МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чорноморський національний університет імені Петра Могили

Факультет комп'ютерних наук

Кафедра автоматизації та комп'ютерно-інтегрованих технологій

ДОПУЩЕНО ДО ЗАХИСТУ
В. о. завідувача кафедри АКІТ,
кандидат технічних наук, доцент

_____ М. І. Сідєлєв

"____" _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему: **«Автоматизована система керування електроживленням лабораторних комплексів»**

Пояснювальна записка

Спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»

151 – КРБ – 471.22017102

Студент _____ Гребеник О.В.

Керівник _____ Сідєлєв М.І.

Консультант _____ Макарова О.В.
(дата)

Миколаїв – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет ім. Петра Могили
(повне найменування вищого навчального закладу)

Інститут, факультет, відділення: Комп`ютерних наук
Кафедра, циклова комісія: Автоматизація та КІТ
Освітньо-кваліфікаційний рівень: рівень вищої освіти перший (бакалавр)

Напрям підготовки 151 «Автоматизація та приладобудування»
(шифр і назва)
Спеціальність 151 «Автоматизація та комп`ютерно-інтегровані технології»
(шифр і назва)

ЗАТВЕРДЖУЮ
В.о.завідувача кафедри, голова циклової комісії

Сідєлєв М. І. _____
"____"_____2023 р

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Гребеника Олександра Володимировича
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)
Автоматизована система керування електроживленням лабораторних комплексів
керівник проекту (роботи) канд.техн.наук, доцент Сідєлєв Микола Іванович,
затверджені наказом вищого навчального закладу від "___"_____2024 р. №___
2. Строк подання студентом проекту (роботи) 14.06. 2024
3. Вихідні дані до проекту (роботи)
Об'єкт: технології керування живленням обчислювальних лабораторних комплексів. Предмет: автоматизована система керування та моніторингу електроживлення обчислювальних лабораторних комплексів.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Вступ; 1 Аналіз технічної літератури та патентної інформації; 2 Розробка АСК електроживленням обчислювального лабораторного комплексу; 3 Розробка АСК доступом до захищених зон обчислювального комплексу; 4 Охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
– структурна схема обчислювального лабораторного комплексу;
– функціональна схема АСК живленням;
– блок-схема алгоритму роботи автоматичного перемикача фаз;
– електрична принципова схема АСК живленням;
– функціональна схема АСК доступом;
– блок-схема алгоритму роботи АСК доступом;
– електрична принципова схема АСК доступом;
– вигляд компонентів розроблених систем.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Сідєлєв М.І., доцент кафедри АКІТ	12.10.2023	
2	Сідєлєв М.І., доцент кафедри АКІТ	03.01.2024	
3	Сідєлєв М.І., доцент кафедри АКІТ	03.01. 2024	
4	Макарова О.В., ст. викладач кафедри екології	19.04. 2024	

7. Дата видачі завдання «12» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Затвердження пропозицій теми від керівника	22.09.2023	
2	Обговорення із студентом затвердженої теми	01.10.2022	
3	Формування завдання	13.10.2022	
4	Визначення актуальності, об’єкту, предмету	01.11.2022	
5	Пошук літератури, патентний пошук, уточнення задач дослідження	15.11.2022	
6	Виконання першої частини	01.12.2023	
7	Аналіз керівником записки першої частини (ЕВ*), формування зауважень та пропозицій	29.12.2023	
8	Передзахист першої частини	26.01.2024	
9	Опрацювання другої частини	15.03.2024	
10	Робота над третьою частиною	19.04. 2024	
11	Робота над розділом з охорони праці	20.05. 2024	
12	Передзахисти	03.06. 2024	
13	Передача (ДВ) кваліфікаційної роботи	14.06. 2024	

*ЕВ – електронний варіант, ДВ – друкований варіант.

Студент _____ Гребеник О. В.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи)

_____ Сідєлєв М. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

до кваліфікаційної роботи бакалавра

«Автоматизована система керування електроживленням лабораторних комплексів»

Студент 471 гр.: Гребеник Олександр Володимирович

Керівник: кандидат технічних наук, доцент Сідєлєв М.І.

Дипломна робота на тему «Автоматизована система керування електроживленням лабораторних комплексів» присвячена проектуванню системи, яка автоматизує процес керування електроживленням обчислювальних комплексів, забезпечуючи високу надійність та захист обладнання від відхилень в системі електропостачання. Для досягнення мети був проведений аналітичний огляд сучасної технічної літератури щодо будови обчислювальних комплексів, досліджено існуючі системи керування та розподілу електроенергії. Розроблено проект пристрою перемикання фаз електромережі з функцією моніторингу та оповіщення на базі мікроконтролера Arduino. Проведено розрахунки діапазону допустимих значень напруги в електромережі, максимального навантаження на систему, а також характеристики силових провідників використаних у системі.

Розроблено проект пристрою контролю доступу до захищених зон обчислювального комплексу. Проведено аналіз RFID та NFC технологій. Розроблено функціональну, електричну принципову та блок-схему алгоритму системи контролю доступу. Застосовувалися сучасні інструменти розробки електронних систем, включаючи мікроконтролери та програмне забезпечення для моделювання електричних схем.

Дипломна робота складається з пояснювальної записки, що містить 91 сторінку, 26 рисунків, 1 таблицю та 45 джерел посилання.

Ключові слова: обчислювальний комплекс, автоматизована система, електромережа, мікроконтролер Arduino, RFID технологія, автоматичний контроль.

ABSTRACT

of the Bachelor`s Thesis

“Automated Power Supply Management System of Laboratory Complexes”

Student: Hrebenyk Oleksandr Volodymyrovych

Supervisor: PhD., Docent Siddelev N. I.

The thesis titled "Automated Power Supply Management System for Laboratory Complexes" is dedicated to the design of a system that automates the process of managing the power supply of computing complexes, ensuring high reliability and protecting equipment from deviations in the power supply system. To achieve this goal, an analytical review of modern technical literature on the structure of computing complexes was conducted, and existing power management and distribution systems were studied. A project for a phase switching device with monitoring and notification functions based on the Arduino microcontroller was developed. Calculations were made for the range of permissible voltage values in the power grid, the maximum load on the system, and the characteristics of the power conductors used in the system.

A project for an access control device to protected areas of the computing complex was developed. An analysis of RFID and NFC technologies was conducted. The functional, electrical schematic, and block diagram of the access control system algorithm were developed. Modern tools for electronic system development were used, including microcontrollers and software for modeling electrical circuits.

The thesis consists of an explanatory note, which contains 91 pages, 26 figures, 1 table, and 45 references.

Keywords: computing complex, automated system, power grid, Arduino microcontroller, RFID technology, automatic control.

ЗМІСТ

ВСТУП

Актуальність теми. У наш час галузь інженерно-комп’ютерних розрахунків та проектування займає досить значне місце у сфері інформаційних технологій. У цій галузі різні пристрої та системи виконують складні функції, які забезпечують безперервну роботу серверів та професійні обчислювальні операції. Це включає управління електроживленням, підтримання оптимального мікроклімату серверної зони, безпеку доступу та інші важливі функції. Системи керування живленням грають важливу роль у забезпеченні стабільної роботи всієї інфраструктури обчислювального лабораторного комплексу. У сучасних умовах, коли навантаження на електричні мережі постійно зростає, забезпечення безперервного та якісного електропостачання є критичним для функціонування ОЛК. З метою забезпечення стабільного живлення та управління процесами на відстані зростає потреба розробки АСК що дозволяє здійснювати керування та моніторинг через WEB-інтерфейс.

Мета: підвищення ефективності механізму керування розподілом електроенергії в обчислювальному лабораторному комплексі.

Об’єкт дослідження: технології керування живленням обчислювальних комплексів.

Предмет дослідження: автоматизована система керування та моніторингу електроживлення лабораторних комплексів.

ЗАДАЧІ

1. Виконати аналіз джерел технічної літератури та патентів.
2. Вивчити стандарти та нормативні документи, що регулюють роботу обчислювальних лабораторних комплексів, та врахувати їх при розробці системи.

3. Розглянути сучасні системи розподілення електроживлення в обчислювальних лабораторних комплексах та оцінити їх ефективність та безпеку.
4. Дослідити роботу систем керування доступом в обчислювальних лабораторних комплексах.
5. Створити функціональні схеми, блок-схеми алгоритму роботи та електричні принципові схеми систем розподілу живлення та керування доступом.
6. Розробити модель автоматизованої системи контролю та розподілу електроенергії з функцією моніторингу стану електромережі обчислювального комплексу через WEB-інтерфейс.
7. Розробити модель автоматизованої системи контролю доступу, що дозволить вести журнал отримання доступу до захищених зон обчислювального лабораторного комплексу.
8. Опрацювати питання з охорони праці.

Практичне значення отриманих результатів. Розроблену систему керування електроживленням можна використовувати при підключенні чутливого до перепаду напруги обладнання. Система розрахована на живлення навантаження з сумарною потужністю до 13.8 кВт. Цього достатньо для живлення невеликого робочого кабінету або серверних стійок.

Структура та обсяг. Дипломна робота складається зі вступу, трьох розділів та висновків.

Перший розділ присвячений аналізу технічної літератури та патентної інформації, що стосуються обчислювальних лабораторних комплексів. У цьому розділі розглянуто основні вимоги до ОЛК, їхні функції та структуру.

У другому розділі описано проектування автоматизованої системи керування електроживленням. Розглянуто теоретичне обґрунтування системи, функціональну схему автоматичного перемикача фаз, проведено розрахунки параметрів системи, а також представлено блок-схему алгоритму роботи та електричну принципову схему.

У третьому розділі представлена розробка системи контролю доступу до захищених зон ОЛК. Описано використану технологію, наявні функціональна схема, блок-схема алгоритму роботи та електрична принципова схема пристрою. Також наведено опис використаної компонентної бази системи.

У висновках зроблено підсумки проведених досліджень, сформульовано основні результати роботи та рекомендації щодо подальших досліджень і розробок.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ОЛК – обчислювальний лабораторний комплекс

АСК – автоматизована система керування

АКБ – акумуляторна батарея

CCTV – система внутрішнього відеоспостереження

NOC – центр операційних команд (Network Operations Center)

RFID – радіочастотна ідентифікація (Radio-Frequency Identification)

NFC – зв’язок ближнього поля (Near Field Communication)

UPS – джерело безперебійного живлення (Uninterruptible Power Supply)

PDU – блок розподілення живлення (Power Distribution Unit)

LAN – локальна мережа (Local Area Network)

IP – інтернет-протокол (Internet Protocol)

1 АНАЛІЗ ТЕХНІЧНОЇ ЛІТЕРАТУРИ ТА ПАТЕНТНОЇ ІНФОРМАЦІЇ

1.1 Поняття обчислювальних лабораторних комплексів, їх вимоги та функції

Обчислювальний лабораторний комплекс (ОЛК) – це організація, підрозділ або комплекс приміщень, призначених для розміщення комп'ютерів та іншого допоміжного обладнання для проведення наукових досліджень та обчислювальних експериментів [1].

Ці комплекси є "захищеними" спорудами, призначеними для забезпечення неперервної роботи важливого обладнання та обробки даних. Серед вимог до даних комплексів можна виділити:

– Надійність безвідмовної роботи та постійний моніторинг
– Управління електроживленням та мережевими комунікаціями, резервність та різноманітність шляхів керування
– Мережева безпека, контроль фізичного доступу та відеоспостереження
– Зоновий контроль внутрішнього середовища комплексу
– Пожежна безпека та системи автоматичного пригнічення пожежі

Робота сучасного обчислювального лабораторного комплексу (ОЛК) тісно пов'язана з процесом експлуатації коштовного IT обладнання. Тому якість і безпека комплексу відіграють важливу роль як базовий елемент IT-експлуатації. Ключові параметри, які є вирішальними для продуктивного функціонування, окрім IT-обладнання, включають виробниче обладнання, таке як системи розподілу електроенергії, генератори, джерела безперебійного живлення (ДБЖ), системи охолодження (чилери, вентилятори, насоси і т. д.), кондиціонери у комп'ютерних залах (CRAC), системи кондиціювання повітря та системи безпеки [2].

1.2 Будова обчислювального комплексу. Системи та складові

Обчислювальний лабораторний комплекс складається з деяких підсистем, які забезпечують функціонування об’єкта. До складу комплексу входить система електропостачання, яка підключена до електромережі та включає блок подачі живлення, акумуляторну батарею (АКБ) і дизельний генератор, що забезпечує резервне живлення у разі відключення електромережі. Система безпеки та контролю доступу гарантує захист і контроль доступу до захищених зон, що є важливим для збереження інформації та безпеки обладнання.

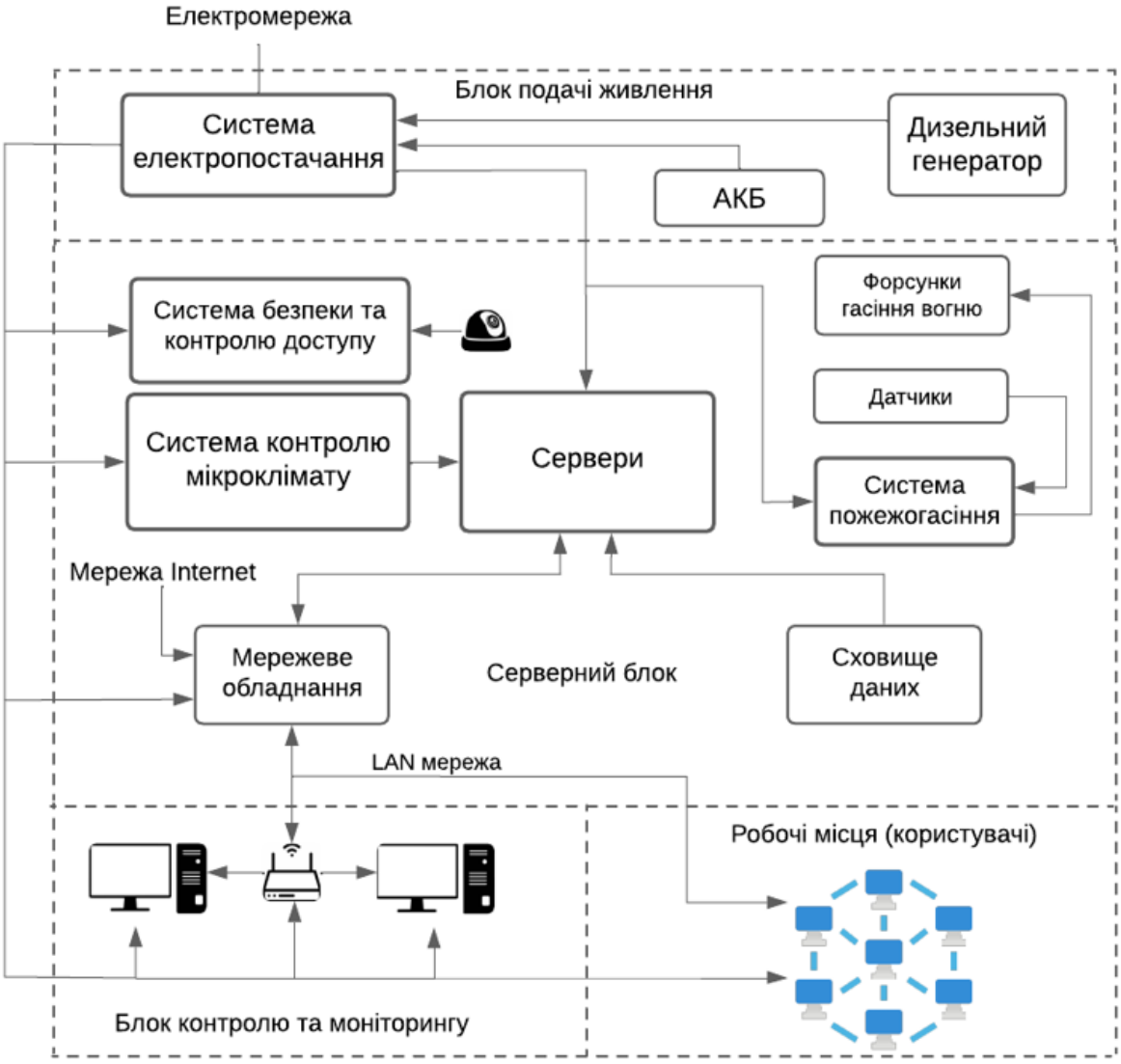

Рисунок 1.1 – Структура ОЛК

Система контролю мікроклімату підтримує оптимальні умови для роботи серверного обладнання, контролюючи такі параметри, як температура і вологість. Основну обчислювальну потужність комплексу забезпечують сервери, які обробляють дані та виконують задачі користувачів. Мережеве обладнання забезпечує зв'язок між серверним блоком та користувачами через мережу Інтернет та локальну мережу (LAN), що дозволяє ефективно передавати та отримувати дані.

Для забезпечення безпеки у випадку пожежі комплекс оснащений системою пожежогасіння, яка включає форсунки гасіння вогню та датчики для виявлення пожежі. Важливим компонентом є сховище даних, де зберігаються накопичувачі що взаємодіють з серверами, з якими працює комплекс. Користувачі взаємодіють з серверами через свої робочі місця, що включають персональні комп'ютери, підключені до мережі.

Для управління та моніторингу роботи всіх систем комплексу існує блок контролю та моніторингу, який дозволяє здійснювати централізоване управління та стежити за станом усіх компонентів. Цей структурний підхід забезпечує безперебійну роботу обчислювального лабораторного комплексу, зберігає його дані, захищає від зовнішніх загроз та підтримує оптимальні умови для функціонування обладнання.

Розглянемо системи що входять до складу ОЛК більш детально.

1.2.1 Система електропостачання

Усе обладнання в обчислювальних комплексах потребує електроживлення для своєї роботи. Так само, всі інші пристрої, які не надають електропостачання, наприклад, системи охолодження та освітлення, також потребують електроживлення. Тому проектант, плануючи електропостачання для ОЛК під час проектної фази, повинен враховувати споживання електроенергії обома групами обладнання. Зазвичай загальна потужність, що постачається до об'єкту, повинна бути у два або більше рази більшою, ніж загальна потужність, що потрібна для роботи ІТ обладнання

(включаючи майбутні навантаження). Інша половина буде споживатися системами охолодження та іншими підсистемами. Питання електропостачання є високотехнічним і професійним, яке регулюється місцевими правовими нормами, регіональними та міжнародними стандартами, а також найкращими практиками галузі [3].

Найчастіше система електропостачання містить:

– Дизель-генератор
– Перемикачі навантаження
– Панелі розподілення електроенергії
– Блоки безперебійного живлення (Uninterruptable Power Supply, UPS)
– Блоки розподілення живлення (Power Distribution Unit, PDU)

Живлення ОЛК може здійснюватися двома шляхами: через електромережу державного постачання та за допомогою генератора. Постачання електроенергії з державної мережі контролюється урядом або державними компаніями, що здійснюють розподіл електроенергії, і не вважається надійним джерелом живлення обчислювального комплексу. Проте воно використовується для зменшення витрат на енергопостачання.

Генератори – це машини, які використовуються для виробництва електроенергії. Вони перетворюють механічну енергію, яка зазвичай надходить від двигунів, у електричну енергію, яка використовується для живлення центру обробки даних. Вони є основним джерелом енергії для ОЛК, оскільки знаходяться під повним контролем операторів.

Перемикачі навантаження – це електричні системи, що використовуються для перенесення електричного навантаження з одного джерела живлення на інше. Перемикання може відбуватися з однієї лінії електропостачання на іншу, з генератора на лінію електромережі та навпаки, або між двома генераторами. Перемикання може бути активовано вручну. Також цей процес може бути автоматичним, коли використовуються автоматичні перемикачі або статичні перемикачі.

