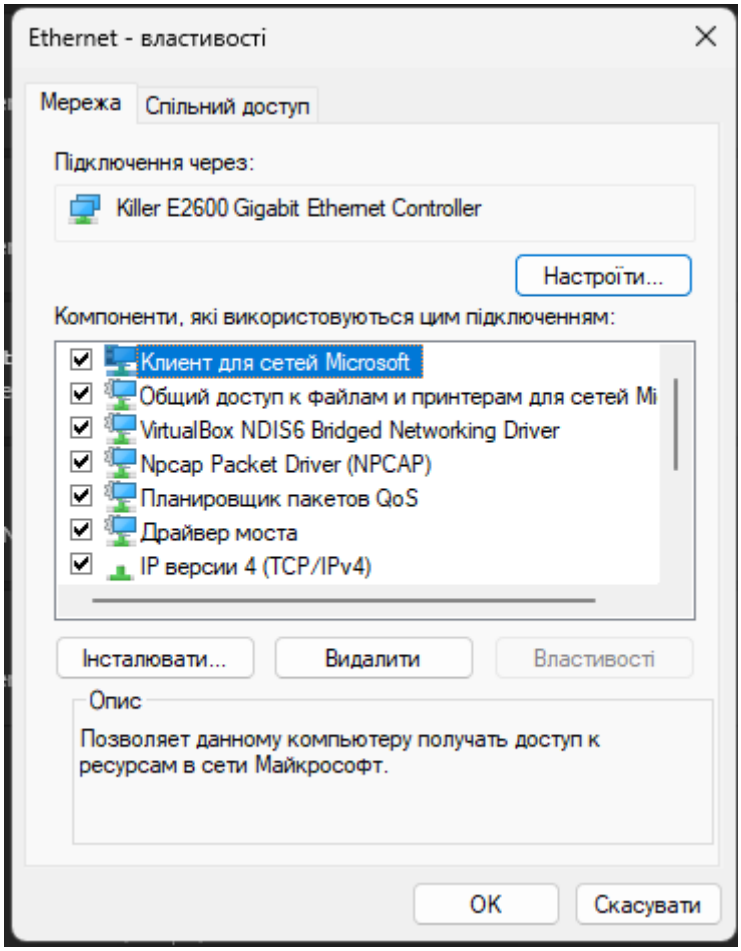


Рисунок 2.6 — Додаткові параметри адаптера

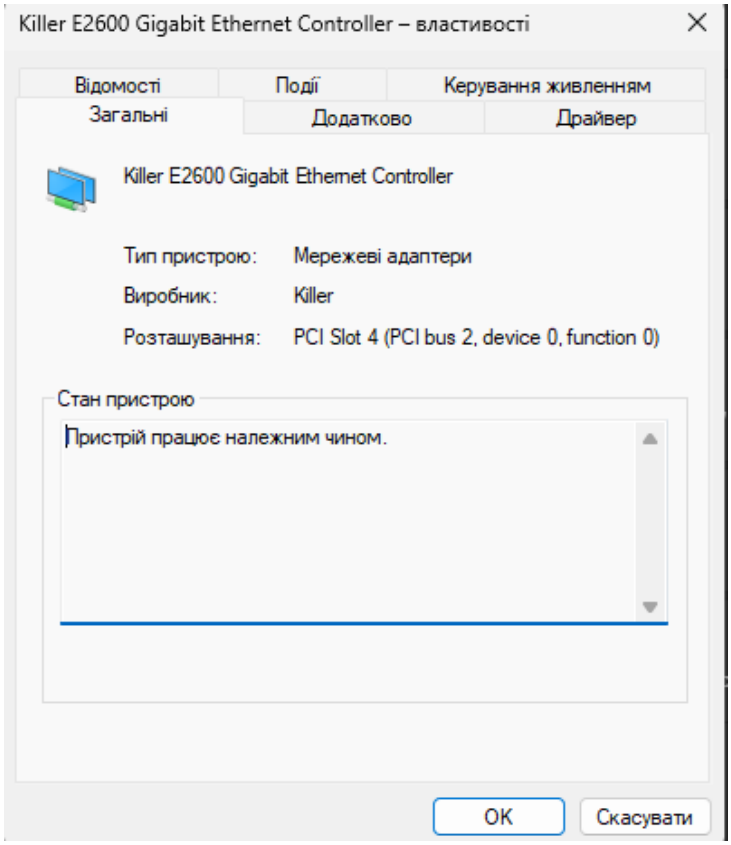


Рисунок 2.7 — Налаштування Адаптера

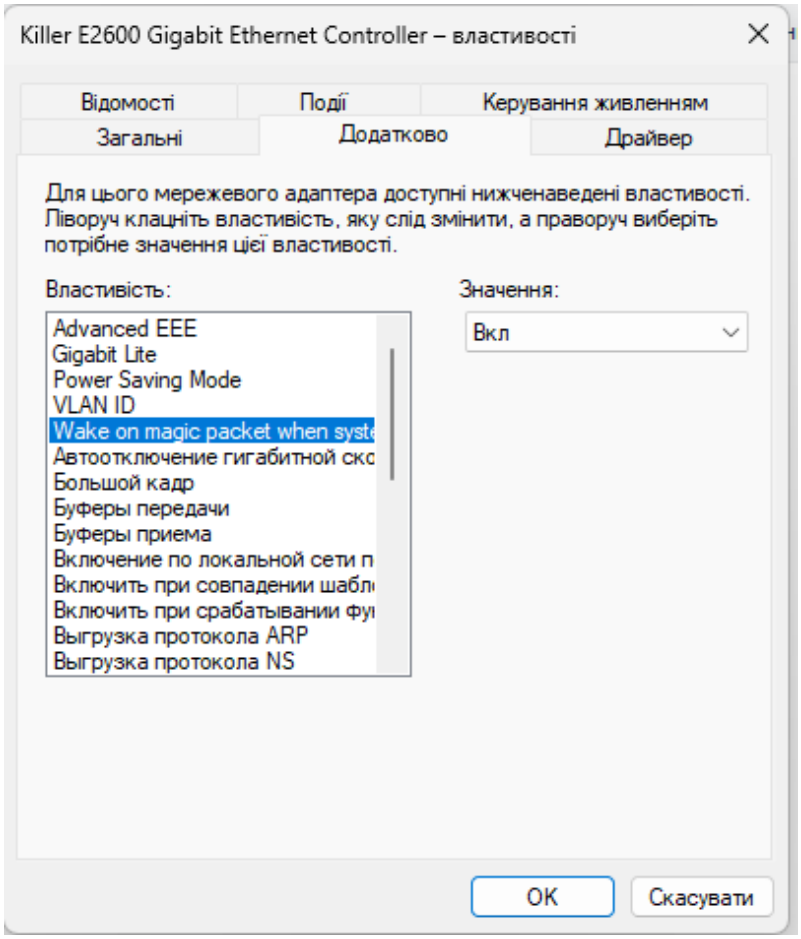


Рисунок 2.8 — Магічний пакет у налаштуваннях мережевого адаптера

Але для того щоб функція запрацювала потрібно увімкнути параметр Wake-On-LAN у налаштуваннях BIOS, цей параметр знаходиться у різних пунктах тому для прикладу буде використовуватись ноутбук Asus PU401L. Як зазначено на 2.9 та 2.10

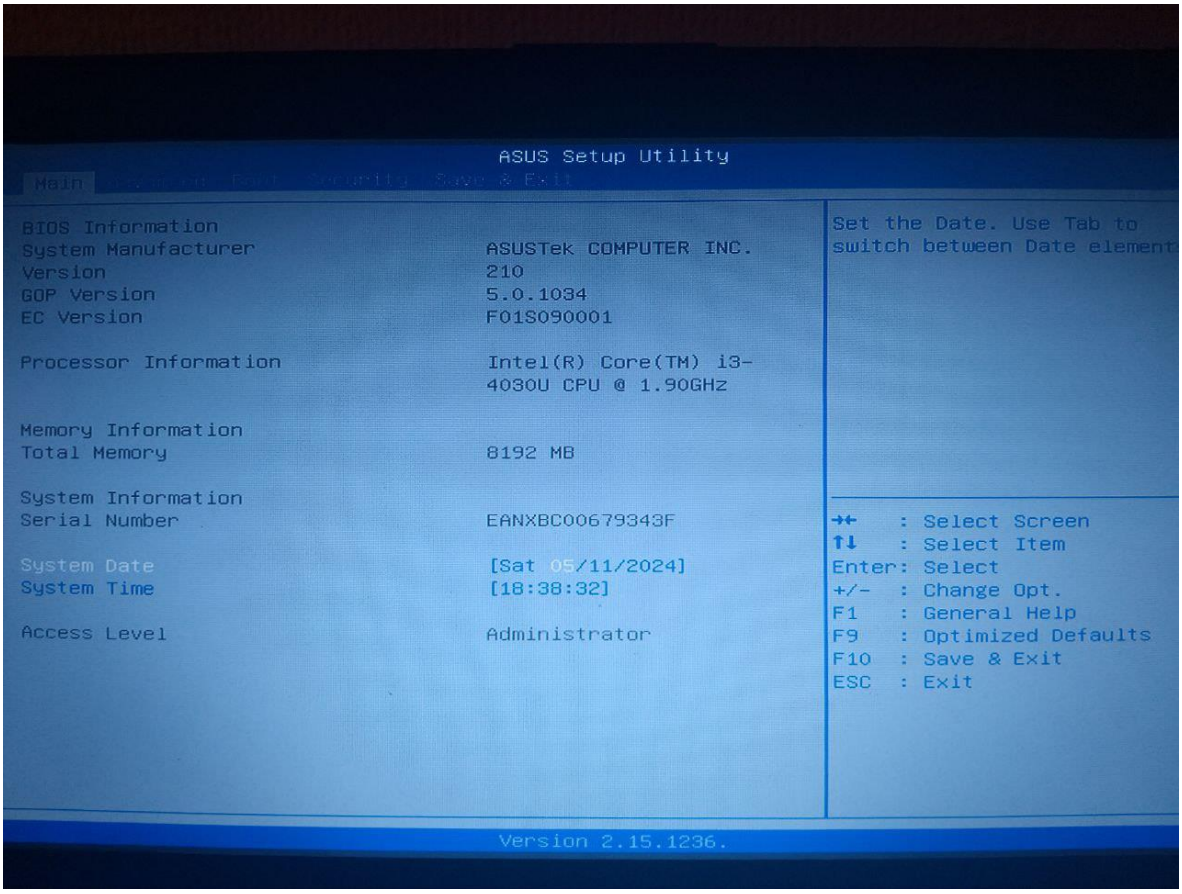


Рисунок 2.9 - BIOS ноутбука Asus PU401L

Функція моніторингу буде проводитись через веб інтерфейс котрий буде створений за допомогою flask, все що потрібно для цього те щоб у ПК був IP адрес [20] . IP-адреса (айпі-адреса, скорочення від англ. Internet Protocol Address) - унікальна мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP. У мережі Інтернет потрібна глобальна унікальність адреси. У випадку роботи в локальній мережі потрібна унікальність адреси в межах мережі. У версії протоколу IPv4 IP-адреса має довжину 4 байти. Після чого при активації клієнтської частини можна буде по IP продивитись стан батареї або ДБЖ.