Розподільча панель, як саме назва вказує, – це корпус, в якому одне електричне живильне коло розбивається на окремі підлеглі кола для живлення різноманітних відокремлених навантажень. Кола можуть мати однакову або різну потужність. Кожне коло захищене від перевищення споживання електроенергії за визначеними межами вимикачем або електричним плавким запобіжником.

Блоки безперебійного живлення (UPS) – це електричний пристрій, який забезпечує безперервне живлення навантаження навіть у випадку відсутності основного джерела електропостачання. Він працює за рахунок зберігання електричної енергії в резервних пристроях, таких як акумулятори, від вхідної електроенергії. Потім UPS подає живлення з резервного джерела за рахунок збереженої енергії. Це відбувається майже миттєво, коли основне джерело електроенергії відключається.

Блоки розподілення живлення (PDU) – це блок, що розподіляє електроенергію до окремих пристроїв. PDU мають різні розміри і форми, деякі з них можна встановлювати на стійку, а інші більш потужні зазвичай займають вільний простір у приміщенні [3].

На рисунку 1.2 показано простий шлях подачі електроенергії до критичного та не критичного навантажень в ОЛК.

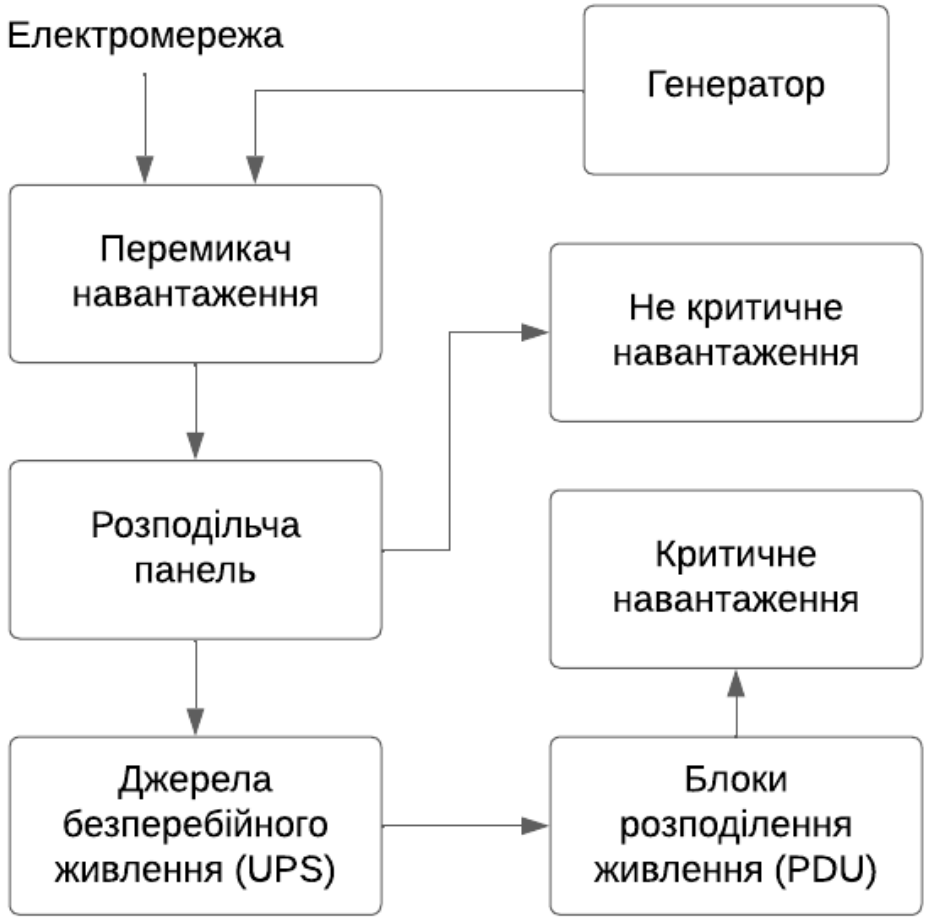

Рисунок 1.2 – Спрощена функціональна схема системи електроживлення

1.2.2 Обчислювальне обладнання

Обчислювальне обладнання, зокрема сервери, є основним елементом обчислювальних лабораторних комплексів. Сервери виконують функції обробки, зберігання та передачі даних. Вони є ключовими для забезпечення високопродуктивних обчислень, обробки великих обсягів даних, віртуалізації та інших завдань.

Сучасні сервери, особливо високощільні (High-Density Servers), забезпечують максимальну ефективність використання простору та енергії. Вони дозволяють ОЛК збільшувати обчислювальні потужності, зберігаючи при цьому компактний розмір. Це досягається завдяки впровадженню багатоядерних процесорів, великої кількості оперативної пам'яті та вдосконалених систем зберігання даних.

Рисунок 1.3 – Сервер високої щільності від компанії Lenovo

Сервери споживають значні обсяги енергії та генерують тепло, що потребує ефективних систем охолодження. Використання сучасних систем керування енергоспоживанням та охолодження дозволяє зменшити витрати на електроенергію та підтримувати стабільну роботу обладнання. Наприклад, системи охолодження на основі рідини стають все більш популярними завдяки їхній ефективності у відведенні тепла.

Крім цього, сервери в ОЛК забезпечують масштабованість та гнучкість для майбутніх розширень. Вони дозволяють легко додавати або замінювати обчислювальні ресурси в межах існуючого простору, що допомагає швидко адаптуватися до змін у потребах обробки даних та бізнес-вимогах.

Високопродуктивні обчислювальні сервери використовуються в різних галузях, таких як наукові дослідження, аналіз великих даних, хмарні обчислення та інші. Вони забезпечують необхідні обчислювальні потужності для складних завдань, таких як моделювання, машинне навчання та аналіз в реальному часі [18].

Сервери організовані в спеціальних стійках, які, у свою чергу, розташовані в рядах. Такий тип організації забезпечує ефективне використання простору, полегшує управління та обслуговування серверів, а також сприяє оптимізації охолодження та енергоспоживання.

Основним елементом структури є серверна стійка (rack), яка представляє собою металеву конструкцію для монтажу IT-обладнання.

Стандартна стійка має ширину 19 дюймів і висоту, вимірювану в "юнітах" (U), де 1U дорівнює 1,75 дюйма. Наприклад, стійка висотою 42U може вмістити до 42 серверів висотою 1U кожен [19].

Рисунок 1.4 – Серверні стійки від компанії Eaton

Сервери в стійках можуть мати різні форм-фактори, найпоширенішими з яких є 1U, 2U та 4U. Кожен з цих форм-факторів визначає висоту серверу і, відповідно, кількість серверів, які можна встановити в одну стійку. Наприклад, стійка 42U може вмістити 21 сервер висотою 2U або 10 серверів висотою 4U [20].

Стійки організовані в ряди, що полегшує управління кабелями, охолодження та забезпечення енергопостачання. Ряди стійок зазвичай розділені на холодні та гарячі проходи, що дозволяє оптимізувати потік повітря: холодне повітря подається спереду стійок, а гаряче відводиться ззаду [19].

Крім того, серверні стійки забезпечують додаткові рівні безпеки та зручність обслуговування. Вони часто оснащені блоками розподілу електроживлення (PDU), системами управління кабелями та системами охолодження. Деякі стійки мають замки на дверцятах, що забезпечує фізичну безпеку обладнання від несанкціонованого доступу [20].

Отже, структура розташування серверів в ОЛК забезпечує високу щільність розміщення обладнання, ефективне управління ресурсами та підтримку оптимальних умов для роботи серверів. Це дозволяє досягти високої продуктивності та надійності обчислювальних систем.

1.2.3 Мережа зберігання даних

Інфраструктура зберігання даних є важливою складовою будь-якої сучасної IT-системи. Вона включає різні технології та методи, що забезпечують зберігання, доступ, управління та захист даних. Двома популярними рішеннями для мережевого зберігання даних є Storage Area Network (SAN) і Network Attached Storage (NAS).

Мережа зберігання даних (SAN) — це високошвидкісна виділена мережа, яка з’єднує сервери та пристрої зберігання даних, уможливлюючи спільне використання ресурсів мережевого зберігання даних. Мережі SAN зазвичай використовують оптоволоконну технологію (Fibre Channel) для створення виділеної мережі виключно для цілей зберігання. Технологія працює незалежно від локальної мережі (LAN) і забезпечує доступ до сховищ на рівні блоків, що робить її придатною для програм, яким потрібен швидкий доступ до даних із низькою затримкою.

Мережеве сховище даних (NAS) — це рішення для зберігання на рівні файлів, яке підключається до локальної мережі та надає спільні ресурси зберігання для кількох клієнтів або серверів. На відміну від SAN, пристрої NAS працюють з використанням стандартних мережевих протоколів, таких як Ethernet, TCP/IP і NFS або SMB/CIFS, і мають резервні структури даних

для відмовостійкості. Системи NAS прості в управлінні та пропонують спрощений підхід до обміну файлами та зберігання даних [9].

SAN — це пул ресурсів зберігання на рівні блоків. SAN забезпечує більш високий рівень управління з включенням кількох серверів, які керують доступом до даних і управляють зберіганням [10]. Крім того, SAN використовує високошвидкісні кабелі та спеціальне мережеве обладнання, наприклад комутатори. Сучасні SAN базуються на оптоволоконному каналі, який забезпечує високу пропускну здатність і швидкість передачі даних до 16 ГБ на секунду. SAN може складатися з масивів твердотільних накопичувачів (SSD), які забезпечують набагато більшу продуктивність введення/виведення, ніж жорсткі диски (HDD). Хоча SAN складно розгортати та керувати, система добре масштабована та має великий показник доступності. Оскільки SAN працює у власній виділеній мережі, вона не стикається з проблемами мережевих сховищ (NAS), такими як пропускна здатність і перевантаження мережі. SAN складається з різних компонентів, які можна згрупувати в 3 основні категорії [11]. Ці категорії — компоненти хоста (сервер), оптоволоконні компоненти і компоненти зберігання.

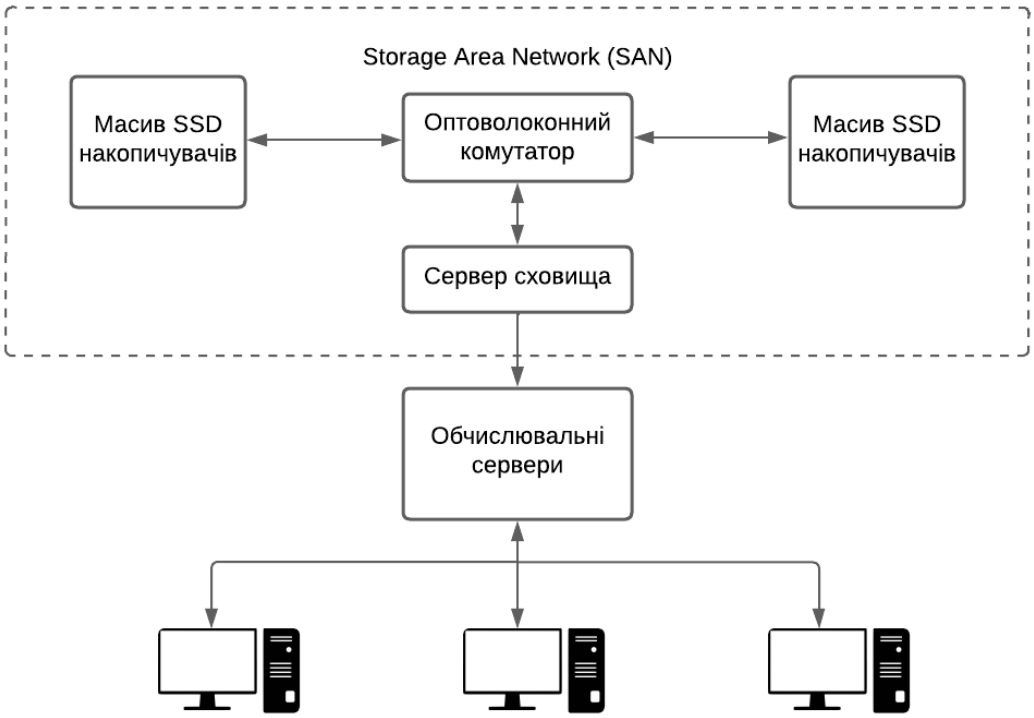

Рисунок 1.5 – Будова сховища даних SAN-типу

Системи NAS, з іншого боку, використовують стандартні мережеві протоколи та працюють як спеціалізовані файлові сервери, підключені до локальної мережі. Вони використовують мережу Ethernet та IP для зв’язку з клієнтами та забезпечують доступ до даних на рівні файлів. Пристрої NAS оснащені власними операційними системами та файловими системами, що дозволяє їм самостійно керувати сховищем файлів і виконувати різноманітні завдання керування даними. Файлова система NAS забезпечує зберігання файлів і можливості спільного використання між пристроями. Клієнти можуть отримати доступ до файлів, що зберігаються на NAS, за допомогою таких протоколів, як NFS (Network File System) або SMB (Server Message Block) [9].

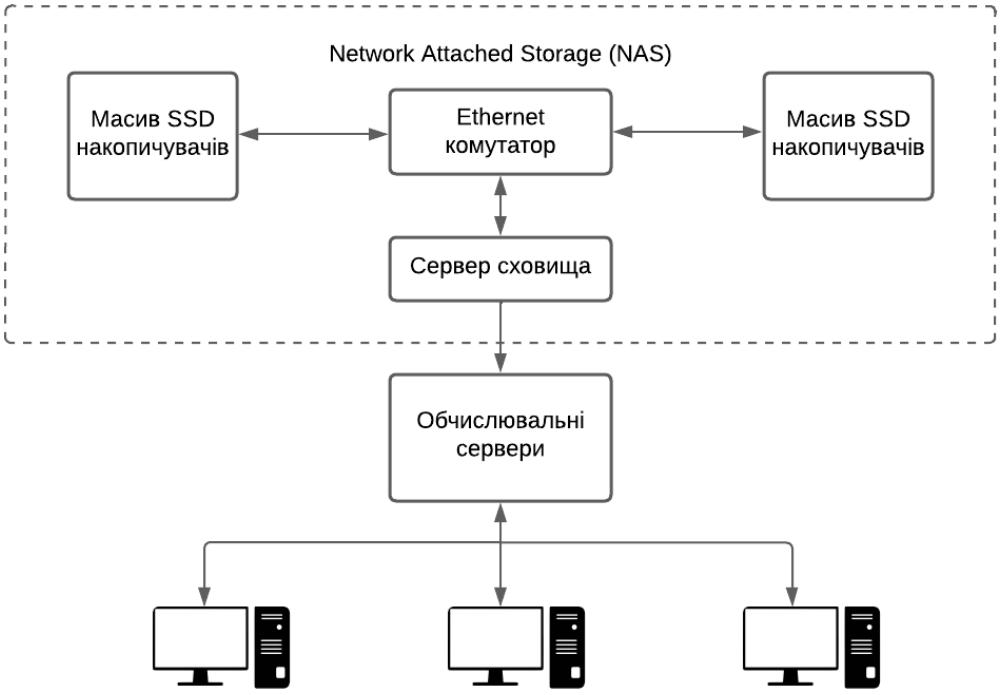

Рисунок 1.6 – Будова сховища даних NAS-типу

Системи SAN і NAS є спільними мережевими рішеннями для зберігання. У той час як SAN — це локальна мережа, що складається з кількох пристроїв, NAS — це один пристрій зберігання даних, який підключається до локальної мережі (LAN). Ось відмінності між двома системами зберігання.

Архітектура: SAN працює як окрема мережа, часто використовуючи спеціальні комутатори та кабелі, тоді як NAS підключається до існуючої інфраструктури локальної мережі (LAN). Для SAN потрібна спеціальна мережева структура, наприклад Fibre Channel або iSCSI, тоді як NAS використовує стандартне з’єднання Ethernet.

Управління: SAN зазвичай потребує більш складного управління через виділену мережу та доступ на рівні блоків. Керувати NAS відносно простіше, оскільки він інтегрується з існуючою локальною мережею та працює на рівні файлів.

Продуктивність: SAN оптимізовано для високопродуктивного мережевого зберігання, забезпечуючи низьку затримку та високошвидкісний доступ до даних на рівні блоків. Цей тип зазвичай використовується в програмах, які вимагають високої пропускної здатності та низької затримки, таких як бази даних і віртуалізація. NAS пропонує хорошу продуктивність для обміну файлами та зберігання загального призначення, але може мати дещо вищу затримку порівняно з SAN.

Масштабованість: мережі SAN відрізняються масштабованістю, оскільки вони можуть легко розміщувати додаткові пристрої зберігання, не впливаючи на цілісність мережі, і масштабуватися відповідно до зростаючих вимог до сховища. Масштабованість NAS залежить від потужності та можливостей окремого пристрою NAS.

Вартість: SAN зазвичай потребує більш спеціалізованого обладнання та інфраструктури, що робить його дорожчим для впровадження та обслуговування. NAS, будучи простішим, має тенденцію бути більш економічно ефективним і доступним для невеликих розгортань [9].

1.2.4 Система охолодження

Охолодження в обчислювальному комплексі дуже важливе, можливо, навіть більш важливе, ніж саме енергопостачання. Це тому, що за відсутності охолодження температура в серверних зонах може стрімко зростати. Це не лише зупинить роботу IT-обладнання через досягнення неприпустимих температурних умов, але й може призвести до його пошкодження. Для кожного менеджера обчислювального комплексу важливо забезпечити належне охолодження під час роботи IT-обладнання.

Враховуючи важливість надання потрібних температурних умов, природно, що створюються організації, які рекомендують найкращі практики для обчислювальних комплексів. Найбільш впізнаваною з цих організацій є ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers).

Тепло, що генерується під час роботи IT-обладнання, разом із базовою температурою приміщення, є причиною високого рівня температури в серверних приміщеннях. Охолодження – це просто відведення тепла з джерела тепла, тобто IT-обладнання, до зовнішнього середовища. Цей процес здійснюється за допомогою обладнання, яке називається кондиціонерами для комп'ютерних залів (CRAC) або обробниками повітря для комп'ютерних залів (CRAH), залежно від методу видалення тепла. ASHRAE рекомендує, щоб критичні зони обчислювального комплексу утримувалися в діапазоні температур від 18°C до 27°C. Існує три основні способи реалізації системи охолодження:

Охолодження приміщення (Room cooling).

У цьому підході охолодження надається для приміщення в цілому. Цей метод добре підходить для невеликих обчислювальних комплексів, але стає значно складнішим зі збільшенням щільності джерел тепла. Причиною є те, що кондиціонери повинні постійно перемішувати повітря в приміщенні, щоб запобігти утворенню гарячих точок і привести його до загальної рівної температури.

Охолодження рядів (Row cooling).

У цьому підході охолодження надається на основі кожного ряду. Це дозволяє кожному ряду працювати з різною щільністю навантаження, щоб можна було застосовувати різну інтенсивність охолодження за необхідністю. Гарячі точки та нерівномірності охолодження можуть легко управлятися шляхом правильного розташування і розміщення обладнання.

Охолодження стійок (Rack cooling).

У цьому підході охолодження надається на основі кожної стійки. Специфічні кондиціонери призначені для конкретних стійок. Цей підхід дозволяє максимально збільшити щільність розміщення обладнання в кожній стійці.

Немає найкращого методу – підхід до охолодження залежить від особливостей ОЛК. Бажано поєднувати різні підходи на одному об’єкті для

досягнення найвищої ефективності охолодження. Проте тенденції в розробці ОЛК надають перевагу підходу, заснованому на охолодженні рядів. Це, ймовірно, є найбільш безпечним варіантом.

Техніки видалення тепла.

З фізики відомо, що тепло може переміщуватися тільки в одному напрямку – від гарячого до холодного. А також відомо, що воно може передаватися шляхом провідності, конвекції або випромінювання.

Провідність – це передача тепла через тверду речовину, відому як провідник. Конвекція – це передача тепла через рух рідини або газу. Випромінювання – це передача тепла за допомогою електромагнітних хвиль, що випромінюються через різницю температур між двома об’єктами.

Для відведення тепла від обчислювального комплексу використовується конвекція. Це відведення здійснюється за допомогою процесу, відомого як холодильний цикл.

Холодильний цикл – це цикл випаровування, стиснення, конденсації та розширення рідини або газу, відомого як холодоагент, який ефективно відводить тепло від джерела до зовнішнього середовища.

На різних стадіях холодильного циклу фізичний стан холодоагенту коливається між рідким і газоподібним. Випаровування поглинає тепло з навколишнього середовища серверного приміщення і перетворює холодоагент у газ. Це тепло у газоподібному холодоагенті передається до компресора.

Процес стиснення збільшує тиск у газоподібному холодоагенті, змушуючи його поглинати ще більше тепла, що призводить до підвищення його внутрішньої температури. Цей гарячий газоподібний холодоагент передається до конденсатора на наступному етапі видалення тепла з серверного приміщення.

Конденсація передає тепло від високотемпературного газу високого тиску до зовнішнього повітря. Оскільки тепло переміщується з гарячої області до холодної, зовнішнє повітря спрямовується до конденсаційної

котушки. Холодоагент, що протікає через котушку, передає тепло зовнішньому повітрю, яке потім виводиться на зовнішнє середовище. Після цього холодоагент стає гарячою рідиною під високим тиском.

Розширення знижує тиск у холодоагенті, тим самим знижуючи температуру. Це завершує цикл, коли холодоагент повертається до стану холодної рідини. Після цього цикл починається знову.

Ще одним методом видалення тепла з приміщення є системи з охолодженою водою (Chilled Water Systems). Цей метод, хоч і більш ефективний та економічний, ніж системи прямого розширення з холодильним циклом, є набагато складнішим. Він використовує вентилятори та охолоджувальні котушки для видалення тепла з обчислювального комплексу за допомогою охолодженої води.

Занурювальне охолодження (Immersion cooling) — це практика охолодження в IT, за якої цілі сервери занурюють у діелектричну рідину, яка має значно вищу теплопровідність, ніж повітря. Тепло відводиться від системи шляхом прямого контакту теплоносія з гарячими компонентами та циркуляції нагрітої рідини через теплообмінники. Ця практика є дуже ефективною, оскільки рідкі охолоджуючі рідини можуть поглинати більше тепла із системи та легше циркулювати в системі, ніж повітря. Занурювальне охолодження має багато переваг: стійкість, продуктивність, надійність і вартість. Загалом діелектричні рідини, які використовуються для охолодження зануренням, поділяються на дві категорії: вуглеводні (тобто мінеральні, синтетичні або біологічні масла) і фторвуглеці (повністю розроблені рідини). Діелектричні рідини поділяються на одно- та двофазні, які відрізняються тим, чи перетворюється на газ охолоджуюча рідина під час циклу охолодження.

На відміну від багатьох інших пристроїв, комп’ютери не можуть використовувати водяне охолодження зануренням , оскільки звичайна вода є електропровідною та може пошкодити електронні компоненти. Таким чином, рідини, які використовуються для занурювального охолодження, є

діелектричними рідинами, щоб гарантувати, що вони можуть безпечно контактувати з електронними компонентами під напругою.

Вологість.

Як і температура, вологість також є важливим фактором навколишнього середовища в серверних приміщеннях. Регулювання вологості є критичним. Занадто низький рівень вологості впливає на виникнення статичної електрики, яка є електричним зарядом у стані спокою. Цей електричний заряд може призвести до електростатичного розряду (Electrostatic Discharge), що може завдати значної шкоди IT-обладнанню. Занадто висока вологість може викликати конденсацію води на IT-обладнанні, що може призвести до потрапляння води на чипи або інші важливі електричні елементи, спричиняючи виникненню короткого замикання.

При вимірюванні вологості використовуються такі терміни, як відносна вологість, точка роси та насичення.

Відносна вологість – це кількість водяної пари в повітрі у відсотках від максимальної кількості водяної пари, яку повітря може утримувати за даної температури. Відповідно, відносна вологість може змінюватися в залежності від температури повітря. Наприклад, при вищій температурі повітря буде розширюватися, що дозволить йому утримувати більше води, і, таким чином, відносна вологість знизиться. Зворотне спостерігається при вищій температурі. ASHRAE рекомендує максимальний рівень відносної вологості 60%.

Точка роси – це точна температура, при якій відносна вологість стає 100%. У цей момент водяна пара залишає повітря і з'являється у вигляді рідких водяних крапель на будь-якому об'єкті. ASHRAE рекомендує максимальну точку роси 15,5°C. Повітря вважається "насиченим" при цій температурі.

Вологість в обчислювальному комплексі регулюється за допомогою прецизійних охолоджувальних установок, які регулюють температуру і

рівень водяної пари в навколишньому середовищі. Використовуються системи зволоження/осушення. Вони виробляють або знижують кількість водяної пари в повітрі до бажаних рівнів.

1.2.6 Система безпеки

Забезпечення безпеки обчислювальних комплексів є критично важливим завданням в умовах сучасного цифрового середовища, де фізичні і кіберзагрози постійно еволюціонують. Для захисту інформації та інфраструктури використовуються різноманітні системи безпеки, які можна розділити на кілька основних категорій: фізичну безпеку, кібербезпеку, контроль доступу та системи відеоспостереження. У цьому розділі буде детально розглянуто дві ключові складові фізичної безпеки обчислювальних комплексів: системи відеоспостереження CCTV та системи контролю доступу на основі RFID технологій.

Системи CCTV (Closed-Circuit Television) є одними з найбільш ефективних інструментів для забезпечення постійного моніторингу та запису подій у режимі реального часу. Вони дозволяють контролювати вхід і вихід персоналу, відстежувати рухи всередині об'єкту та запобігати несанкціонованому доступу до критично важливих зон. Впровадження систем CCTV в обчислювальних комплексах допомагає не лише забезпечити безпеку, але й створює стримуючий ефект для потенційних порушників.

Системи контролю доступу на основі RFID (Radio Frequency Identification) технологій забезпечують ще один рівень захисту, дозволяючи точно визначати та контролювати доступ до різних зон обчислювального комплексу. Використання RFID-карток або браслетів забезпечує швидкий і зручний спосіб ідентифікації персоналу, знижуючи ризики, пов’язані з використанням традиційних ключів або паролів. Інтеграція RFID систем з іншими системами безпеки, такими як CCTV, забезпечує комплексний підхід до захисту обчислювальних комплексів.

Розглянемо принципи роботи, переваги та особливості впровадження систем CCTV та RFID в обчислювальних комплексах.

Системи CCTV (Closed-Circuit Television) відіграють вирішальну роль у забезпеченні безпеки, допомагаючи запобігати фізичним загрозам і вторгненням. Ці системи забезпечують комплексний підхід до охорони фізичної інфраструктури, доповнюючи традиційні засоби кібербезпеки.

Основною функцією CCTV є моніторинг і запис подій у реальному часі, що дозволяє виявляти і документувати будь-які підозрілі або небезпечні дії. Камери встановлюються на всіх входах, виходах та критичних зонах всередині ОК. Це дозволяє відстежувати переміщення персоналу та запобігати несанкціонованому доступу до важливих ділянок, таких як серверні кімнати та зони зберігання даних. Відеоспостереження також слугує стримуючим фактором, оскільки знання про наявність камер може відбити бажання вчинити злочинні дії [12].

Системи CCTV використовують компоненти, які безпосередньо підключені для генерації, передачі, відображення та зберігання відеоданих. Система відеоспостереження може бути настільки простою, як камера, куплена у магазині та підключена до відеомонітора. Однак більші системи, що експлуатуються професійними спеціалістами, складаються з численних компонентів, які належать до кількох основних категорій:

– Камери

– Об'єктиви

– Корпуси та кріплення

– Монітори

– Перемикачі та мультиплексори

– Відеореєстратори

Найбільш складні системи відеоспостереження можуть включати сотні камер і датчиків, інтегрованих в одну загальну систему безпеки. На рисунку 1.7 наведено схему компонентів CCTV системи. Більшість нових систем відеоспостереження максимізують переваги цифрових технологій,

використовуючи електронні бази даних, компактні компоненти та бездротові техніки передачі [15].

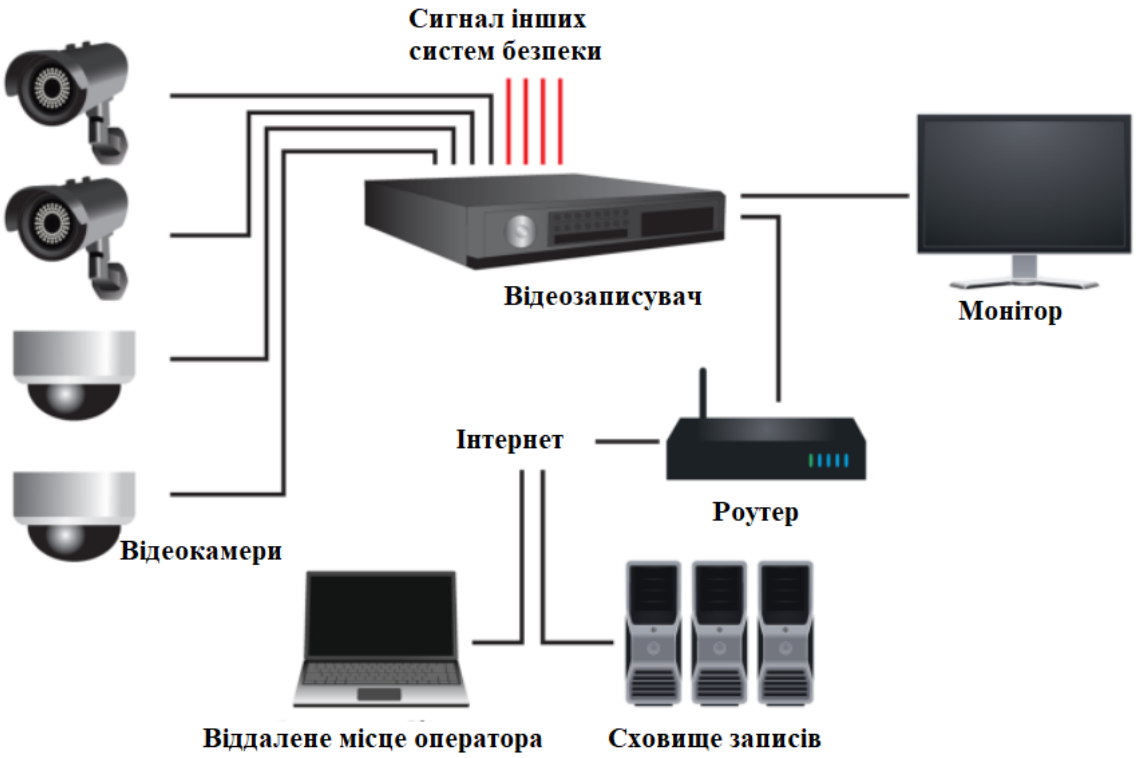

Рисунок 1.7 – Схема CCTV системи

Інфрачервоні камери CCTV здатні виявляти перегрівання серверів та іншого критичного обладнання, що є важливим для підтримання оптимальних умов експлуатації. Ці камери дозволяють здійснювати моніторинг температури і виявляти потенційно небезпечні ситуації, такі як перегрівання блоків живлення або кабелів. Це сприяє своєчасному реагуванню на аварійні ситуації та забезпечує безперервну роботу системи.

Важливою перевагою сучасних систем CCTV є можливість віддаленого моніторингу. Це дозволяє відповідальним особам спостерігати за станом обладнання з будь-якої точки світу через інтернет-з’єднання. Віддалений доступ до системи CCTV забезпечує постійний контроль та оперативне реагування на інциденти, що значно підвищує загальний рівень безпеки об'єкта.

Крім того, CCTV системи можуть бути інтегровані з іншими системами безпеки, такими як контроль доступу та системи виявлення вторгнень. Така інтеграція створює багаторівневий підхід до захисту, де всі компоненти працюють разом для забезпечення максимальної безпеки. Наприклад, система контролю доступу може бути налаштована таким чином, щоб обмежувати вхід лише для авторизованого персоналу, а CCTV забезпечує відеофіксацію цих процесів [12].

Ще одним важливим аспектом CCTV систем є можливість довготривалого зберігання відеоданих та використання відеоаналітики для аналізу безпеки. Сучасні системи дозволяють зберігати великі обсяги відеоінформації та використовувати їх для проведення детальних розслідувань інцидентів, а також для оптимізації роботи дата-центру на основі отриманих даних [14].

Таким чином, системи CCTV є невід'ємною частиною комплексної безпеки ОК, забезпечуючи захист від фізичних загроз і підтримуючи високий рівень надійності та безпеки інформації. Їх використання дозволяє не тільки запобігти фізичним вторгненням, але і забезпечити безперервний моніторинг та аналіз стану інфраструктури.

RFID і NFC контроль доступу.

У контексті контролю доступу, технологія радіочастотної ідентифікації (RFID) використовується для забезпечення обміну даними між ключовими картками та зчитувачами. Ідеально підходячи для систем контролю доступу, RFID-картки мають унікальний ідентифікаційний тег, який може бути виявлений зчитувачем на відстані до 1 метра.

Технологія ближнього поля (NFC) дуже схожа на RFID, але є більш сучасною. Хоча функціональність схожа, NFC частіше використовується в системах мобільного контролю доступу, де смарт-теги, активовані на смартфонах, можуть виступати як приймачами, так і передавачами даних. Ключова різниця полягає в більш обмеженому діапазоні дії технології NFC.

Основні компоненти системи контролю доступу RFID включають зчитувачі RFID, RFID-мітки (або картки) і апаратно-програмне забезпечення для контролю доступу. Коли людина з RFID-міткою підходить до точки входу, зчитувач випромінює радіочастотний сигнал, який активує мітку. Мітка передає свій унікальний ідентифікатор назад до зчитувача, який передає цю інформацію до контролера, який обробляє її. Програмне забезпечення перевіряє ідентифікатор у базі даних авторизованих користувачів і надає або відмовляє у доступі на основі заздалегідь визначених дозволів.

Рисунок 1.8 – Візуалізація використання технології RFID

Однією з ключових переваг систем контролю доступу RFID є підвищена безпека. Кожна RFID-мітка містить унікальний ідентифікатор, який важко підробити, що зменшує ризик несанкціонованого доступу. Крім того, ці системи можуть легко інтегруватися з іншими технологіями безпеки, такими як CCTV та сигналізаційні системи, створюючи комплексну інфраструктуру безпеки [16].

Системи RFID також забезпечують значну зручність і ефективність. Вони усувають необхідність використання фізичних ключів або складних паролів, дозволяючи швидкий і безперешкодний доступ до різних зон

всередині комплексу. Це зменшує час очікування і покращує операційну ефективність. Масштабованість систем RFID робить їх придатними для зростаючих організацій, оскільки нові мітки можна легко додати або видалити з системи.

Крім того, системи контролю доступу RFID надають цінні можливості для аудиту і звітності. Програмне забезпечення контролю записує кожен вхід і вихід, включаючи час і особу, що є важливим для проведення аудиторських перевірок безпеки та відповідності вимогам.

Проте важливо враховувати певні вразливості. Системи низької частоти RFID можуть бути піддані атакам через використання підсилювачів сигналу, а електромагнітні перешкоди можуть порушувати роботу RFID-карт і зчитувачів. Незважаючи на ці виклики, сучасні RFID-системи з використанням надійного шифрування і функцій безпеки зазвичай забезпечують високий рівень захисту.

Отже, системи контролю доступу RFID підвищують безпеку та ефективність обчислювальних комплексів, забезпечуючи надійний метод управління і контролю доступу. Їх інтеграція з іншими технологіями безпеки та масштабованість роблять їх універсальним рішенням для різних потреб у сфері безпеки [17].

1.2.7 Пункт контролю та моніторингу

Пункти моніторингу в обчислювальних комплексах являють собою спеціально обладнані приміщення, де оператори стежать за станом і роботою серверів та іншого обладнання. Ці приміщення, відомі як центри операційних або моніторингових команд (Network Operations Centers, NOCs), відіграють важливу роль в забезпеченні безперервної і надійної роботи всього обчислювального комплексу.

Основною метою пунктів моніторингу є виявлення та вирішення проблем на ранніх етапах, що дозволяє запобігти серйозних збоїв в роботі обладнання та систем. Оператори в пунктах моніторингу використовують

спеціалізоване програмне забезпечення для відстеження різних параметрів роботи серверів, мережевих пристроїв, систем зберігання даних та інших компонентів інфраструктури. Це програмне забезпечення дозволяє збирати дані про навантаження на процесори, використання пам’яті, температуру, стан живлення та багато інших показників, які можуть свідчити про потенційні проблеми.

Однією з важливих функцій пунктів моніторингу є сповіщення операторів про аномалії та критичні ситуації. Це може відбуватися через різні канали, такі як електронна пошта, SMS-повідомлення, або спеціальні системи оповіщення. Таким чином, оператори можуть оперативно реагувати на виниклі проблеми, виконувати необхідні дії для їх усунення та запобігати подальшим збоям.

Пункти моніторингу також забезпечують збір та аналіз даних, що дозволяє керівникам обчислювальних комплексів приймати обґрунтовані рішення щодо модернізації та оптимізації інфраструктури. Завдяки аналізу даних можна виявити тенденції та закономірності, що допомагають ефективніше використовувати ресурси та планувати розвиток обчислювального комплексу.

Безперебійна робота пунктів моніторингу є критично важливою, оскільки будь-яка відмова або збій може призвести до втрати даних або навіть до повної зупинки роботи обчислювального комплексу. Тому до організації цих приміщень пред'являються високі вимоги щодо надійності, резервування та безпеки.

Високий рівень автоматизації та використання сучасних технологій моніторингу дозволяють мінімізувати людський фактор і підвищити ефективність роботи операторів. Це, у свою чергу, забезпечує більш високий рівень безпеки та надійності роботи всього обчислювального комплексу.

1.3 Стандарти обчислювальних лабораторних комплексів

Проведено пошук та аналіз стандартів щодо обчислювальних комплексів. У роботі використано такі стандарти:

– ДСТУ EN 50160:2014 “Характеристики напруги електропостачання в електричних мережах загальної призначеності” [23].

– Uptime Institute Standard: Tier Classifications Define Site Infrastructure Performance [4].

– TIA-942 Telecommunications Infrastructure Standard for Data Centers (TIA-942-2005) [5].

– ASHRAE: The American Society of Heating, Refrigerating and Air-Conditioning Engineers [6].

– IEEE: Institute of Electrical and Electronic Engineers [7].

1.4 Завдання до проектування

Поставлена задача полягає в розробці автоматизованої системи керування електроживленням, що забезпечить стабільну та безперебійну роботу компонентів комплексу. Основне завдання полягає у створенні ефективної системи управління і розподілу електроенергії, яка враховуватиме нестабільність мережі електропостачання, гарантуючи високу надійність та ефективність роботи обладнання.

Крім того, проектування охоплює розробку функціональної і безпечної системи контролю доступу до ОЛК. Ця система повинна включати механізм моніторингу і управління доступом через веб-інтерфейс, що дозволить підвищити рівень безпеки та спростить ведення обліку відвідувань окремих зон ОЛК.

Інтеграція системи моніторингу є важливим етапом проектування, оскільки вона дозволить контролювати стан електроживлення та доступу в реальному часі. Впровадження інтерфейсів для віддаленого контролю і

управління системами ОЛК забезпечить ефективний нагляд і оперативне реагування на можливі проблеми.