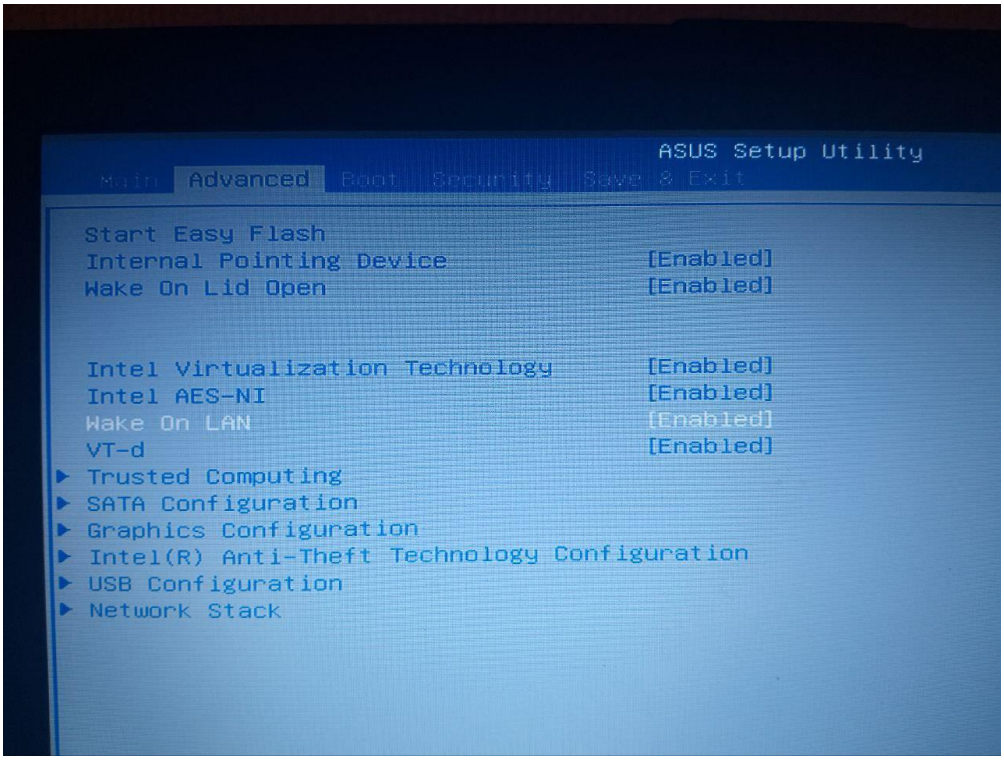


Рисунок 2.10 - Wake-On-LAN ноутбука Asus PU401L

Структура програми являє собою 3 основних файли та 2 файли даних один у вигляди бази даних а інший у вигляди звичайного текстового файлу.

Перший файл буде основним у котрому буде зібрано увесь функціонал програми та він повністю автономний він є центральним та має інтерфейс у вигляді CLI. Другий файл забезпечує графічний інтерфейс що дозволяє зручно керувати програмою, без основного файлу він не буде працювати. Третій це веб інтерфейс у котрому буде відображатись статистика про стан акумуляторної батареї.

Далі було розроблено план системи моніторингу та управління електронно інформаційними системами. Підібрано програмне забезпечення для виконання моніторингу та управління. Було сплановано структуру системи так які інтерфейси потрібно реалізувати. Було визначено додаткове налаштування робочих станцій для функції Wake-On-LAN.

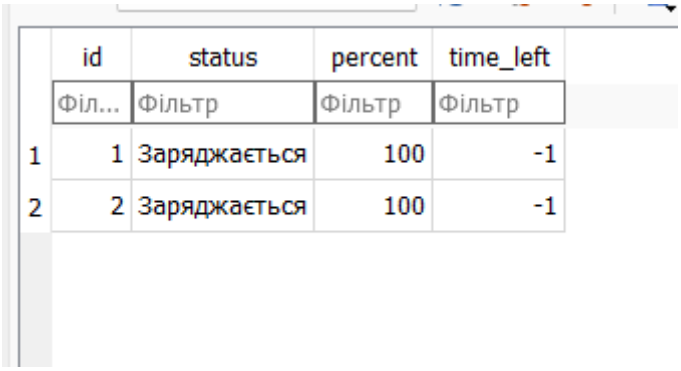
3 СИСТЕМА МОНІТОРИНГУ ТА КОНТРОЛЮ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Загальна схема взаємодії апаратно-програмного забезпечення моніторингу стану системи безперебійного енергопостачання

Перше що потрібно зробити це вирішити який тип керування ПЗ ви плануєте використовувати варіант через команду строку чи через графічний інтерфейс після чого на сервері та клієнті запускається ПЗ із вибраним типом керування, яке йде під управлінням певної кількості бібліотек серед яких основною є psutil для відстеження стану інфраструктури енергозабезпечення комп'ютера, стану акумулятора UPS та інших компонентів системи. Окремо потрібно запустити “server” частину програми котра відповідає за віддалений доступ до даних із певної машини . Також реалізовувано функціонал Wake-On-LAN, функціонал відрізняється при використані графічного чи командного інтерфейсів для того щоб були зручно використовувати обидва.

3.2 Структура та вміст бази даних

Структурно база даних має 3 таблиці : Статус,Відсоток,Залишок часу при активації програми в певний період часу дані будуть вноситись у базу даних, в залежності від стану дані звісно будуть відрізнятись. Структуру таблиці наведено на рис.3.1



	id	status	percent	time_left
	Філ...	Фільтр	Фільтр	Фільтр
1	1	Заряджається	100	-1
2	2	Заряджається	100	-1

Рисунок 3.1 — База даних

Другим типом фалу є файл налаштувань комп'ютерів під управлінням

Wake-On-LAN у якому зберігаються назва та MAC-адреса кожного із комп'ютерів, котрі були внесені через графічний інтерфейс. Приклад запису у файлі наведено на рис.3.2

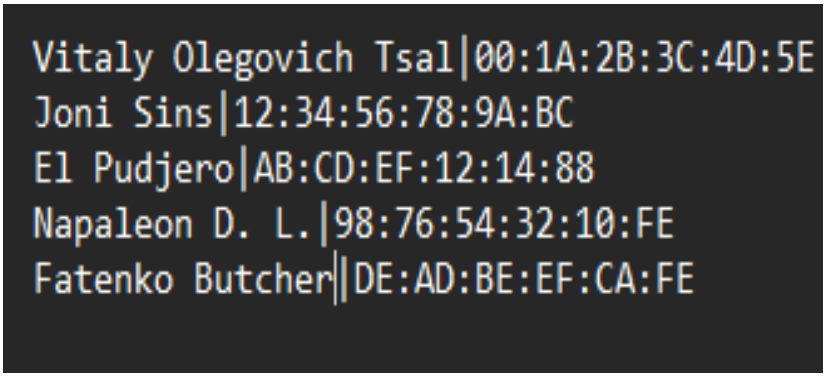


Рисунок 3.2 — Настройки Wake-On-LAN

3.3 Опис інтерфейсів та тестування ПО

Почнемо із CLI інтерфейса, він має 4 пункти, із своїм функціоналом. На рисунку 3.3 наведено головне меню, на рисунку 3.4 — приклад даних про статус батареї, яка заряджається, на рисунку 3.5 — статус роботи від батареї.