1.5 Висновки до розділу 1

У першому розділі проведено аналіз технічної літератури та патентної інформації, що стосуються обчислювальних лабораторних комплексів (ОЛК). Визначено основні вимоги, функції та структуру обчислювальних лабораторних комплексів. Досліджено ключові аспекти їх будови.

Проведений аналіз показав, що ОЛК надають великі можливості для забезпечення безперервної роботи ІТ-обладнання, що дозволяє проводити наукові дослідження та забезпечує високу доступність ОЛК для проведення тривалих наукових досліджень. Основні вимоги до ОЛК включають надійність, безпеку, ефективне управління електроживленням та мережевими комунікаціями, а також забезпечення оптимальних умов мікроклімату.

Розглянуто низку стандартів, що регулюють проектування та експлуатацію ОЛК. Виявлено, що дотримання цих стандартів є необхідним для забезпечення стабільного та ефективного функціонування комплексу.

Таким чином, проведене дослідження технічної літератури дозволило сформувати чітке уявлення про сучасні вимоги та підходи до проектування ОЛК. В процесі вивчення ОЛК створено план розробки механізмів для забезпечення якості електроживлення та контролю доступу. На основі аналізу технічних джерел прийнято рішення інтегрувати технологію керування системами ОЛК через Інтернет, що сприятиме підвищенню ефективності управління та безпеки. Створено план для подальших етапів розроблення автоматизованої системи керування електроживленням, яка забезпечить високу надійність та ефективність роботи ОЛК, та написання наступних розділів дипломної роботи.

2 РОЗРОБКА АСК ЕЛЕКТРОЖИВЛЕННЯМ ОБЧИСЛЮВАЛЬНОГО ЛАБОРАТОРНОГО КОМПЛЕКСУ

2.1 Теоретичне обґрунтування системи

Використання автоматичного перемикача фаз в обчислювальних лабораторних комплексах є ключовим елементом забезпечення надійності електроживлення та захисту обладнання від нестабільності в мережі. Автоматичний перемикач фаз (Automatic Phase Selector) автоматично визначає найкращу доступну фазу з трифазного джерела живлення та перемикає навантаження на цю фазу, що особливо важливо в умовах високих вимог до безперервного електроживлення в ОЛК.

Основний принцип роботи автоматичного перемикача фаз полягає в постійному моніторингу напруги та частоти кожної фази. Якщо одна з фаз виходить за межі допустимих параметрів (наприклад, при виникненні перенапруги, заниженої напруги чи втрати фази), пристрій автоматично перемикає навантаження на іншу, більш стабільну фазу. Це дозволяє уникнути простоїв у роботі обчислювального обладнання та мінімізувати ризики пошкодження техніки через нестабільність електроживлення [21].

Типові автоматичні перемикачі фаз, такі як модель PEF-301 від Novatek Electro, здатні працювати з широким діапазоном напруги (220-415 В АС) та забезпечують перемикання навантаження до 16А безпосередньо або через магнітні контактори для більших навантажень. Ці пристрої також оснащені функціями захисту від перенапруги та заниженої напруги, що додатково підвищує рівень безпеки та надійності живлення [22].

Автоматичні перемикачі фаз мають низку переваг, зокрема:

– Покращення надійності роботи обладнання. Автоматичні перемикачі фаз запобігають перебоям у роботі обладнання, викликаним відмовами фази або перекосами фаз.
– Захист обладнання від коливань напруги, що може призвести до пошкоджень.

– Підвищення продуктивності. Зниження часу простоїв через проблеми з електроживленням.
– Зменшення витрат на обслуговування. Автоматичні перемикачі фаз потребують мінімального обслуговування порівняно з ручними методами перемикання [21].

2.2 Функціональна схема автоматичного перемикача фаз

Після вивчення інформації про автоматичні перемикачі фаз, їх конструкцію та принцип роботи, розроблено функціональну схему автоматичного перемикача фаз з функцією моніторингу параметрів живлення для обчислювального лабораторного комплексу. Розроблювана система призначена для забезпечення безперервного електроживлення та захисту обладнання від нестабільностей в трифазній мережі. Вона включає кілька ключових компонентів, які працюють разом для досягнення цієї мети.

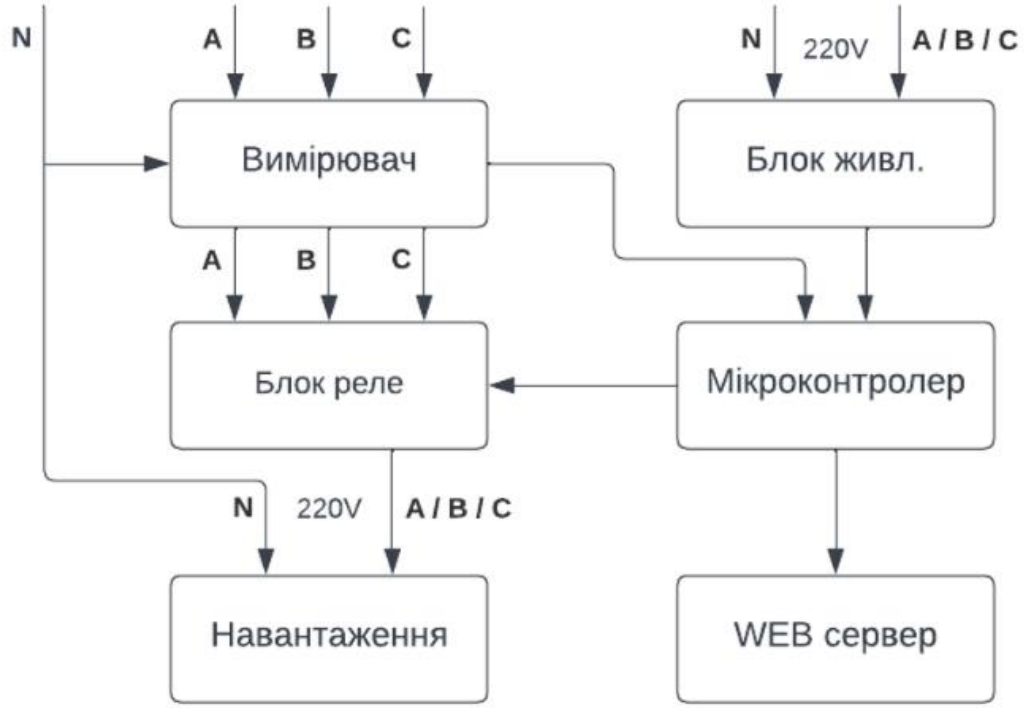

Рисунок 2.1 – функціональна схема автоматичного перемикача фаз

Функціональна схема автоматичного перемикача фаз, зображена на рисунку 2.1, складається з наступних основних компонентів:

1. Вимірювач. Цей блок підключено до усіх фазових провідників трифазної мережі електроживлення (A, B, C), та до нейтрального провідника. Вимірювач здійснює постійний моніторинг напруги, навантаження та частоти кожної фази, визначаючи їхню відповідність допустимим параметрам.

2. Блок реле. Отримуючи три фази від вимірювача, блок реле забезпечує перемикання навантаження на ту фазу, яка має найкращі показники. Він також підключений до мікроконтролера, який контролює процес перемикання.

3. Мікроконтролер. Логічний контролер обробляє дані від вимірювача та керує блоком реле на основі отриманих вимірювань. Мікроконтролер забезпечує логіку роботи всієї системи, включаючи алгоритми вибору фази та захисту від небажаних режимів роботи.

4. Блок живлення. Забезпечує живлення всіх компонентів схеми, включаючи мікроконтролер та блок реле. Він перетворює 220V змінного струму до 12V постійного струму, забезпечуючи живлення для системи.

5. Навантаження. Це обладнання, яке підключено до системи автоматичного перемикача фаз і отримує стабільне живлення від обраної фази.

6. WEB-сервер. Забезпечує можливість віддаленого моніторингу. WEB-сервер підключений до мікроконтролера і дозволяє операторам переглядати стан системи, отримувати сповіщення та змінювати налаштування в режимі реального часу.

Функціональна схема дозволяє уявити, як виглядатиме система в цілому, та слугує детальним планом для її реалізації. Вона візуально відображає взаємозв’язок між різними компонентами системи, допомагає зрозуміти принципи їх роботи та інтеграції. Це також дозволяє більш точно

планувати процес розробки, виявляти можливі недоліки та знаходити оптимальні рішення на етапі проектування.

2.3 Розрахунки параметрів АСК

Розрахунок максимальної потужності та струму.

Для розрахунку максимального струму, який буде споживатися групою робочих місць в одному кабінеті ОЛК, розглянемо середнє споживання електроенергії персональним комп'ютером разом з периферійними пристроями. Припустимо, що один персональний комп'ютер (ПК) разом з монітором споживає приблизно 600W. У випадку, коли всі ПК в кабінеті активні, максимальна потужність, яку споживає група ПК, буде вищою. Розрахуємо максимальне споживання потужності для навантаження у вигляді групи робочих місць що складається з 10 ПК:

$P_{total} = N \cdot P_{PC}$, де N – кількість робочих місць, P_{PC} – споживання одного робочого місця;

$$P_{total} = 10 \cdot 600W = 6000W = 6kW$$

Для визначення струму, який буде споживатися при такій потужності, використаємо формулу:

$I = \frac{P_{total}}{U}$, де P_{total} – загальна потужність навантаження у ватах, U – напруга в мережі;

$$I = \frac{6000W}{230V} \approx 26A$$

Отже, група з 10 робочих місць буде споживати приблизно 26А. Враховуючи можливість пікових навантажень та резерв для підключення додаткових пристроїв, візьмемо показник струму в системі 60А. Відповідно

реле та провідники мають стабільно працювати зі струмом не перевищуючим 60А.

Систему можна використовувати для забезпечення стабільного живлення серверних стійок. Для серверної зони ОЛК розглянемо стандартну серверну стійку, яка може вміщувати до 20 блочних серверів високої щільності (High-density servers). Припустимо, що середнє споживання одного серверного блоку складає 400W.

Розрахуємо максимальне споживання потужності й сили струму для серверної стійки використовуючи вищезазначені формули:

$$P_{total} = 20 \cdot 400W = 8000W = 8kW$$

$$I = \frac{8000W}{230V} \approx 35A$$

Отже, серверна стійка буде споживати приблизно 35А при повному навантаженні. Враховуючи можливі пікові навантаження, обираємо реле та провідники що розраховані на роботу з максимально допустимим струмом 60А, що забезпечить надійність роботи системи навіть при максимальній завантаженості серверної стійки.

Розрахунок діапазону допустимої напруги.

Згідно з ДСТУ EN 50160:2014 “Характеристики напруги електропостачання в електричних мережах загальної призначеності”, номінальна напруга в мережі повинна складати 230V між фазним провідником та нейтраллю. Відхилення напруги не повинно перевищувати ±10% від номінальної напруги [23]. Розрахуємо мінімально та максимально допустимі напруги:

$$U_{min} = U_{nom} \cdot 0.9 = 230V \cdot 0.9 = 207V$$

$$U_{max} = U_{nom} \cdot 1.1 = 230V \cdot 1.1 = 253V$$

$$[U_{min}, U_{max}] = [207V, 253V]$$

Таким чином, допустимий діапазон напруги між фазним провідником та нейтраллю в мережі повинен мати значення від 207V до 253V. Враховуючи цей діапазон, параметри розроблюваної системи автоматичного перемикача фаз будуть розраховані на роботу в межах 207V–253V.

Розрахунок перерізу силових провідників.

Для електричних ланцюгів з максимальним допустимим струмом 60A і напругою 230V, необхідно обрати відповідний переріз силових провідників. Відповідно до норм ПУЕ (Правила улаштування електроустановок), переріз провідників визначається за максимально допустимим струмом та допустимим нагріванням провідника [24].

Максимальний струм, що проходить через силові провідники, становить 60A. Вибір перерізу провідника залежить від матеріалу провідника (мідь або алюміній) та умов його прокладання. Зазвичай використовуються мідні провідники через їх кращі провідні властивості.

Максимальний допустимий струм для мідного кабелю та проводу регулюється таблицею 1. Згідно з цією таблицею, допустимий тривалий струм для проводів з мідними жилами з гумовою ізоляцією в металевих захисних оболонках, а також кабелів з мідними жилами з гумовою ізоляцією в свинцевій, полівінілхлоридній, найритовій або гумовій оболонці встановлюється відповідно до стандартів безпечної експлуатації та ефективності електроустановок.

Таблиця 1 – Допустимий тривалий струм для проводів і шнурів з мідними жилами

Переріз струмопровідної жили, мм²	Струм, А, для проводів та кабелів					Навантаження потужності, кВт, для проводів та кабелів				
	одножильних	двожильних		трижильних		одножильних	двожильних		трижильних	
	при прокладці					при прокладці				
	в повітрі	в повітрі	в землі	в повітрі	в землі	в повітрі	в повітрі	в землі	в повітрі	в землі
1,5	23	19	33	19	27	5,1	4,2	7,3	12,5	17,8
2,5	30	27	44	25	38	6,6	5,9	9,7	16,5	25,0
4	41	38	55	35	49	9,0	8,4	12,1	23,0	32,3
6	50	50	70	42	60	11,0	11,0	15,4	27,6	39,5
10	80	70	105	55	90	17,6	15,4	23,1	36,2	59,2
16	100	90	135	75	115	22,0	19,8	29,7	49,4	75,7
25	140	115	175	95	150	30,8	25,3	38,5	62,5	98,7

За даними з таблиці, для провідника з максимальною силою струму 60А, найближчий допустимий переріз, який перевищує це значення, є 10 мм².

Отже, переріз мідного провідника що використовується для подачі електроживлення в розроблюваній АСК повинен бути не менше 10 мм².

2.4 Блок-схема алгоритму роботи автоматичного перемикача фаз

Після розробки функціональної схеми та розрахункової частини автоматичного перемикача фаз для живлення ОЛК важливо деталізувати алгоритм роботи системи. Блок-схема алгоритму роботи системи надає наочне уявлення про послідовність дій, які виконуються для забезпечення стабільного електроживлення. На рисунку 2.2 представлено блок-схему алгоритму.

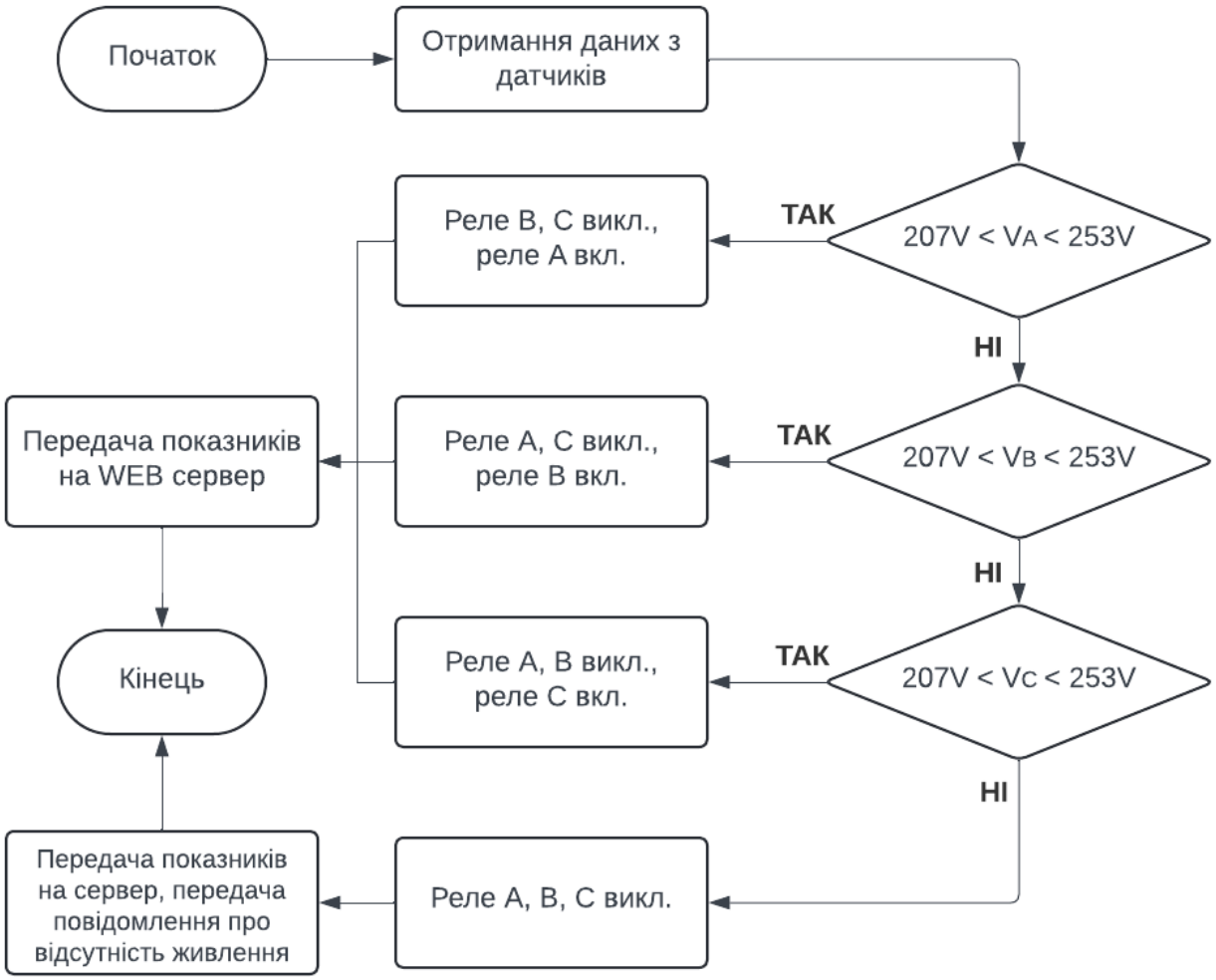

Рисунок 2.2 – Блок-схема алгоритму роботи автоматичного перемикача фаз

Опис алгоритму:

– Початок. Алгоритм починається з ініціалізації системи, яка включає запуск мікроконтролера та підготовку до отримання даних з датчиків.

– Отримання даних з датчиків. Модулі вимірювання збирають дані про напругу, силу струму, коефіцієнт потужності та частоту з усіх трьох фаз (A, B, C) та передають ці дані на обробку контролеру.

– Перевірка напруги фази A. Перевіряється, чи знаходиться напруга між фазою A та нейтраллю в межах допустимих значень (від 207V до 253V). Якщо умова виконується, система переходить до наступного кроку. Якщо ні, перевіряється наступна фаза.

– Перемикання на фазу A. Якщо напруга фази A в нормі, реле перемикається таким чином, щоб живлення навантаження здійснювалось від фази A (реле B та C вимкнені, реле A увімкнене). Після цього показники передаються на сервер, і алгоритм завершується.

– Перевірка напруги фази B. Якщо напруга фази A не відповідає допустимим значенням, аналогічно перевіряється напруга фази B. Якщо умова виконується, система переходить до наступного кроку. Якщо ні, перевіряється остання фаза C.

– Перемикання на фазу B. Якщо напруга фази B в нормі, реле перемикається таким чином, щоб живлення навантаження здійснювалось від фази B (реле A та C вимкнені, реле B увімкнене). Після цього показники передаються на сервер, і алгоритм завершується.

– Перевірка напруги фази C. Якщо напруга фази B не відповідає допустимим значенням, аналогічно перевіряється напруга фази C. Якщо умова виконується, система переходить до наступного кроку.

– Перемикання на фазу C. Якщо напруга фази C в нормі, реле перемикається таким чином, щоб живлення навантаження здійснювалось від фази C (реле A та B вимкнені, реле C увімкнене). Після цього показники передаються на сервер, і алгоритм завершується.