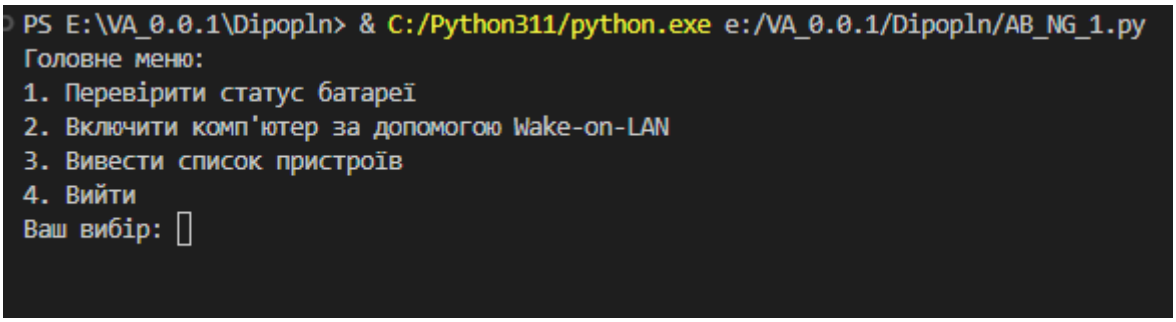


Рисунок 3.3 — CLI – інтерфейс

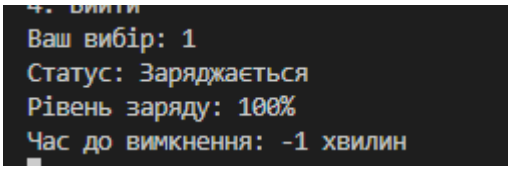


Рисунок 3.4 — Статус батареї (Заряджається)

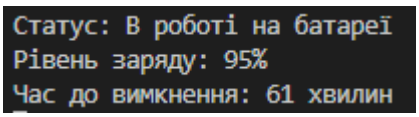


Рисунок 3.5 — Статус батареї (В роботі від батареї)

При виборі варіанту Wake On LAN, нам потрібно ввести мак адресу ПК

котрий ми хочемо увімкнути. IP адреса вводиться у сам код програми. На рисунку 3.6 показано ввід MAK адресу, рисунок 3.7 показує список пристроїв.

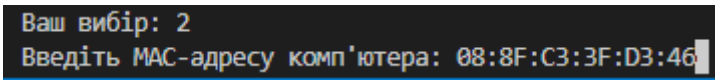


Рисунок 3.6 — Wake On LAN

У пункті 3 ми бачимо список пристроїв.

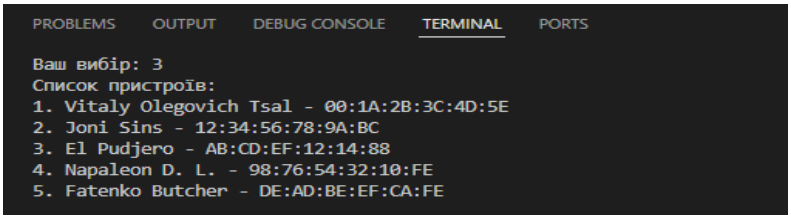


Рисунок 3.7 — Список пристроїв

Вибір пункт 4 припиняє роботу програми.

На рисунку 3.8 наведено загальний вигляд GUI.

Цей інтерфейс має той самий функціонал але є функція додавання пристроїв.