– Відключення усіх фаз. Якщо напруга фази C також не відповідає допустимим значенням, усі з наявних реле будуть вимкнені, а до оператора надійде сповіщення про відсутність живлення, що дасть змогу перевірити показники та встановити причини відхилень.

2.5 Електрична принципова схема автоматичного перемикача фаз

Електричну принципову схему автоматичного перемикача фаз зображено на рисунку 2.3. Система побудована на основі плати мікроконтролера Arduino UNO R3. Схема включає в себе декілька ключових компонентів: модулі вимірювання напруги PZEM-004T-100A,

мікроконтролер Arduino UNO R3, MOSFET транзистори IRF3205 та реле JQX-60F DC12V.

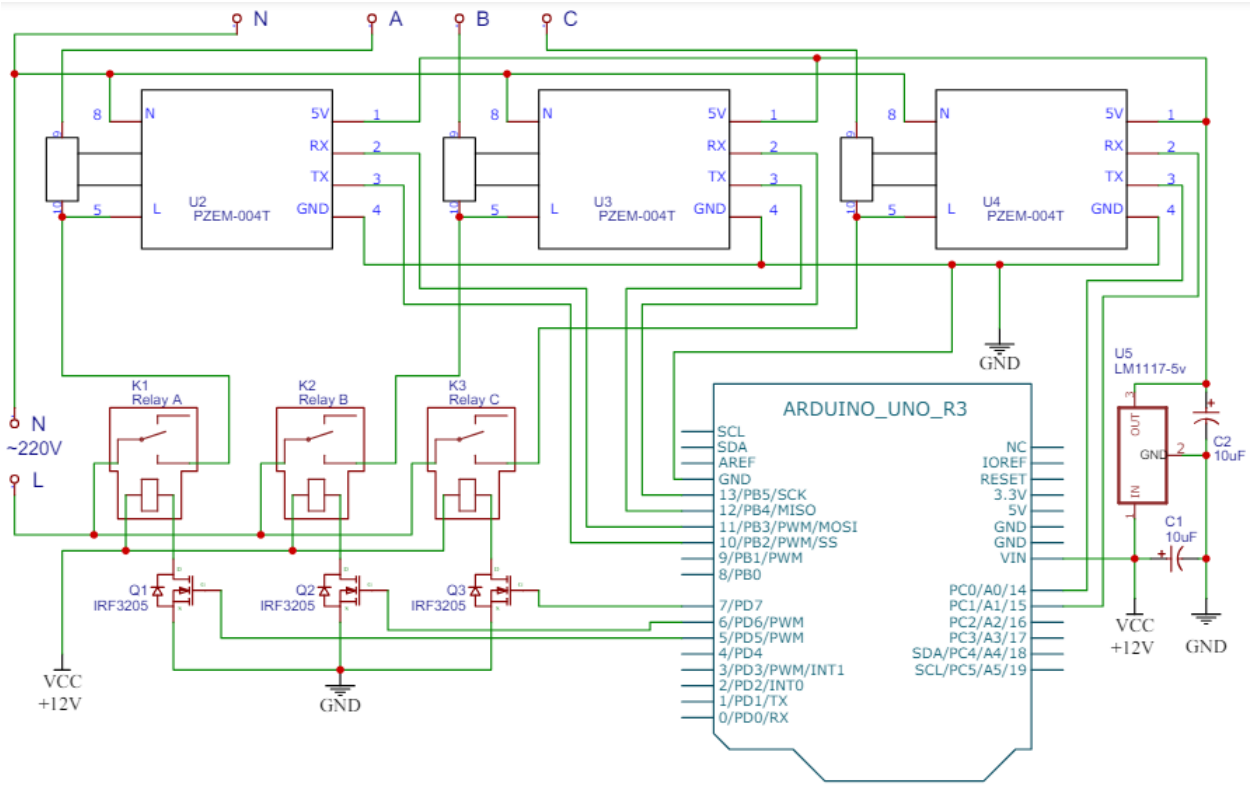

Рисунок 2.3 – Електрична принципова схема АСК живленням

Мікроконтролер Arduino UNO R3 є центральним елементом схеми, який відповідає за збір даних з модулів PZEM-004T-100A, обробку цих даних та управління реле. Модулі PZEM-004T-100A підключені до Arduino через UART інтерфейс для вимірювання напруги на кожній з трьох фаз. Перший модуль підключений до пінів 10 (TX) та 11 (RX), другий - до пінів 12 (TX) та 13 (RX), третій - до пінів 14 (TX) та 15 (RX).

Транзистори IRF3205 використовуються для комутації реле. Керуючі сигнали з Arduino (пін 5 для першого реле, пін 6 для другого реле, пін 7 для третього реле) подаються на затвори транзисторів. Витоки транзисторів з'єднані з землею, а стоки - з реле.

Реле JQX-60F DC12V розраховані на роботу з управляючим сигналом при напрузі 12V. Саме через це використовуються транзистори, адже Arduino

не може керувати реле такої потужності. Один контакт з кожної котушки реле приєднано напряму до джерела живлення. Керуючі сигнали з транзисторів комутують реле, забезпечуючи перемикання між фазами. Нормально розімкнуті контакти реле підключені до усіх трьох фаз (A, B, C), а іншим контактом реле з’єднані в одну лінію фази що йде до навантаження.

Для забезпечення стабільної роботи системи та живлення модулів PZEM-004T-100A, використовується регулятор напруги LM1117-5V, який знижує напругу з 12V до 5V. У якості обв'язки для LM1117 використано два електролітичних конденсатори на 10uF. Плюсові контакти конденсаторів підключені до входу та виходу мікросхеми, мінусові контакти – до спільного контакту заземлення (GND) [25].

Система живиться від імпульсного блоку живлення постійного струму з напругою 12V, яка подається на контакт VCC всіх відповідних елементів: Arduino, регулятора напруги LM1117 та комутуючих реле.

2.6 Компонентна база

Для проектування системи керування доступом використано такі елементи: мікроконтролер Arduino UNO з платою розширення Ethernet Shield W5100, три модуля PZEM-004T-100A, три електромагнітних реле JQX-60F DC12V, регулятор напруги LM1117-5V з двома конденсаторами в якості обв’язки, три польових MOSFET транзистори IRF3205.

Arduino UNO.

Arduino UNO – одна з найпопулярніших мікроконтролерних плат, широко використовувана для створення прототипів та навчання електроніці. Вона оснащена мікроконтролером ATmega328P, який працює на частоті 16 МГц. Плата має 14 цифрових входів/виходів, 6 з яких можуть працювати як ШІМ-виходи, та 6 аналогових входів. Її можна живити через USB або зовнішній блок живлення з напругою 7-12V. Вбудована пам'ять складає 32КБ Flash, 2КБ SRAM та 1КБ EEPROM. Завдяки своїй універсальності та великій спільноті підтримки, Arduino UNO є ідеальним вибором для даного проекту,

забезпечуючи надійність та простоту інтеграції з іншими компонентами системи.

Arduino UNO існує у декількох версіях, кожна з яких має свої особливості та переваги. Найбільш відома версія — Arduino UNO R3 (Rev3), яка є останньою та найбільш поширеною версією цієї плати. Вона відрізняється від попередніх моделей поліпшеною сумісністю з шилдами (розширювальними платами) та додатковими пінами SDA і SCL для I2C-комунікації, а також окремими пінами для IOREF і RESET. Попередні версії включають Arduino UNO R1 та R2, які мали дещо інші компоненти та розташування пінів, але загалом зберігали основну функціональність та сумісність з більшістю аксесуарів. Також існують спеціальні версії, такі як Arduino UNO WiFi, яка має вбудований Wi-Fi модуль для бездротового підключення до мережі, і Arduino UNO SMD, яка відрізняється наявністю мікросхеми в SMD-корпусі замість DIP [26].

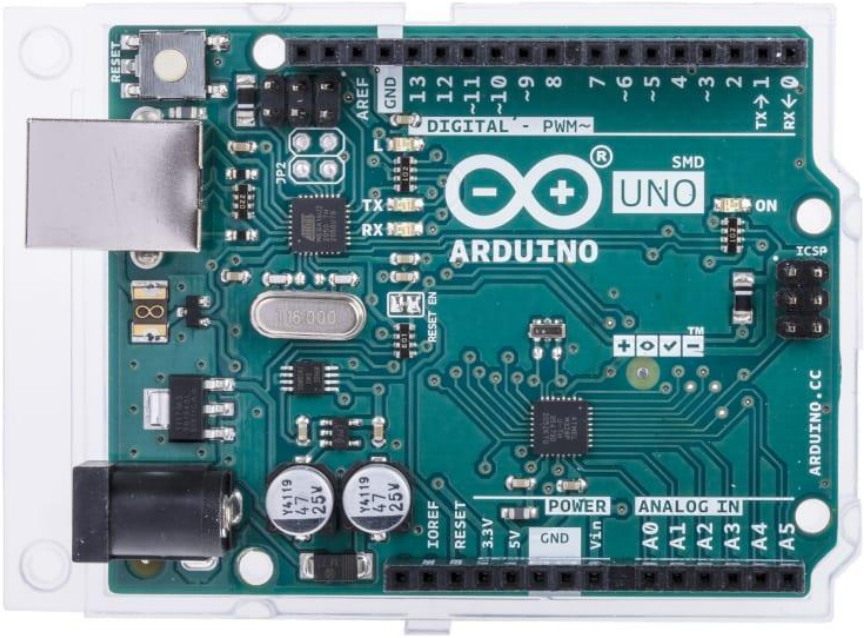

Рисунок 2.4 – Плата Arduino UNO з мікросхемою в SMD-корпусі

У моєму проекті Arduino UNO використовується як центральний контролер для системи автоматичного перемикання фаз. Вона отримує дані

від модулів вимірювання напруги PZEM-004T, обробляє їх і, залежно від отриманих значень, керує відповідними реле через транзистори IRF3205. Однією з ключових переваг Arduino є її сумісність з численними платами розширення (шилдами), що дозволяє значно розширити функціональність базової плати. За допомогою Ethernet Shield W5100 плата забезпечує передачу даних на веб-сервер, що дозволяє здійснювати моніторинг у реальному часі.

Ethernet Shield W5100.

Ethernet Shield W5100 є одним з найпопулярніших модулів для додавання мережевих можливостей до плати Arduino. Цей шилд дозволяє підключати Arduino до мережі Ethernet, що відкриває можливості для створення інтернет-з'єднаних пристроїв, віддаленого керування, передачі даних та багато іншого.

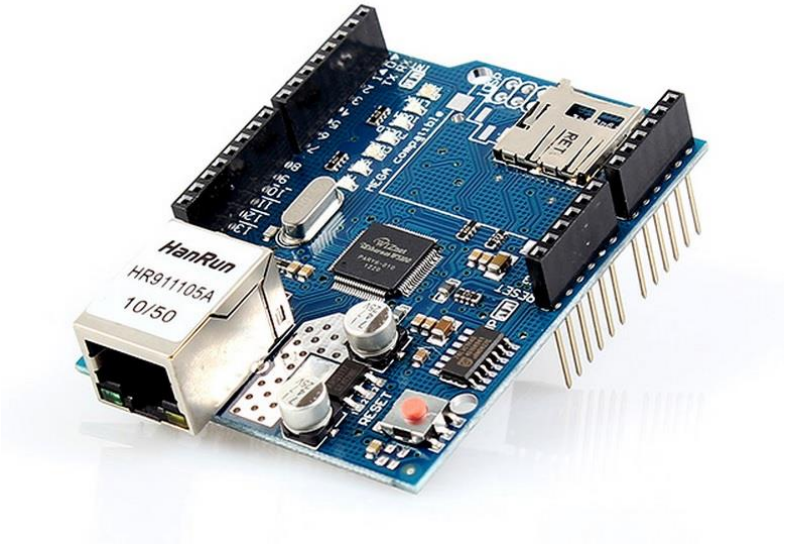

Рисунок 2.5 – Модуль Ethernet Shield W5100

Основні характеристики:

– Чіпсет: W5100, інтегрований контролер Ethernet.
– Протоколи: Підтримка TCP та UDP.
– Інтерфейс: SPI для зв'язку з Arduino.
– Порти: Чотири незалежні сокети для одночасного підключення.
– Швидкість передачі даних: 10/100 Мбіт/с.

Ethernet Shield W5100 підключається до плати Arduino через інтерфейс SPI, що забезпечує швидку і надійну передачу даних між шилдом та мікроконтролером. Шилд оснащений стандартним мережевим портом RJ-45, який дозволяє легко підключати Arduino до локальної мережі або Інтернету.

Однією з ключових переваг цього шилда є його здатність підтримувати одночасно до чотирьох незалежних з'єднань. Це означає, що Arduino може працювати як сервер, обслуговуючи кілька клієнтів одночасно, або виконувати роль клієнта, підключаючись до кількох серверів для отримання або передачі даних.

Ethernet Shield W5100 забезпечує роботу з найпоширенішими мережевими протоколами TCP та UDP, що робить його універсальним інструментом для різних мережевих додатків. Наприклад, можна створити веб-сервер для віддаленого моніторингу і керування пристроями, або налаштувати відправку даних на віддалений сервер для їх обробки і зберігання [27].

Вимірювач електроенергії PZEM-004T-100A

В якості датчиків для вимірювання електричних показників системи було обрано модуль PZEM-004T-100A. Цей модуль може вимірювати напругу, силу струму, потужність, частоту та кількість спожитої енергії, що робить його ідеальним для різних застосувань в автоматизації та контролі енергоспоживання.

Основні характеристики:

– Напруга живлення: 5V постійного струму
– Вимірювання напруги: 80-260V змінного струму
– Вимірювання струму: до 100A
– Точність: ±0.5%
– Вимірювання потужності: до 23Kw
– Вимірювання частоти змінного струму: 45-60Hz
– Вимірювання спожитої енергії: до 9999kWh

Рисунок 2.6 – Модуль PZEM-004T-100A

Модуль PZEM-004T-100A розроблений для точного вимірювання основних електричних параметрів у промислових та домашніх умовах. Він оснащений трансформатором струму, який дозволяє безпечно вимірювати високі струми до 100A без потреби в прямому контакті з високовольтними частинами електричної системи.

Основною перевагою цього модуля є його здатність надавати точні вимірювання в режимі реального часу, що робить його ідеальним для моніторингу енергоспоживання та аналізу ефективності використання електроенергії. За допомогою UART інтерфейсу модуль легко інтегрується з різними мікроконтролерами, включаючи Arduino, що дозволяє зчитувати дані та передавати їх на віддалені сервери для подальшого аналізу [28].

Модуль може використовуватися в різних додатках, таких як системи управління енергоспоживанням, розумні будинки, системи захисту електромереж та інші автоматизовані системи. Він підтримує простий протокол зв'язку, що дозволяє легко налаштовувати та інтегрувати його в існуючі системи.

Електромагнітне реле JQX-60F DC12V.

JQX-60F DC12V – це високонадійне електромагнітне реле від компанії, розроблене для використання в різних промислових та побутових застосуваннях. Це реле здатне керувати ланцюгами з високою силою струму, що робить його ідеальним для задач, пов'язаних з управлінням живленням електричних схем.

Основні характеристики:

– Номінальна напруга котушки: 12V постійного струму
– Максимальний струм контактів: 60A при 250V змінного струму
– Опір котушки: 75Ohm
– Струм та потужність котушки: 170mA, 2W
– Три силові виводи
– Механічна довговічність: 1 мільйон операцій [29].

Рисунок 2.7 – Реле JQX-60F DC12V

Реле JQX-60F DC12V широко використовується завдяки своїм відмінним електричним характеристикам та довговічності. Воно розроблене для комутації високих струмів, що дозволяє використовувати його в

додатках, де необхідна висока потужність перемикання, таких як системи автоматизації, HVAC (опалення, вентиляція і кондиціонування), побутова техніка та промислове обладнання.

Завдяки своїм характеристикам та надійності, JQX-60F DC12V є ідеальним вибором для систем автоматизації та управління живленням, де потрібна висока потужність перемикання та довговічність.

Регулятор напруги LM1117.

LM1117-5V – це стабілізатор напруги з фіксованою вихідною напругою 5 В. Він є лінійним стабілізатором і часто використовується в електроніці для отримання стабільної напруги з більш високої напруги джерела.

Основні характеристики:

– Тип: Лінійний стабілізатор напруги.
– Вхідна напруга: 6.5 В - 15 В.
– Вихідна напруга: 5 В (фіксована).
– Максимальний вихідний струм: 800 мА.
– Точність вихідної напруги: ±1.0%.
– Падіння напруги: 1.1 В при струмі 800 мА.
– Тепловий захист: Вбудований.
– Захист від короткого замикання: Вбудований.

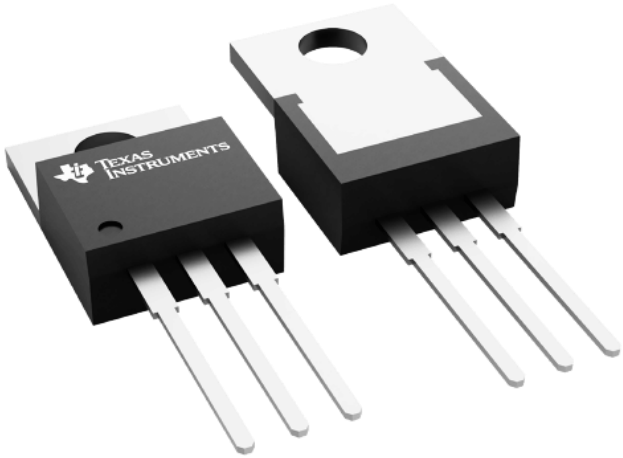

Рисунок 2.8 – Вигляд стабілізатора LM1117 в корпусі типу TO-220

LM1117-5V має три виводи:

Вхід (VIN): Підключається до джерела живлення з напругою від 6.5 В до 15 В.

Земля (GND): Підключається до загального провідника схеми (нульового потенцціалу).

Вихід (VOUT): Вихід стабілізованої напруги 5 В.

При підключенні рекомендується використовувати конденсатори для стабілізації роботи [25].

Польовий MOSFET транзистор IRF3205.

IRF3205 – це n-канальний MOSFET транзистор з високою потужністю, який широко використовується в різних електронних і електричних застосуваннях завдяки своїм відмінним технічним характеристикам. Його призначення полягає у використанні в схемах регуляторів потужності, високочастотних імпульсних джерел живлення, перетворювачів, звукових підсилювачів та іншого.

Рисунок 2.9 – MOSFET транзистор IRF3205

Технічні характеристики:

– Тип транзистора: N-канальний MOSFET
– Максимальна напруга стік-витік (VDSS): 55 В
– Максимальний струм стоку (ID): 110 А

– Опір стік-витік (RDS(on)): 8.0mΩ при VGS = 10V
– Максимальна потужність розсіювання: 200W
– Напруга порогу (VGS(th)): 2-4V

Завдяки максимальному струму стоку 110 А, IRF3205 може керувати великими навантаженнями. Низький опір у відкритому стані забезпечує мінімальні втрати енергії при перемиканні та високу ефективність. Транзистор володіє гарною термічною стабільністю. Завдяки високій потужності розсіювання 200 Вт, транзистор може працювати при високих температурах без перегріву. IRF3205 випускається у стандартному корпусі TO-220, який забезпечує ефективне відведення тепла та можливість використання радіаторів для додаткового охолодження.

MOSFET IRF3205 має три виводи:

Стік (Drain, D): Підключається до навантаження або джерела живлення.

Затвор (Gate, G): Підключається до керуючого сигналу.

Витік (Source, S): Підключається до землі або мінусового виводу живлення [30].

Висновки до розділу 2

У другому розділі описано усі етапи проектування автоматизованої системи керування електроживленням ОЛК. Спроектований пристрій може вимірювати характеристики електроенергії в мережі, автоматично керувати навантаженням, перемикаючи його на більш стабільну фазу. Дані передаються на веб-сервер на опрацьовуються операторами.

Створено функціональну схему пристрою з її детальним описом кожного блока. Створено блок-схему алгоритму роботи системи, а також побудовано електричну принципову схему в середовищі Easy EDA. Виконано розрахунки та підбір електричних компонентів системи.

3 РОЗРОБКА АСК ДОСТУПОМ ДО ЗАХИЩЕНИХ ЗОН ОБЧИСЛЮВАЛЬНОГО КОМПЛЕКСУ

3.1 Теоретичне обґрунтування системи

У сучасних умовах забезпечення фізичної безпеки обчислювального лабораторного комплексу є критично важливим завданням. Особливо це стосується контролю доступу до захищених зон, наприклад серверних приміщень, розподільчих щитів або самих серверних стійок. Для цього широко використовуються технології RFID (радіочастотна ідентифікація) та NFC (комунікація ближнього поля). Ці технології забезпечують високий рівень безпеки, зручність у користуванні та можливість інтеграції з іншими системами безпеки.

RFID (Radio Frequency Identification) і NFC (Near Field Communication) є технологіями, які дозволяють безконтактно ідентифікувати об’єкти та особи за допомогою радіохвиль. Основна відмінність між ними полягає у відстані, на яку здійснюється зчитування. NFC працює на відстані до 10 см, тоді як RFID може працювати на значно більших відстанях, в залежності від частоти та потужності сигналу [17].

Системи контролю доступу з використанням клавіатур дозволяють встановлювати персоналізовані паролі для входу до захищених зон. Цей метод часто використовується як додатковий рівень безпеки разом з безконтактними технологіями, або як резервний варіант ідентифікації у випадку відсутності карти. Системи складаються з матричних клавіатур (зазвичай 4x4 кнопки), де кожному користувачеві призначається унікальний код. Введення правильного коду дозволяє доступ до певної зони ОЛК.

Інтеграція систем контролю доступу на основі RFID/NFC та клавіатур дозволяє створити багаторівневу систему безпеки. Такі системи можуть включати:

– Журнали доступу. Всі спроби доступу реєструються у системі з вказанням часу, ідентифікаційного номеру картки або введеного пароля. Це

дозволяє відслідковувати всі входи та виходи з обчислювального лабораторного комплексу.

– Аудит безпеки. Регулярний аналіз журналів доступу для виявлення підозрілої активності або порушень безпеки.

– Дистанційне управління. Адміністратори можуть керувати правами доступу віддалено, змінювати паролі, блокувати картки у разі їх втрати або крадіжки.

Системи контролю доступу до захищених зон ОЛК, засновані на технологіях RFID/NFC та паролях на клавіатурі, забезпечують високий рівень безпеки, зручність та гнучкість в управлінні доступом. Інтеграція цих технологій дозволяє створити надійну та ефективну систему захисту для обчислювальних лабораторних комплексів [16].

3.2 Функціональна схема АСК доступом

Після вивчення теоретичних аспектів та технологій у сфері систем контролю доступу, було розроблено функціональну схему автоматизованої системи керування доступом до захищених зон обчислювального лабораторного комплексу. Ця система може використовуватися для отримання доступу до різних критично важливих зон, таких як серверні приміщення, розподільчі шафи, зони зберігання даних та інших об'єктів, що вимагають високого рівня безпеки.

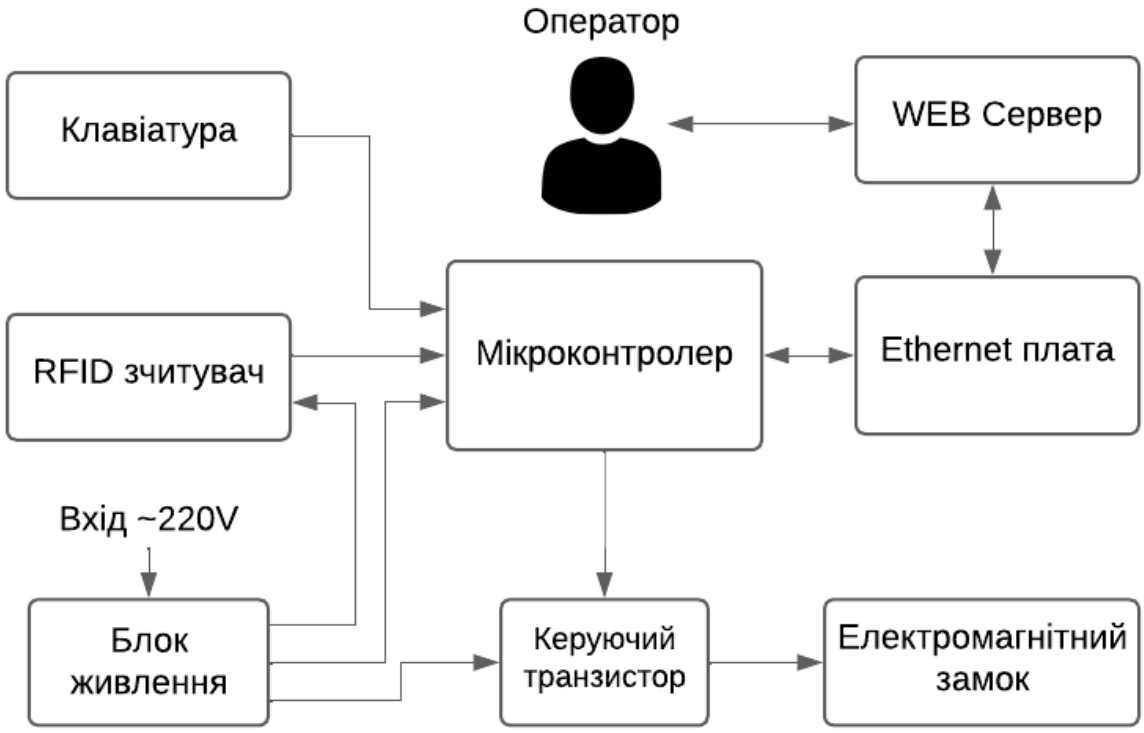

Рисунок 3.1 – Функціональна схема АСК доступом

Функціональна схема системи керування доступом, зображена на рисунку 3.1, складається з наступних основних компонентів:

1. RFID зчитувач. Зчитує ідентифікаційні дані з RFID карток та передає ці дані на мікроконтролер для подальшої обробки.

2. Клавіатура. Використовується для введення кодів доступу. Дані з клавіатури також передаються на мікроконтролер для перевірки та обробки.

3. Мікроконтролер. Центральний елемент системи, який керує всіма іншими компонентами. Обробляє сигнали з RFID зчитувача та клавіатури, а також керує електромагнітним замком через керуючий транзистор.

4. Ethernet плата. Забезпечує зв’язок мікроконтролера з WEB сервером. Надсилає до серверу дані про отриманий доступ.

5. WEB-сервер. Зберігає та обробляє інформацію про всі спроби доступу. Дозволяє оператору контролювати доступ.

6. Керуючий транзистор. Виконує функцію керування електромагнітним замком. Отримує сигнали від мікроконтролера для відкриття або закриття замка.

7. Електромагнітний замок. Являє собою соленоїд, що забезпечує фізичне блокування доступу до захищених зон. Працює під керуванням мікроконтролера та керуючого транзистора.

8. Блок живлення. Забезпечує живлення всіх компонентів системи. Перетворює вхідну напругу 220V змінного струму на низьку напругу постійного струму для живлення різних частин системи.

3.3 Блок-схема алгоритму роботи АСК доступом

Алгоритм роботи автоматизованої системи керування доступом до захищених зон ОЛК представлений у вигляді блок-схеми на рисунку 3.2. Ця схема описує послідовність дій, які виконуються системою для перевірки авторизації користувача та надання доступу до захищених зон.

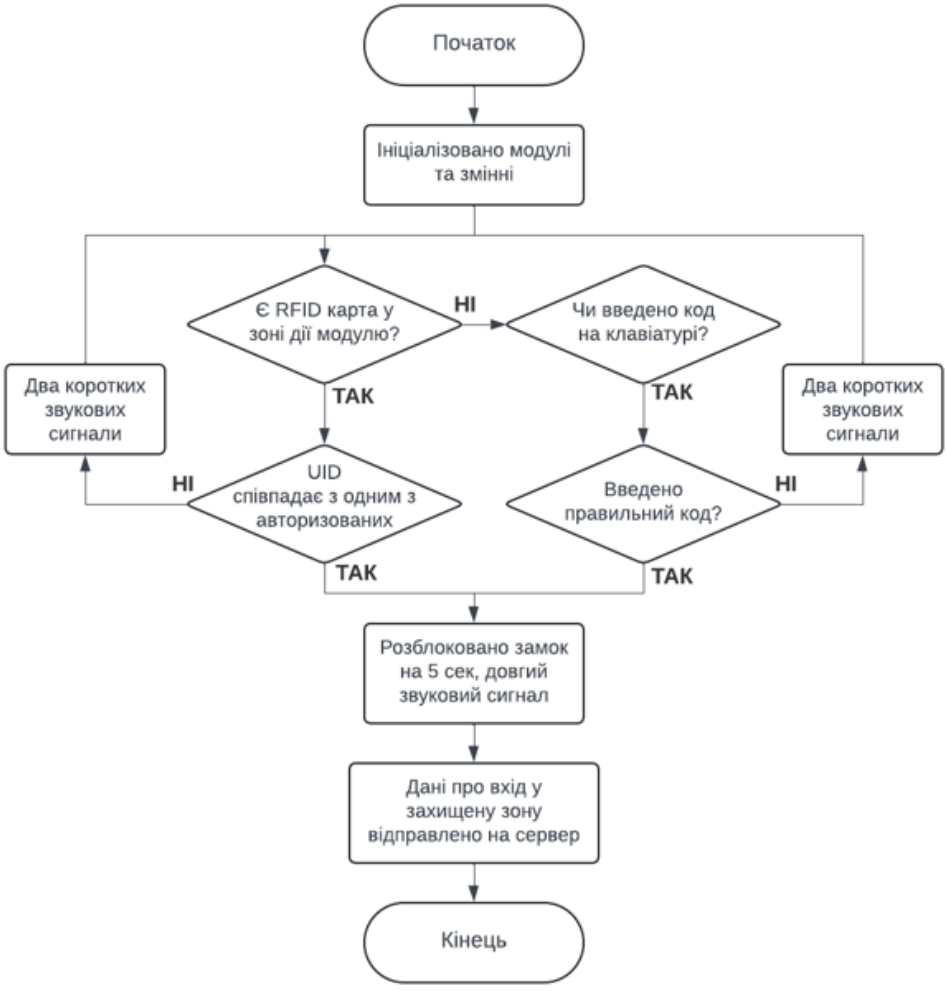

Рисунок 3.2 – Блок-схема алгоритму роботи АСК доступом

Опис алгоритму:

– Початок. Алгоритм починається з ініціалізації всіх модулів та змінних, необхідних для роботи системи. Це включає ініціалізацію мікроконтролера, RFID-зчитувача, клавіатури та інших компонентів системи.

– Наявність RFID карти у зоні дії модуля. Система перевіряє, чи знаходиться RFID карта у зоні дії зчитувача. Якщо карта відсутня, алгоритм переходить до наступного етапу - перевірки введення коду на клавіатурі. Якщо карта присутня, система переходить до наступного етапу перевірки авторизації.

– Перевірка UID RFID карти. Система перевіряє, чи співпадає UID (унікальний ідентифікаційний номер) з одним із авторизованих UID. Якщо UID не співпадає, видається два коротких звукових сигнали, що сигналізують про неуспішну спробу доступу.

– Введення коду на клавіатурі. Якщо RFID карта не знайдена, система перевіряє, чи введено код на клавіатурі. Якщо код не введено, видається два коротких звукових сигнали, що сигналізують про неуспішну спробу доступу.

– Перевірка правильності введеного коду. Якщо код введено, система перевіряє його правильність. Якщо код неправильний, видається два коротких звукових сигнали.

– Авторизація користувача. Якщо UID RFID карти співпадає з авторизованим або введено правильний код на клавіатурі, система розблоковує електромагнітний замок на 5 секунд, супроводжуючи цей процес довгим звуковим сигналом.

– Запис успішних спроб доступу. Після успішного доступу система відправляє дані про вхід на сервер для подальшого зберігання та аналізу.

– Кінець. Алгоритм завершується, очікуючи на наступну спробу доступу.

Таким чином, розроблений алгоритм забезпечує чітку та послідовну перевірку авторизації користувачів за допомогою RFID карт та клавіатури, а

також надання доступу до захищених зон ОЛК. Цей алгоритм дозволяє забезпечити високий рівень безпеки та зручність у використанні.

3.4 Електрична принципова схема АСК доступом

Електричну принципову схему системи керування доступом зображено на рисунку 3.3. Система побудована на основі плати мікроконтролера Arduino UNO R3. Він керує всіма підключеними до нього модулями та елементами. До пінів Arduino підключено інші компоненти системи, які забезпечують функціональність пристрою. Arduino живиться через пін V_{in} та спільний мінусовий контакт (GND), до яких підведено напругу 12V від блоку живлення.

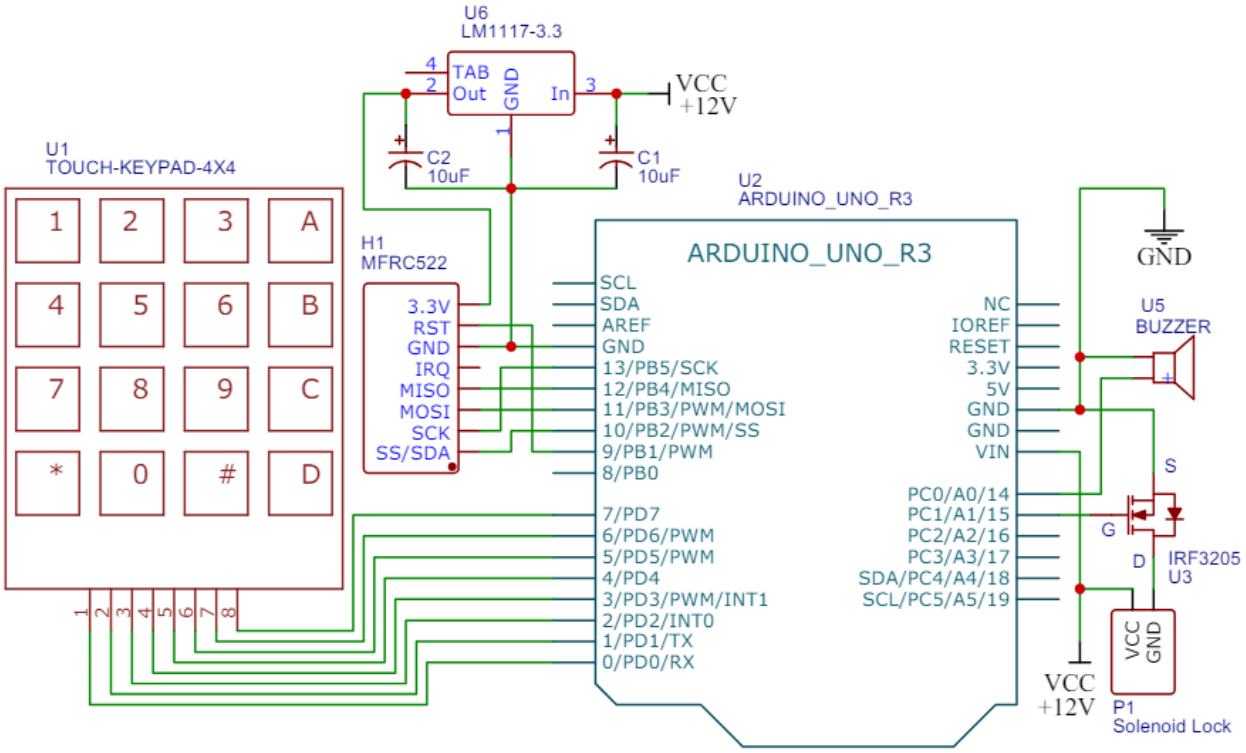

Рисунок 3.3 – Електрична принципова схема АСК доступом

Для введення коду доступу використовується матрична клавіатура 4x4, підключена до пінів 0-7 Arduino. Клавіатура дозволяє користувачам вводити код-пароль, який потім обробляється мікроконтролером для перевірки співпадіння з правильним кодом.

Модуль MFRC522 підключено до пінів D9 (RST), D10 (SS/SDA), D11 (MOSI), D12 (MISO), D13 (SCK) Arduino, а також до землі (GND) і виходу 3.3V, який отримує живлення через регулятор напруги LM1117. RFID модуль використовується для зчитування RFID-карт, що дозволяє безконтактно ідентифікувати користувачів.

Регулятор напруги LM1117 забезпечує стабільне живлення RFID модуля. Вхідна напруга 12V подається на вхід LM1117, а вихідна стабілізована напруга 3.3V живить модуль MFRC522. У якості обв'язки для LM1117 використано два електролітичних конденсатори на 10uF. Плюсові контакти конденсаторів підключені до входу та виходу мікросхеми. Мінусові контакти – до спільного контакту заземлення (GND). Конденсатори C1 та C2 виконують важливу роль в стабілізації напруги і фільтрації шумів. Вони згладжують напругу, зменшуючи пульсації та імпульсні завади, що можуть виникати від імпульсного блоку живлення.

Електромагнітний замок (соленоїд) підключений плюсовим контактом до джерела живлення 12V, а мінусовий контакт йде через MOSFET транзистор IRF3205. MOSFET керується мікроконтролером через пін D15, що дозволяє замикати і розмикати замок в залежності від стану системи. Коли користувач вводить правильний код або використовує авторизовану RFID-карту, MOSFET відкривається, подаючи живлення на соленоїдний замок, що призводить до його розблокування.

Зумер, підключений до піна D14 Arduino, видає звукові сигнали для індикації різних станів системи. При правильному введенні коду або зчитуванні RFID-карти зумер видає довгий сигнал, а при неправильній спробі доступу – два короткі сигнали.

Система живиться від джерела напруги 12V, яке подається на VCC всіх відповідних елементів: Arduino, регулятора напруги LM1117 та електромагнітного замка.

3.5 Компонентна база системи керування доступом

Для проектування системи керування доступом використано такі елементи: мікроконтролер Arduino UNO з платою розширення Ethernet Shield W5100, плата модуля MFRC522, матричний клавіатурний модуль, регулятор напруги LM1117 з двома конденсаторами в якості обв’язки, польовий транзистор IRF3205, соленоїдний замок та високочастотний п’єзоелектричний генератор звуку (зуммер).

Arduino UNO.

Arduino UNO – одна з найпопулярніших мікроконтролерних плат, широко використовувана для створення прототипів та навчання електроніці. Вона оснащена мікроконтролером ATmega328P, який працює на частоті 16 МГц. Плата має 14 цифрових входів/виходів, 6 з яких можуть працювати як ШІМ-виходи, та 6 аналогових входів. Її можна живити через USB або зовнішній блок живлення з напругою 7-12V. Вбудована пам'ять складає 32КБ Flash, 2КБ SRAM та 1КБ EEPROM. Завдяки своїй універсальності та великій спільноті підтримки, Arduino UNO є ідеальним вибором для даного проекту, забезпечуючи надійність та простоту інтеграції з іншими компонентами системи.