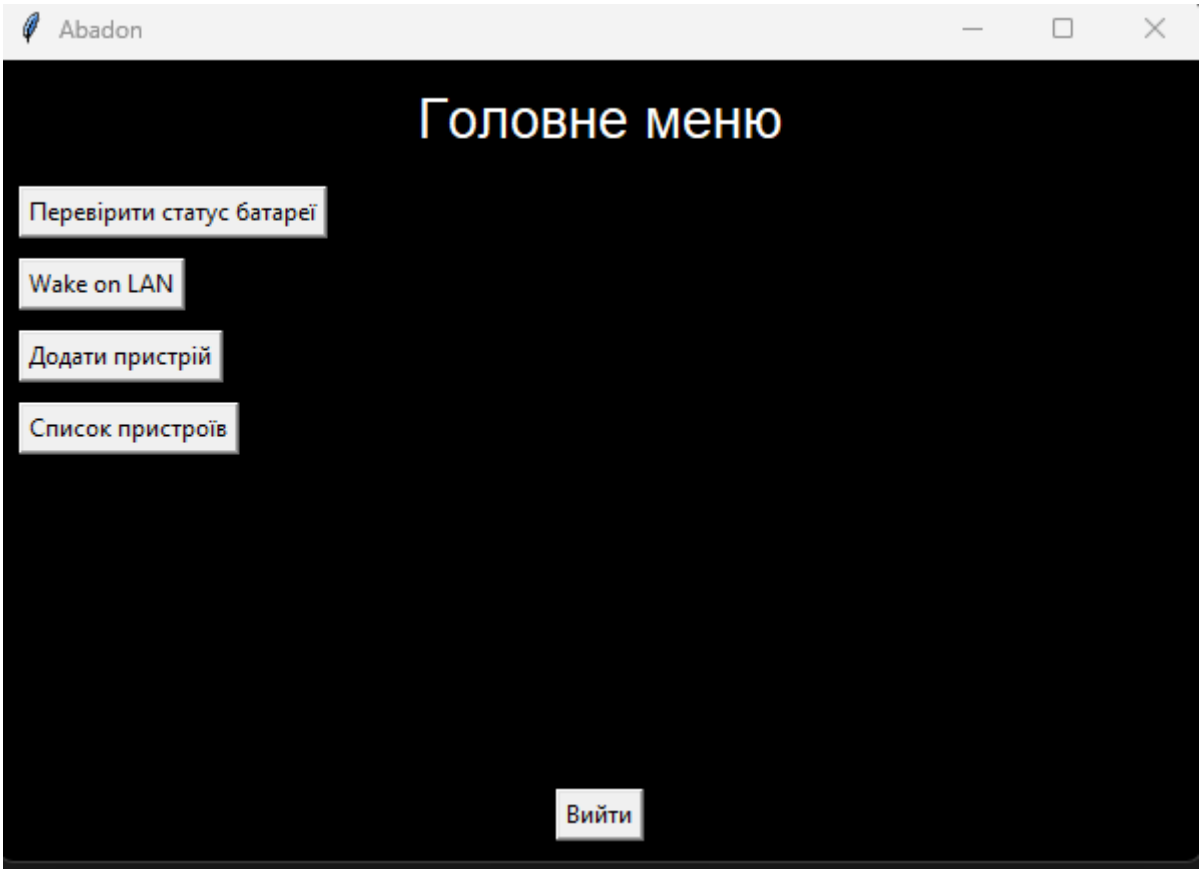


Рисунок 3.8 — вигляд GUI (Головне меню)

Після вибору 1 пункту “статус батареї” в у командній строки звідки ви

запустили цей файл з’явиться дані про стан батареї.

На малюнку 3.9 показано меню додавання нового пристрою, рисунок 3.10 показує повідомлення про додавання пристрою.

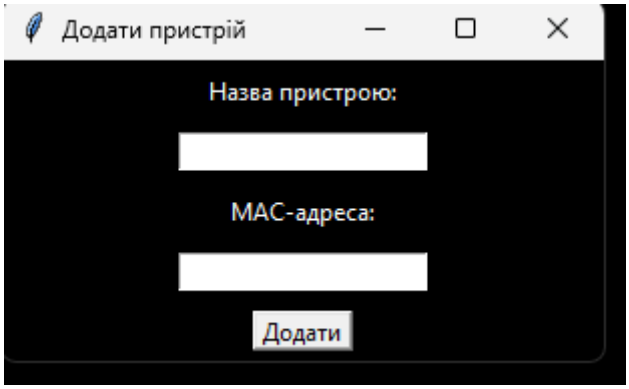


Рисунок 3.9 — Додати пристрій

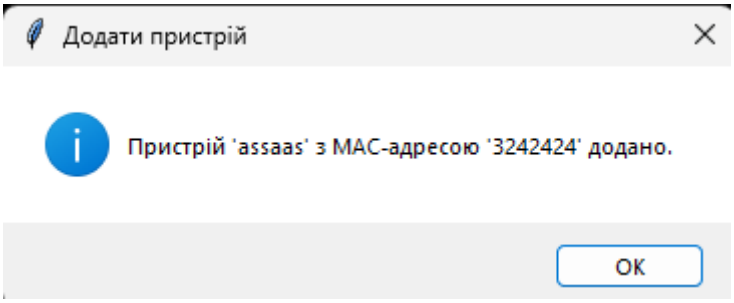


Рисунок 3.10 — Успішне додання пристрою

Список пристроїв виводить список у маленькому віконці для зручності із нумерацією. На рисунку 3.11 показано список пристроїв.

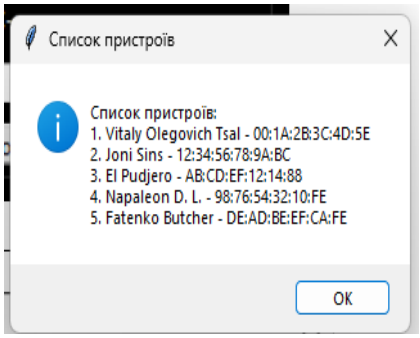


Рисунок 3.11 — Список пристроїв

Для перегляду WEB інтерфейсу потрібно буде запустити 3 файл якщо задубти за це до видасть помилку.

У меню Wake On LAN, рисунок 3.12 при введені даних буде 2 варіанти або магічний пакет сформовано згідно стандарту, відправлено на пристрій, або при введені некоректних даних програма повідомить про помилку. На рисунку

3.13 показано успішне виконання функції Wake-On-LAN, а на 3.15 показано неправильне введення даних.

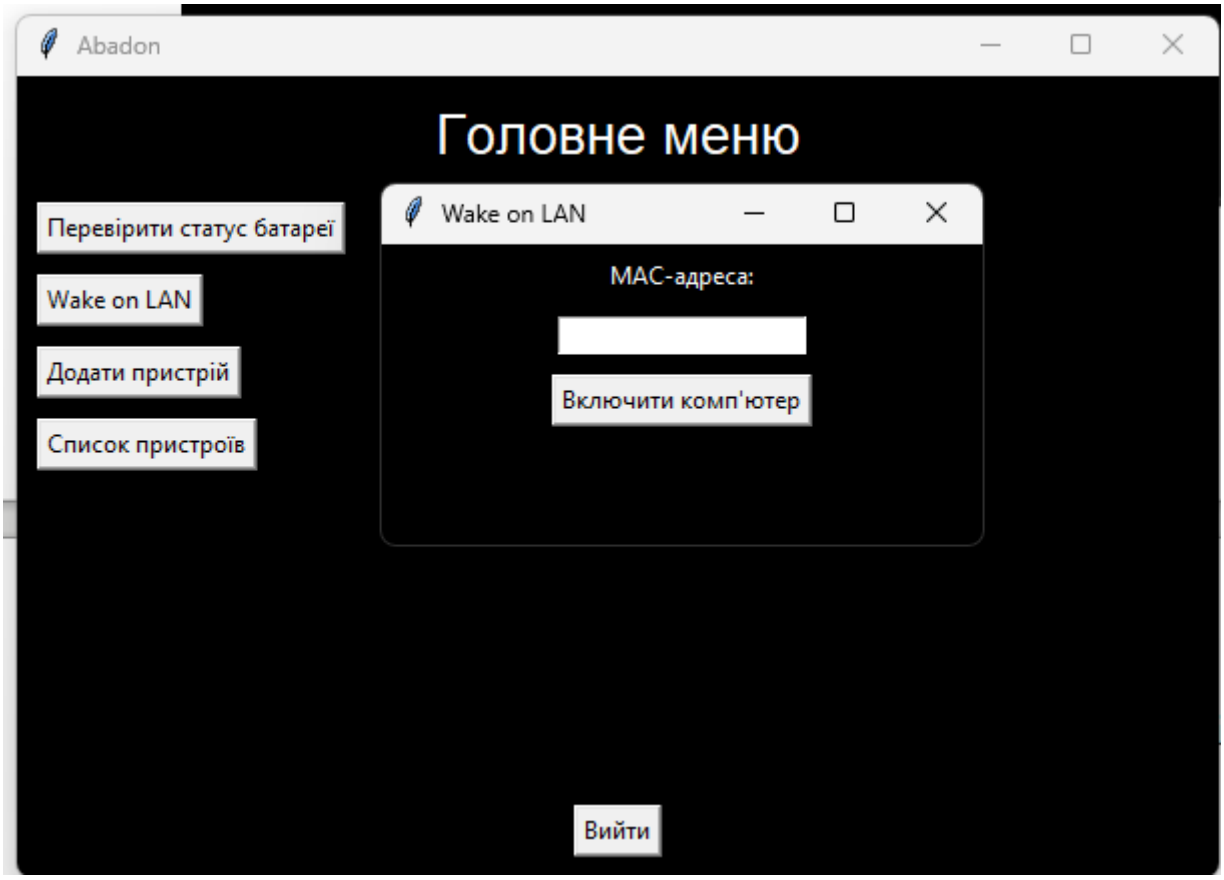


Рисунок 3.12 — Wake On LAN (GUI)

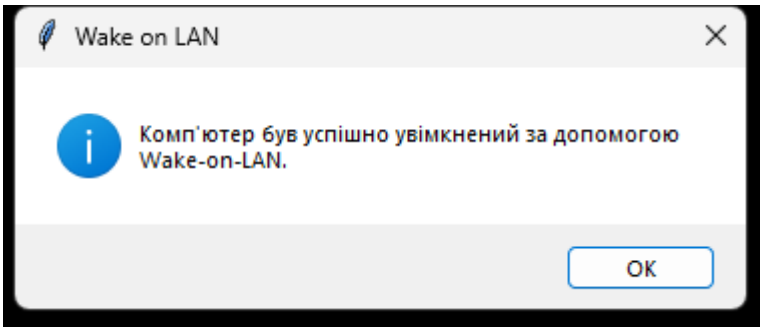


Рисунок 3.13 —Wake On LAN – успішне виконання

Спрацювання функції надсилання магічного пакета можна відстежити за допомогою сніфера WireShark. На рисунку 3.14 наведено відображення пакета. Якщо мережева карта робочої станції отримає правильно сформований магічний пакет і її налаштування виконано правильно, то це призведе до ввімкнення комп'ютера.