Arduino UNO існує у декількох версіях, кожна з яких має свої особливості та переваги. Найбільш відома версія — Arduino UNO R3 (Rev3), яка є останньою та найбільш поширеною версією цієї плати. Вона відрізняється від попередніх моделей поліпшеною сумісністю з шилдами (розширювальними платами) та додатковими пінами SDA і SCL для I2C-комунікації, а також окремими пінами для IOREF і RESET. Попередні версії включають Arduino UNO R1 та R2, які мали дещо інші компоненти та розташування пінів, але загалом зберігали основну функціональність та сумісність з більшістю аксесуарів. Також існують спеціальні версії, такі як Arduino UNO WiFi, яка має вбудований Wi-Fi модуль для бездротового підключення до мережі, і Arduino UNO SMD, яка відрізняється наявністю

мікросхеми в SMD-корпусі замість DIP. Плату Arduino UNO зображено на рисунку 2.4.

В моєму проекті Arduino UNO виконує роль центрального контролера. Вона отримує сигнали від RFID-зчитувача та клавіатури, обробляє їх, і відповідно керує електромагнітним замком. Також плата забезпечує комунікацію з веб-сервером через Ethernet Shield, передаючи дані про доступ у реальному часі.

Ethernet Shield W5100.

Ethernet Shield W5100 – це популярний модуль для платформи Arduino, який дозволяє підключати мікроконтролери до мережі Інтернет через Ethernet. Цей шилд базується на мікросхемі W5100 від компанії Wiznet, яка підтримує до чотирьох одночасних з'єднань TCP/IP. Плату Ethernet Shield W5100 зображено на рисунку 2.5.

В моєму проекті Ethernet Shield W5100 виконує функцію мережевого інтерфейсу, що дозволяє мікроконтролеру Arduino UNO передавати дані про доступ до захищених зон обчислювального лабораторного комплексу на веб-сервер у реальному часі.

Модуль MFRC522.

Модуль MFRC522 – це RFID-зчитувач, який широко використовується для безконтактної ідентифікації за допомогою радіочастотної технології. Цей модуль працює на частоті 13.56 МГц і підтримує стандарти ISO/IEC 14443 A/MIFARE.

В модулі MFRC522 наявні наступні хост-інтерфейси:

– Послідовний периферійний інтерфейс (SPI)

– Послідовний UART (схожий на RS232 з рівнями напруги, що залежать від напруги на контакті)

– I2C інтерфейс [31].

Рисунок 3.4 – Модуль MFRC522

Матрична клавіатура 4x4 кнопки

Матрична клавіатура є зручним пристроєм для введення даних у різноманітних електронних проектах. Цей тип клавіатури часто використовується з мікроконтролерами для створення інтерфейсів користувача.

Рисунок 3.5 – Матрична клавіатура 4*4

Технічні характеристики клавіатури:

– Кількість кнопок: 16 (4 рядки х 4 стовпці)
– Інтерфейс підключення: 8 пінів (4 рядки і 4 стовпці)
– Матеріал: Гнучка мембранна конструкція

– Розміри: 70 x 77 мм

– Контакти: 8 пінів (1, 2, 3, 4 для рядків; 5, 6, 7, 8 для стовпців)

Матрична клавіатура працює за принципом сканування рядків і стовпців. Кожна кнопка з'єднана на перетині рядка та стовпця. Коли користувач натискає кнопку, вона замикає відповідний рядок і стовпець, що дозволяє мікроконтролеру визначити, яка саме кнопка була натиснута. Для цього Arduino послідовно посилає сигнали на рядки і зчитує сигнали зі стовпців (або навпаки), що дозволяє точно визначити положення натиснутої кнопки. Схему з’єднання кнопок показано на рисунку 3.6.

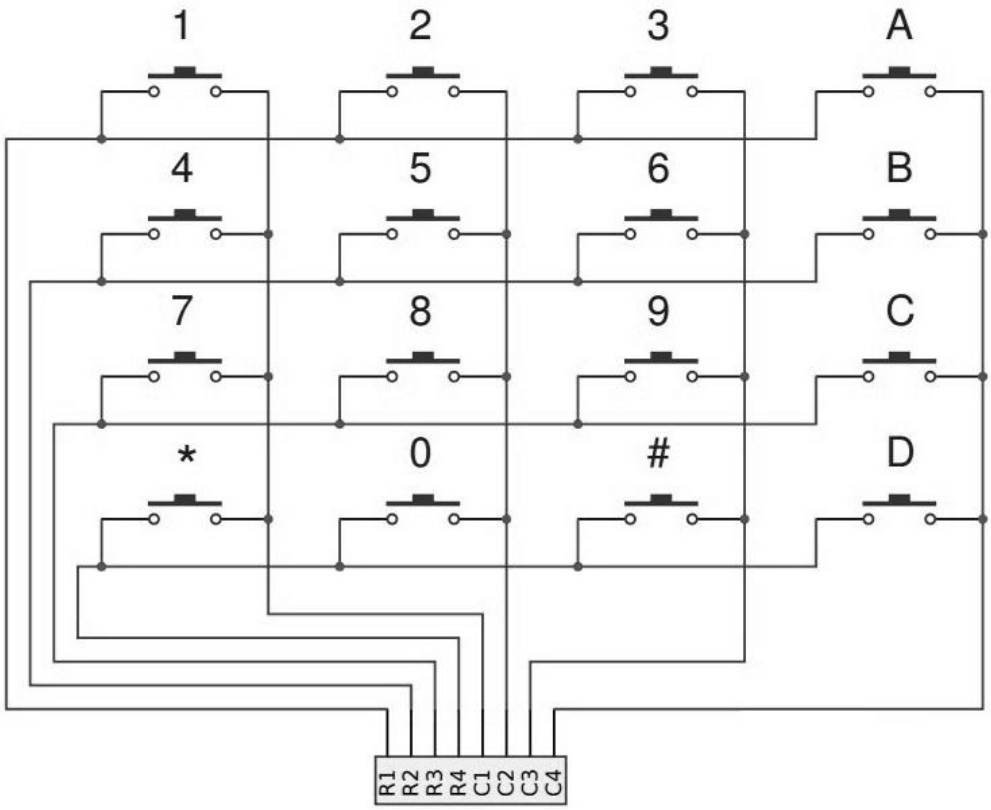

Рисунок 3.6 – Схема з’єднання кнопок в матричному модулі

Регулятор напруги LM1117.

LM1117 3.3V — це регулятор напруги (voltage regulator), який забезпечує стабільну напругу 3.3V, живлячись від вхідної напруги, що може варіюватися від 4.75V до 15V. Цей регулятор використовується для забезпечення живлення електронних компонентів, що потребують стабільної

напруги 3.3V, зокрема, таких як модулі RFID, датчики та інші мікроконтролери.

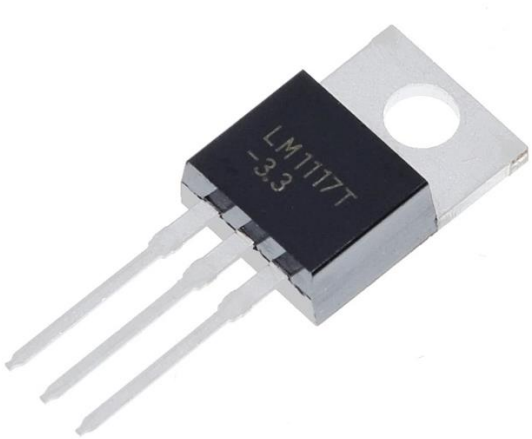

Рисунок 3.7 – регулятор напруги LM1117-3.3

Технічні характеристики LM1117-3.3:

– Вхідна напруга: 4.75V-15V
– Вихідна напруга: 3.3V
– Максимальний вихідний струм: 800mA
– Тип регулятора: LDO (Low Dropout)
– Падіння напруги: приблизно 1.1V при максимальному струмі
– Термозахист: вбудований захист від перегріву
– Наявний захист від короткого замикання

У моєму проекті регулятор LM1117 3.3V використовується для забезпечення стабільного живлення для RFID модуля MFRC522, який потребує напругу 3.3V. Arduino має вбудований регулятор, що дозволяє виводити 3.3V до спеціального піну, але так як RFID модуль MFRC522 може споживати струм дещо більший ніж може забезпечити пін 3.3V з Arduino, рішення щодо живлення модулю обрано саме через зовнішній спосіб, тобто через регулятор напруги для перетворення 12V в 3.3V. Регулятор LM1117 може бути виконаний в інших версіях, наприклад для вихідної напруги 1.8V, 2.5V, 5V, а також для регульованої напруги, що задається параметрами

обв’язки мікросхеми. Від стабільного живлення залежить коректна робота модуля RFID, який відповідає за зчитування та обробку даних з RFID-карт [25].

Польовий MOSFET транзистор IRF3205.

IRF3205 – це n-канальний MOSFET транзистор з високою потужністю, який широко використовується в різних електронних і електричних застосуваннях завдяки своїм відмінним технічним характеристикам. Його призначення полягає у використанні в схемах регуляторів потужності, високочастотних імпульсних джерел живлення, перетворювачів, звукових підсилювачів та іншого. Вигляд транзистора зображено на рисунку 2.6.

Технічні характеристики:

– Тип транзистора: N-канальний MOSFET
– Максимальна напруга стік-витік (VDSS): 55 В
– Максимальний струм стоку (ID): 110 А
– Опір стік-витік (RDS(on)): 8.0mΩ при VGS = 10V
– Максимальна потужність розсіювання: 200W
– Напруга порогу (VGS(th)): 2-4V [30].

У моєму проекті IRF3205 використано для керування електромагнітним замком, забезпечуючи достатній струм для активації соленоїда. Завдяки низькому опору та високій потужності, транзистор ефективно комутує живлення, мінімізуючи енергетичні втрати та нагрів.

Соленоїдний замок.

Соленоїдний замок – це електромеханічний пристрій, що використовується для контролю доступу шляхом блокування або розблокування дверей, ящиків або інших об'єктів. При подачі напруги соленоїдний замок зсуває або піднімає замковий механізм, дозволяючи доступ.

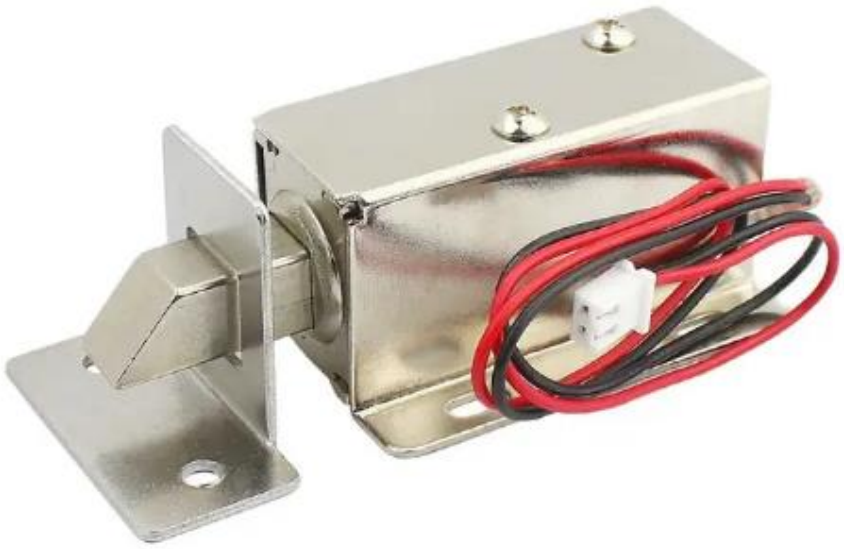

Рисунок 3.8 – Соленоїдний замок 12V

Технічні характеристики:

– Робоча напруга: 12V постійного струму
– Споживана потужність: 4-8W
– Струм споживання: 0.3-0.6A [32].

П’єзоелектричний генератор звуку (Buzzer).

Зуммер (англ. Buzzer) — це пристрій, який використовується для генерування звукових сигналів. Вони можуть бути використані у різних застосуваннях, включаючи сигналізацію, підтвердження натискання кнопок, таймери та інші системи оповіщення.

Існують два основних типи зуммерів: п'єзоелектричні та електромагнітні. П'єзоелектричні зуммери використовують п'єзоелектричний елемент для створення звуку. Вони мають низьке споживання енергії, тому часто використовуються в портативних пристроях, годинниках і невеликих гаджетах. Електромагнітні зуммери використовують електромагнітну котушку для створення звуку. Вони генерують більш насичений і гучний звук, що робить їх ідеальними для використання в автомобільних сигналізаціях і великих пристроях [33].

Рисунок 3.9 – П’єзоелектричний генератор звуку

Висновки до розділу 3

В даному розділі описано усі етапи проектування автоматизованої системи керування доступом до захищених зон ОЛК. Спроектований пристрій керує соленоїдним замком за допомогою мікроконтролера Arduino та підключених RFID модуля MFRC522 та клавіатури. Дані про отриманий доступ передаються на веб-сервер на опрацьовуються операторами.

Створено функціональну схему пристрою з її детальним описом кожного блока. Створено блок-схему алгоритму роботи системи, а також побудовано електричну принципову схему в середовищі Easy EDA. Виконано підбір усіх компонентів.

Охорона праці

Спеціальний розділ до дипломної роботи бакалавра

на тему: «Автоматизована система керування електроживленням лабораторних комплексів»

Спеціальність 151 «АКІТ»

151 – КРБ.1 – 471.22017102

Студент _____ О. В Гребеник

«___» червня 2024 р.

Керівник _____ М. І. Сідєлев

д.т.н., доцент

«___» червня 2024 р.

Консультант _____ О.В. Макарова

ст. викладач

«___» червня 2024 р.

Завідувач кафедри _____ М. І. Сідєлев

д.т.н., доцент

«___» червня 2024 р.

Миколаїв – 2024

ВСТУП

Охорона праці є критично важливою складовою для забезпечення безпечних і здорових умов праці в обчислювальних лабораторних комплексах. У таких умовах, де використовується електричне обладнання під високою напругою, дотримання стандартів безпеки та гігієни праці є обов’язковим для запобігання нещасним випадкам і збереження здоров’я працівників. Безпечне поводження з електрикою та забезпечення належного мікроклімату та освітлення мають прямий вплив на продуктивність і довговічність техніки, а також на загальний комфорт і працездатність персоналу.

Основна увага приділяється правильному використанню електроприладів. Техніка безпеки є невід'ємною частиною роботи з електроустановками. У підрозділі розглянуто розробку та затвердження відповідних інструкцій та положень. Також розглядаються технічні засоби захисту, такі як заземлення, автоматичні вимикачі та засоби індивідуального захисту, які значно знижують ризики, пов'язані з роботою з електрообладнанням.

Важливе місце у забезпеченні безпечних умов праці займає підтримка оптимального мікроклімату в лабораторіях. Це включає контроль температури, вологості, швидкості руху повітря та чистоти повітря, які є важливими для забезпечення ефективної роботи обладнання та комфорту персоналу.

Таким чином, охорона праці в обчислювальних лабораторних комплексах є багатогранною задачею, яка включає правильне поводження та обслуговування електрообладнання, підтримку температурного режиму, належного освітлення та дотримання норм пожежної безпеки.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ДСТУ – державний стандарт України

КЗпП – Кодекс законів про працю в Україні

ПБЕЕС – Правила безпечної експлуатації електроустановок споживачів.

ПТЕЕС – Правила технічної експлуатації електроустановок споживачів.

ПУЕ – Правила улаштування електроустановок.

ЗІЗ – Засоби індивідуального захисту.

ДСТУ – Державний стандарт України.

CO_2 – Вуглекислий газ (діоксид вуглецю).

4 ОХОРОНА ПРАЦІ

4.1 Основні закони та нормативні акти України в галузі охорони праці

В Україні законодавча база з охорони праці складається з Конституції України, Закону України «Про охорону праці», Кодексу законів про працю, та інших нормативно-правових актів. Основні положення визначають державну політику в галузі охорони праці, яка спрямована на забезпечення безпечних та здорових умов праці.

Основні законодавчі акти:

1. Конституція України — гарантує громадянам право на безпечні й здорові умови праці.

2. Закон України «Про охорону праці» — визначає основні засади державної політики у сфері охорони праці, обов'язки роботодавців та права працівників.

3. Кодекс законів про працю в Україні (КЗпП) — регулює трудові відносини, включаючи питання охорони праці.

4. Закон України «Про забезпечення санітарного та епідеміологічного благополуччя населення» — визначає санітарно-гігієнічні норми на робочих місцях.

5. Державні стандарти України (ДСТУ) — містять технічні регламенти та стандарти, що регулюють питання безпеки праці.

4.2 Специфічні вимоги до охорони праці в обчислювальних лабораторіях

Охорона праці в обчислювальних лабораторіях має свої специфічні вимоги, які включають забезпечення безпеки працівників, які працюють з електронним обладнанням та комп'ютерами.

Основні вимоги та рекомендації:

1. Електробезпека.

– Регулярні перевірки та обслуговування електричних мереж та обладнання.

– Використання пристроїв захисного відключення (ПЗВ) для запобігання електротравм.

– Дотримання правил безпечної експлуатації електроустановок.

2. Мікроклімат та освітлення.

– Забезпечення відповідного мікроклімату в лабораторії (температура, вологість, вентиляція).

– Адекватне освітлення робочих місць, з урахуванням рекомендацій щодо природного та штучного освітлення.

3. Ергономіка робочого місця.

– Використання ергономічних меблів (стільців, столів), що регулюються по висоті.

– Забезпечення правильного розташування комп'ютерів, моніторів та іншого обладнання для зменшення навантаження на зір та опорно-рухову систему.

4. Протипожежна безпека.

– Оснащення лабораторії засобами пожежогасіння.

– Проведення регулярних інструктажів та тренувань з евакуації.

– Дотримання правил зберігання та використання легкозаймистих матеріалів.

5. Організаційні заходи.

– Проведення інструктажів з охорони праці для нових працівників та регулярних повторних інструктажів.

– Розробка та впровадження інструкцій з охорони праці для конкретних робіт та процесів.

– Забезпечення працівників засобами індивідуального захисту (ЗІЗ) при необхідності [35].

Ці заходи спрямовані на створення безпечних умов праці та запобігання нещасним випадкам та професійним захворюванням в обчислювальних лабораторіях.

4.3 Електробезпека. Основні вимоги електробезпеки в обчислювальних лабораторіях

Електробезпека – це система організаційних і технічних заходів і засобів, які забезпечують захист людей від шкідливого і небезпечного впливу електричного струму, електричної дуги, електромагнітного поля і статичної електрики [34].

Електробезпека в обчислювальних лабораторіях забезпечується через систему організаційних та технічних заходів, що включають низку нормативних актів і стандартів. Основні вимоги електробезпеки регулюються такими документами:

1. Правила безпечної експлуатації електроустановок споживачів (ПБЕЕС), затверджені наказом Держнаглядохоронпраці України від 09.01.1998 № 4. Вони встановлюють вимоги до працівників, що обслуговують електроустановки напругою до 220 кВ.

2. Правила технічної експлуатації електроустановок споживачів (ПТЕЕС), затверджені наказом Мінпаливенерго України від 25.07.2006 № 258. Ці правила визначають організаційні та технічні вимоги щодо експлуатації електроустановок.

3. Правила улаштування електроустановок (ПУЕ), затверджені наказом Міністерства енергетики та вугільної промисловості України від 24.07.2017 № 476, є зведенням правил з проектування, розміщення, утримання, експлуатації та ремонту електроустановок [35].

Керівник підприємства повинен забезпечити належне утримання, експлуатацію та обслуговування електроустановок згідно з чинними нормативними актами. Для цього він має виконати такі заходи:

- Призначити працівника, відповідального за справний стан і безпечну експлуатацію електроустановок.
- Створити та укомплектувати електротехнічну службу з осіб, які досягли 18 років, мають відповідну освіту, пройшли медичний огляд та не мають медичних протипоказань.
- Розробити та затвердити Положення про енергетичну службу підприємства, посадові інструкції працівників та інструкції з безпечного виконання робіт.
- Забезпечити навчання працівників та регулярну перевірку їх знань, а також своєчасний огляд електроустановок, проведення профілактичних, протиаварійних та приймально-здавальних випробувань.
- Встановити порядок, за яким працівники, відповідальні за обслуговування електроустановок, будуть ретельно спостерігати за дорученим їм обладнанням і мережами.
- Постійно вживати заходів щодо оптимізації та модернізації виробничих процесів.