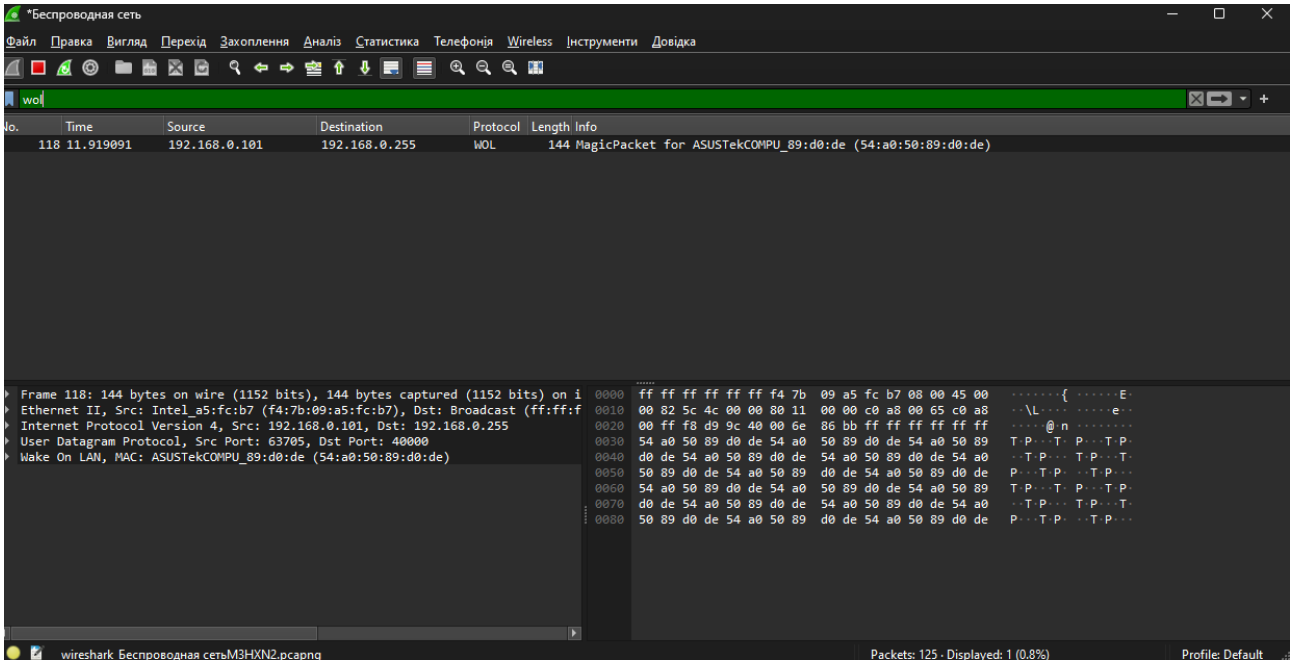


Рисунок 3.14 — пакет Wake On LAN

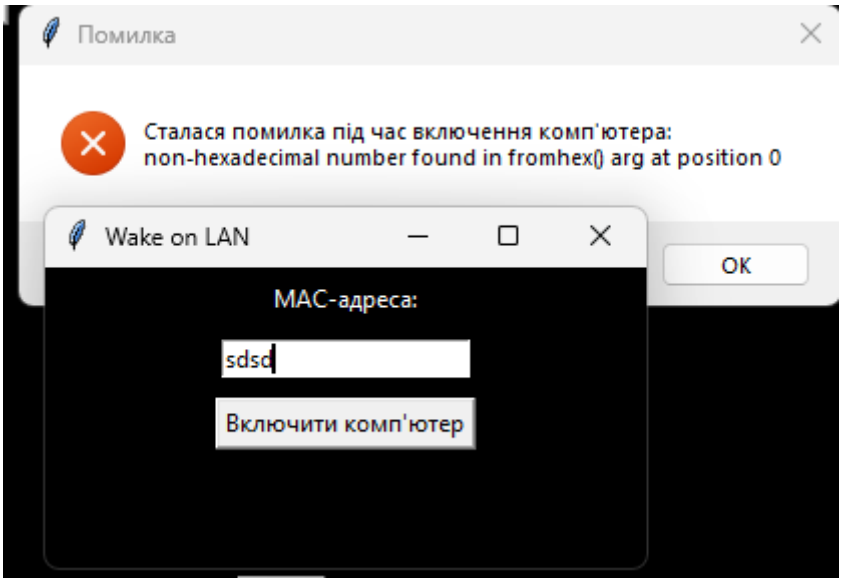


Рисунок 3.15 — Wake On LAN – неправильне введення даних

На рисунку 3.16 показано помилку при спробі зайти на веб інтерфейс без увімкнення виконавчого файлу.

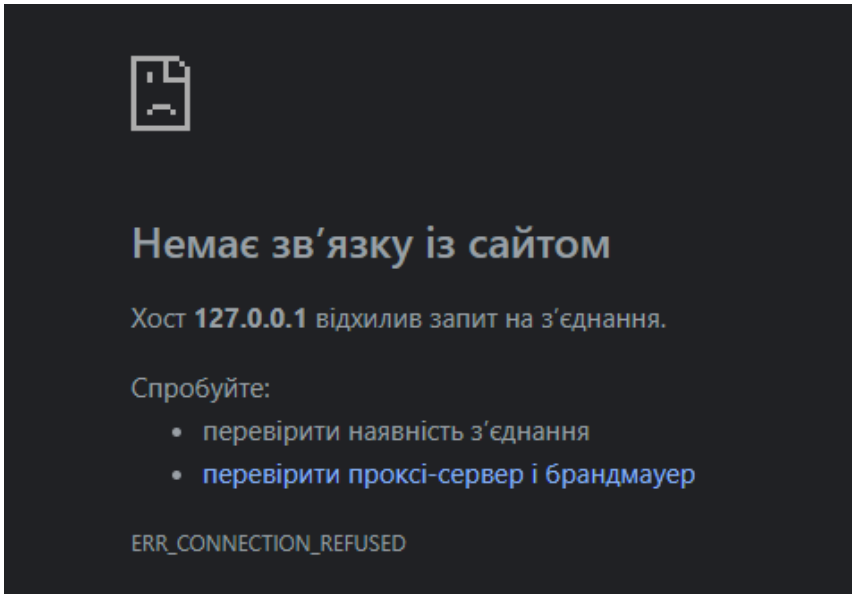


Рисунок 3.16 — Помилка при спробі переглянути веб інтерфейс без активації файлу.

При активації “server” видасть дані про початок роботи серверу flask на рисунку 3.17

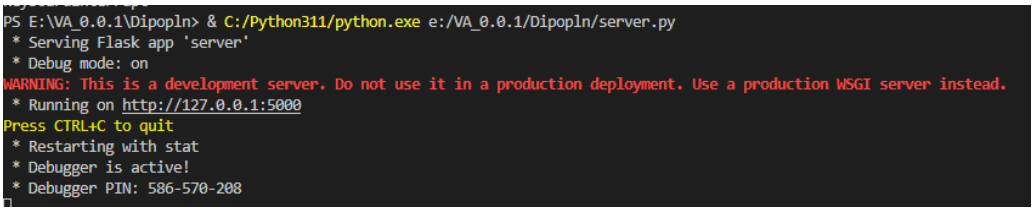


Рисунок 3.17 — сервер FLASK

Якщо перейти просто просто по адресу то з’явиться помилка як у рисунок 3.18, тому у самому коді потрібно прописати додаткову адресу у строки @app.route. На рисунку 3.19 показано вигляд адресної строки.

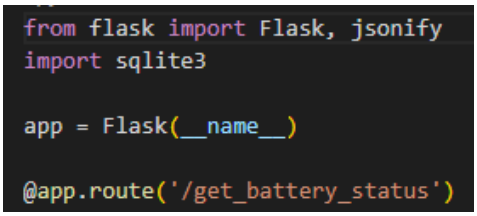


Рисунок 3.18 — Частина коду FLASK

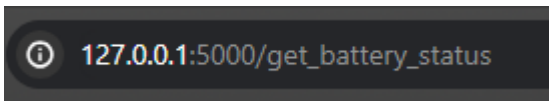


Рисунок 3.19 — Вигляд правильного запиту для доступу до WEB інтерфейсу

Після активації цієї частини програми сторінка зміниться на “активовану”

рисунок 3.20

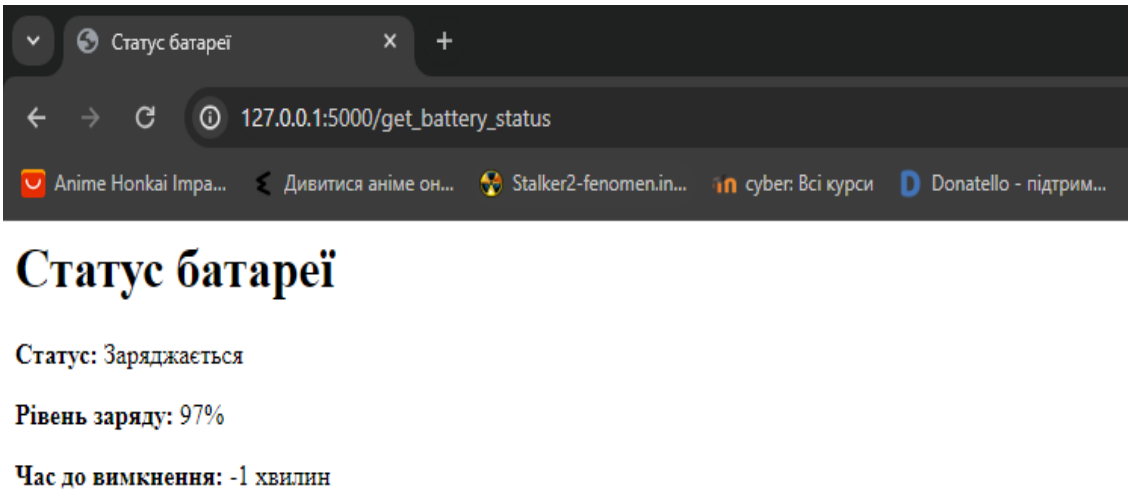


Рисунок 3.20 — Робоча частина WEB інтерфейсу

У рамках цього розділу була успішно реалізована система моніторингу та контролю енергетичної інфраструктури. Процес розробки та впровадження системи був ретельно спланований та ефективно виконаний. Під час тестування не виникло помилок.

ВИСНОВКИ

У цій роботі було проаналізовано роль енергетичної інфраструктури в забезпеченні кібербезпеки. Було поставлено завдання побудови ефективної системи управління та моніторингу інфраструктури кібербезпеки та захисту даних в умовах вимкнення електроенергії, маючи на увазі простоту використання та ефективність для звичайних користувачів і малих підприємств та бізнесів. Для цього треба розв'язати задачу з розроблення системи моніторингу та управління інформаційно-комунікаційними мережами в умовах планових або раптових блекаутів.

Далі було розроблено план системи моніторингу та управління електронно інформаційними системами. Підібрано програмне забезпечення для виконання моніторингу та управління. Було сплановано структуру системи так які інтерфейси потрібно реалізувати. Було визначено додаткове налаштування робочих станцій для функції Wake-On-LAN.

Було успішно реалізовано побудову системи моніторингу та контролю енергетичної інфраструктури. Процес розробки та впровадження системи був ретельно спланований та ефективно виконаний. Під час тестування не виникло помилок.

Отже, було реалізовано створення, та впровадження системи моніторингу та управління енергетичною інфраструктурою інформаційно комунікаційних систем в умовах можливих збоїв в енергопостачанні, яка буде надавати користувачам інформацію про стан батареї, таку як заряд та час до розрядження, щоб своєчасно приймати рішення щодо своєчасного відключення ІКС, та додаткову можливість віддалено поновити роботу.

Це є важливим кроком у напрямку підвищення стійкості енергетичної інфраструктури до можливих кіберзагроз. Це також важливий вклад у забезпечення кібербезпеки та збереження нормального функціонування суспільства, ефективне управління та спостереження.

ЛІТЕРАТУРА

1. Large blackouts in North America: Historical trends and policy implications URL: https://www.sciencedirect.com/science/article/abs/pii/S0301421509005667?via%3Dihub

2. Lessons Learned from July 2012 Indian Blackout URL: https://bura.brunel.ac.uk/bitstream/2438/22746/1/FullText.pdf

3. Hines, P., Apt, J., & Talukdar, S. (2009). Large blackouts in North America: Historical trends and policy implications. Energy Policy, 37(12), 5249–5259. doi:10.1016/j.enpol.2009.07.049 URL: https://www.researchgate.net/publication/46495999_Large_blackouts_in_North_America_Historical_trends_and_policy_implications

3. Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war URL: https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/

4. The cyber war between Ukraine and Russia: An overview URL: https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/

5. Risks Power Outages Pose to Cyber Security URL: https://www.utilitybidder.co.uk/compare-business-energy/risks-power-outages-pose-to-cyber-security/

6. Cost to run power underground vs. above ground URL: https://homeguide.com/costs/cost-to-run-power

7. SEIM URL: https://www.microsoft.com/uk-ua/security/business/security-

101/what-is-siem

8. An Overview of C++ URL: https://dl.acm.org/doi/pdf/10.1145/323779.323736

9. Java: An Overview URL: https://www.researchgate.net/profile/Ellen-Isaacs/publication/220168963_Why_do_users_like_video/links/02e7e5186b67219c70000000/Why-do-users-like-video.pdf#page=130

10.Python URL: https://www.python.org/about/

11. PSUTIL URL: https://github.com/giampaolo/psutil

12.time — Time access and conversions URL: https://docs.python.org/3/library/time.html

13. socket— Low-level networking interface URL: https://docs.python.org/3/library/socket.html

14. threading- Thread-based parallelism URL: https://docs-python-org.translate.goog/uk/3/library/threading.html?_x_tr_sl=uk&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc

15. request — Extensible library for opening URL: https://docs.python.org/3/library/urllib.request.html

16. sqlite3 — DB-API 2.0 interface for SQLite databases : https://docs.python.org/3/library/sqlite3.html

17.tkinter — Python interface to Tcl/Tk URL: https://docs.python.org/uk/3/library/tkinter.html

18. FLASK URL: https://flask.palletsprojects.com/en/3.0.x

19. Wake-on-LAN URL: https://en.wikipedia.org/wiki/Wake-on-LAN

20. Що таке IP-адреса? URL: https://2ip.ua/ua/blog/ip-address