Для організації експлуатації електроустановок роботодавець повинен призначити відповідальну особу за електрогосподарство [35].

Технічні засоби захисту.

Для забезпечення електробезпеки в обчислювальних лабораторіях застосовуються різноманітні технічні засоби захисту:

Заземлення. Заземлення електроустановок запобігає ураженню електричним струмом за рахунок зниження потенціалу струму до безпечного рівня. Вимоги до заземлення викладені у ДСТУ Б В.2.5-82:2016, який визначає захисні заходи від ураження електричним струмом в будівлях і спорудах [36].

Автоматичні вимикачі. Автоматичні вимикачі використовуються для автоматичного відключення електричного живлення у випадку короткого замикання або перевантаження мережі, що запобігає можливим аваріям і

пожежам. Вимоги до використання таких вимикачів регулюються ПБЕЕС та ПТЕЕС [35].

Засоби індивідуального захисту (ЗІЗ). До засобів індивідуального захисту належать діелектричні рукавиці, килимки, ізолюючі штанги та інші засоби, які використовуються для захисту працівників при роботі з електрообладнанням. Правила експлуатації електрозахисних засобів, затверджені наказом Міністерства праці та соціальної політики України від 05.06.2001 № 253, визначають перелік засобів, вимоги до них та порядок їх застосування [34].

Дотримання зазначених вимог та застосування відповідних технічних засобів є ключовими для забезпечення електробезпеки в обчислювальних лабораторіях.

4.4 Мікроклімат та освітлення в обчислювальних лабораторних комплексах

Метеорологічні умови, або мікроклімат, включають такі показники як температура повітря, відносна вологість, швидкість руху повітря, інтенсивність теплового випромінювання та барометричний тиск. Ці параметри можуть впливати на самопочуття та працездатність людини, особливо в умовах, коли температура навколишнього середовища підвищується до 25 °С і вище, а відносна вологість становить більше ніж 75%.

В обчислювальних лабораторіях важливо підтримувати оптимальні мікрокліматичні умови для забезпечення ефективної роботи обладнання і комфорту для персоналу.

1. Температура і вологість. Оптимальна температура для приміщень з комп'ютерною технікою повинна бути в межах 18-22 °С. Відносна вологість повітря повинна становити 40-60%. Висока температура і вологість можуть спричинити перегрів та корозію обладнання, а надмірно сухе повітря може призвести до статичної електрики [37].

2. Швидкість руху повітря. Швидкість повітря не повинна перевищувати 0,2 м/с в зоні робочих місць. Це допомагає запобігти утворенню протягів, які можуть викликати дискомфорт і зниження працездатності персоналу [37].

3. Чистота повітря. Для забезпечення чистоти повітря необхідно використовувати вентиляційні системи з фільтрацією, які здатні затримувати пил, мікроорганізми, гази та запахи. Свіжість повітря може бути визначена концентрацією CO2, яка не повинна перевищувати 800 ppm для комфортних умов роботи [38].

Освітлення в обчислювальних лабораторіях.

Освітлення є критичним фактором для забезпечення комфортної та продуктивної роботи в обчислювальних лабораторіях. Норми освітлення включають як природне, так і штучне освітлення.

1. Природне освітлення. Лабораторії повинні бути розташовані таким чином, щоб максимально використовувати природне освітлення. Це допомагає знизити навантаження на зір та забезпечує психологічний комфорт. Важливо, щоб робочі місця були розташовані біля вікон, а штори та жалюзі використовувалися для регулювання кількості світла.

2. Штучне освітлення. Рівень штучного освітлення в обчислювальних лабораторіях повинен бути не менше 500 люкс на робочих поверхнях. Рекомендується використовувати світильники з розсіювачами, щоб уникнути утворення тіней і бликів на екранах моніторів. Для цього можна застосовувати комбіновані системи освітлення, які включають як загальне, так і локальне освітлення [39].

Дотримання оптимальних параметрів мікроклімату і освітлення є ключовим фактором для підтримки ефективної роботи в обчислювальних лабораторіях. Це допомагає забезпечити довговічність обладнання та високу продуктивність персоналу.

4.5 Пожежна безпека. Вимоги щодо пожежної безпеки в обчислювальних лабораторних комплексах

Пожежна безпека в обчислювальних лабораторних комплексах є критично важливим аспектом, що вимагає дотримання низки правил і стандартів для запобігання пожежам та мінімізації їх наслідків.

Основні вимоги пожежної безпеки.

1. Загальні положення:

– Згідно з ДБН В.1.1-7:2016 "Пожежна безпека об'єктів будівництва", будівлі та споруди повинні відповідати вимогам пожежної безпеки на всіх етапах їх життєвого циклу, від проектування до експлуатації [40].

– Усі приміщення мають бути обладнані системами автоматичної пожежної сигналізації та пожежогасіння відповідно до ДБН В.2.5-56:2014 "Системи протипожежного захисту" [40].

2. Електрообладнання:

– Електричні установки повинні бути захищені від коротких замикань і перевантажень. Необхідно використовувати автоматичні вимикачі та пристрої захисту від перенапруг [41].

– Забороняється експлуатація пошкодженого електрообладнання та використання тимчасових електричних проводок.

3. Організація простору:

– Робочі місця мають бути облаштовані таким чином, щоб забезпечити вільний доступ до засобів пожежогасіння та евакуаційних шляхів. Евакуаційні виходи повинні бути чітко позначені відповідно до ДСТУ ISO 6309:2007 "Протипожежний захист. Знаки безпеки" [42].

– Обчислювальні пристрої та лабораторне обладнання мають бути розміщені на негорючих поверхнях, а кабелі та дроти - у спеціальних коробах або каналах, що запобігають їх пошкодженню та займанню.

4. Зберігання матеріалів:

– Легкозаймисті та горючі рідини (ЛЗР, ГР) повинні зберігатися у металевих шафах з вогнезахисним покриттям і бути чітко марковані. Зберігання має відповідати вимогам пожежної безпеки щодо асортименту та кількості речовин, що не перевищують змінну потребу.

– Відпрацьовані ЛЗР і ГР повинні збиратися у герметичну тару для подальшої утилізації або регенерації [43].

5. Системи вентиляції:

– Витяжні системи повинні бути оснащені ефективними фільтрами та регулярно перевірятися на справність. Робота витяжних шаф з пошкодженими склом або несправною вентиляцією заборонена [43].

– Заборонено встановлювати витяжні шафи поблизу дверей та без дозволу керівництва.

6. Навчання та інструктажі:

– Всі працівники повинні проходити регулярні інструктажі з пожежної безпеки, знати місцезнаходження засобів пожежогасіння та вміти ними користуватися.

– План евакуації має бути розміщений на видних місцях, а персонал має знати свої дії у випадку пожежі [43].

4.6 Організація робочого місця. Ергономічні вимоги до робочих місць

Робоче місце — це зона простору, що оснащена необхідним устаткуванням, де відбувається трудова діяльність одного працівника чи групи працівників [44].

Ергономічне планування робочих місць в обчислювальних лабораторних комплексах є важливим аспектом для забезпечення ефективності та безпеки праці. Основні ергономічні вимоги можна розділити на кілька категорій: антропометричні, фізіологічні, психофізіологічні та гігієнічні.

Антропометричні вимоги.

Антропометричні вимоги враховують розміри тіла людини, забезпечуючи зручність і доступність усіх елементів робочого місця. Зокрема:

– Робочі столи та стільці повинні відповідати зросту і пропорціям тіла працівників, що дозволяє уникнути перенапруження м’язів.

– Робоче обладнання має бути розташоване в оптимальних зонах досяжності, щоб звести до мінімуму непотрібні рухи та зусилля [45].

Фізіологічні та психофізіологічні вимоги.

Ці вимоги стосуються здатності працівників ефективно сприймати, обробляти інформацію та приймати рішення:

– Забезпечення зручної робочої пози, яка підтримує стійкість корпусу, ніг, рук і голови, мінімізує затрати енергії та максимізує продуктивність.

– Правильне розміщення моніторів комп’ютерів на рівні очей для зменшення навантаження на шию і очі [45].

Гігієнічні вимоги.

Гігієнічні умови включають підтримку комфортного мікроклімату на робочому місці, зокрема:

– Адекватне освітлення, яке не створює бліків на екранах і забезпечує достатній рівень освітленості для роботи.

– Підтримка оптимальної температури та вологості в приміщенні.

– Мінімізація рівня шуму та вібрації для зниження стресу та втоми працівників [44].

Загальні принципи організації робочого місця.

До основних принципів організації робочого місця відносяться:

– На робочому місці не повинно бути нічого зайвого. Усі необхідні предмети мають бути розташовані поруч із працівником, але не заважати йому.

– Предмети, якими користуються частіше, повинні бути розташовані ближче, ніж ті, які використовуються рідше.

– Якщо працівник використовує обидві руки, місце розташування пристосувань вибирається з урахуванням зручності захоплення їх обома руками.

– Робоче місце повинно забезпечувати необхідну оглядовість, не бути захаращеним і дозволяти швидкий доступ до всіх необхідних інструментів та обладнання.

Забезпечення відповідності цим вимогам сприятиме зменшенню втоми та підвищенню продуктивності працівників, а також створенню комфортних та безпечних умов праці в обчислювальних лабораторних комплексах.

Висновки до розділу 4

В розділі "Охорона праці" розглянуто різні аспекти охорони праці, що спрямовані на збереження життя, здоров’я та працездатності працівників обчислювальних лабораторних комплексів. Зокрема розглянуто питання з електробезпеки, мікроклімату, освітлення, пожежної безпеки та організацію робочих місць в обчислювальних лабораторіях. Основна увага була приділена впливу дотримання стандартів безпеки та гігієни праці на продуктивність та здоров'я працівників.

Електробезпека. Дотримання вимог електробезпеки є ключовим фактором для запобігання нещасним випадкам та аваріям при роботі з електрообладнанням. Керівник підприємства зобов’язаний забезпечити утримання, експлуатацію і обслуговування електроустановок відповідно до вимог чинних нормативних документів, таких як ПБЕЕС, ПТЕЕС та ПУЕ. Важливо призначити відповідальну особу за справний стан і безпечну експлуатацію електроустановок, створити електротехнічну службу, розробити необхідні інструкції, а також організувати навчання і перевірку знань працівників.

Технічні засоби захисту. Для забезпечення електробезпеки в обчислювальних лабораторіях застосовуються технічні засоби захисту, такі як заземлення, автоматичні вимикачі та засоби індивідуального захисту.

Заземлення електроустановок запобігає ураженню електричним струмом, автоматичні вимикачі запобігають аваріям і пожежам, а засоби індивідуального захисту, такі як діелектричні рукавиці та килимки, забезпечують безпеку працівників при роботі з електрообладнанням.

Мікроклімат. Оптимальний мікроклімат в обчислювальних лабораторіях включає підтримку відповідної температури 18-22 °C та відносної вологості 40-60%. Важливим є також контроль швидкості руху повітря, яка не повинна перевищувати 0.2 м/с, та забезпечення чистоти повітря через ефективні вентиляційні системи.

Освітлення. Освітлення в обчислювальних лабораторіях повинно відповідати нормам, що включають як природне, так і штучне освітлення. Природне освітлення має бути максимально використане для забезпечення комфорту працівників, а штучне освітлення повинно бути не менше 500 люкс на робочих поверхнях. Використання комбінованих систем освітлення допомагає уникнути утворення тіней та бліків на екранах моніторів, що сприяє зниженню навантаження на зір та підвищенню продуктивності праці.

Дотримання стандартів безпеки та гігієни праці в обчислювальних лабораторних комплексах має значний вплив на продуктивність та здоров'я працівників. Забезпечення електробезпеки, використання технічних засобів захисту, підтримка оптимальних параметрів мікроклімату та належного освітлення створюють безпечні та комфортні умови праці, що сприяє підвищенню ефективності роботи та зменшенню ризику професійних захворювань і нещасних випадків.

ВИСНОВКИ

Системи керування живленням грають важливу роль у забезпеченні стабільної роботи всієї інфраструктури обчислювального лабораторного комплексу. Система автоматичного перемикання фаз дозволяє уникнути проблем, пов'язаних із нестабільністю напруги, перевантаженням окремих фаз та можливими аварійними ситуаціями.

Поставлене завдання полягало в розробці системи, принципом роботи якої є вимірювання значення напруги на всіх трьох фазах мережі за допомогою модулів PZEM-004T-100A, які знімають електричні параметри та передають дані на мікроконтролер Arduino UNO. У разі виявлення відхилення напруги за межі допустимого діапазону, система автоматично переключає навантаження на іншу фазу з нормальними параметрами. Використання модулів PZEM-004T-100A зумовлене їх доступністю, точністю та можливістю безконтактного вимірювання струму, що підвищує надійність і безпеку системи.

Важливим аспектом розробки є інтеграція з веб-сервером через Ethernet Shield W5100, що дозволяє оператору віддалено контролювати стан електричної мережі ОЛК. На веб-сайті відображаються показники, що вимірюються модулями PZEM-004T-100A. Це дозволяє своєчасно реагувати на зміни в мережі та запобігати можливим неполадкам. Такий підхід значно підвищує оперативність та ефективність управління електропостачанням ОЛК.

Обрана конфігурація системи, включаючи реле JQX-60F 60A 1C 12VDC, забезпечує максимальну надійність та безпеку при роботі з великими навантаженнями. Розрахунки допустимого діапазону напруги, перерізу силових провідників та максимального струму навантаження підтвердили, що розроблена система здатна ефективно функціонувати в умовах високих навантажень, характерних для обчислювального лабораторного комплексу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Інформаційно-обчислювальний центр. URL: https://wiki.nuwm.edu.ua/index.php/Інформаційно-обчислювальний_центр (дата звернення 10.04.2024)

2. Manal A.Abdel-Fattah, Yehia M.Helmy, Alaa M.Gabr: A Proposed Framework for Evaluating Performance of Data Center: International Journal of Computer Science and Information Security (IJCSIS). 2018. Vol. 16, No. 11

3. DATA CENTER FOR BEGINNERS: User Guide. URL: https://www.academia.edu/35967912/DATA_CENTER_FOR (дата звернення 11.05.2024)

4. Uptime Institute: Tier Classification System. URL: https://uptimeinstitute.com/tiers (дата звернення 11.05.2024)

5. ANSI/TIA-942-B: Telecommunications Infrastructure Standard for Data Centers. Arlington: Telecommunications Industry Association, 2017. 145 p.

6. ASHRAE. American Society of Heating, Refrigerating and Air-Conditioning Engineers. URL: https://www.ashrae.org/about (дата звернення 11.05.2024)

7. IEEE Standards association. URL: https://standards.ieee.org/search/?q=Power%20Energy&type=Standard (дата звернення 11.05.2024)

8. FISC Guidelines. URL: https://www.treasuredata.com/wp-content/uploads/Arm-Treasure-Data-Response-to-FISC-Guidelines.pdf (дата звернення 13.05.2024)

9. Fs Community. Storage Area Network vs Network Attached Storage. URL: https://community.fs.com/article/storage-area-network-san-vs-network-attached-storage-nas.html (дата звернення 13.05.2024)

10. RedHat. What is network attached storage? URL: https://www.redhat.com/en/topics/data-storage/network-attached-storage (дата звернення 13.05.2024)

11. VMware. SAN Conceptual and Design Basics. 2016. URL: https://www.vmware.com/pdf/esx_san_cfg_technote.pdf (дата звернення 13.05.2024)

12. Versitron. Data Center Security and Surveillance. URL: https://www.versitron.com/blogs/post/data-center-security-system-complete-guide (дата звернення 13.05.2024)

13. FS Community. Why Data Center Security Must Include Video Surveillance. URL: https://community.fs.com/article/data-center-video-surveillance-a-must-for-security.html (дата звернення 11.05.2024)

14. CCTV Security & Monitoring System for server room. URL: https://www.newtechapac.com/cctv-security-monitoring-system/ (дата звернення 11.05.2024)

15. System Assessment and Validation for Emergency Responders (SAVER). CCTV Technology Handbook. U.S. Department of Homeland Security, 2013. 147 p. URL: https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf (дата звернення 12.05.2024)

16. RFID Access Control System. URL: https://www.asecuri.com/rfid-access-control-system/ (дата звернення 15.05.2024)

17. What is RFID and NFC Access Control. URL: https://info.verkada.com/door-access-systems/rfid-vs-nfc-access-control-guide (дата звернення 15.05.2024)

18. FS Community. High-Density Servers: Maximizing Efficiency and Performance. URL: https://community.fs.com/article/highdensity-servers-maximizing-efficiency-and-performance-in-data-centers.html (дата звернення 16.05.2024)

19. FS Community. Exploring Rack Servers. URL: https://community.fs.com/article/exploring-rack-servers-the-scalable-solution-for-data-centers.html (дата звернення 16.05.2024)

20. FS Community. Server Racks: Purpose, Benefits, and Selection Tips. URL: https://community.fs.com/article/-what-is-a-server-rack-and-how-does-it-work.html (дата звернення 16.05.2024)

21. Smartech. How to Design Automatic Phase Selector Panel – Auto Phase Selector. URL: https://smartechmolabs.com/how-to-design-automatic-phase-selector-panel-auto-phase-selector (дата звернення 01.06.2024)

22. Новатек-Електро. Електронний перемикач фаз ПЕФ-301. URL: https://novatek-electro.com/product/elektronnij-peremikach-faz-pef-301.html (дата звернення 01.06.2024)

23. ДСТУ EN 50160:2014. Характеристики напруги електропостачання в електричних мережах загальної призначеності. Київ: Мінекономрозвитку України, 2014. 34 с.

24. Правила улаштування електроустановок. Київ: Міністерство енергетики та вугільної промисловості України, 2014. 720 с.

25. Texas Instruments. LM1117: Low Dropout Voltage Regulator. URL: https://www.ti.com/lit/ds/symlink/lm1117.pdf (дата звернення 06.06.2024)

26. Arduino. Arduino UNO Rev3. URL: https://docs.arduino.cc/hardware/uno-rev3/ (дата звернення 28.05.2024)

27. Arduino. Arduino Ethernet Shield W5100. URL: https://docs.arduino.cc/retired/shields/arduino-ethernet-shield-without-poe-module/ (дата звернення 28.05.2024)

28. GitHub. PZEM-004T V3.0 Datasheet and User Manual. URL: https://github.com/vortigont/pzem-edl/blob/main/docs/PZEM-004T-V3.0-Datasheet-User-Manual.pdf (дата звернення 06.06.2024)

29. Amazon. JQX-60F High Power Relay AC220V. URL: https://www.amazon.com/JQX-60F-High-Power-Relay-AC110V-AC220V/dp/B0CY84MSN4?th=1 (дата звернення 06.06.2024)

30. AllTransistors. MOSFET Transistor IRF3205. URL: https://alltransistors.com/mosfet/transistor.php?transistor=2363 (дата звернення 06.06.2024)

31. NXP Semiconductors. MFRC522: Standard Performance. URL: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf (дата звернення 06.06.2024)

32. Amazon. Electromagnetic Solenoid Assembly Electric. URL: https://www.amazon.com/uxcell-Electromagnetic-Solenoid-Assembly-Electirc/dp/B07TMWY94C (дата звернення 07.06.2024)

33. Piezoelectric Sound Components. URL: https://wiki-content.arduino.cc/documents/datasheets/PIEZO-PKM22EPPH4001-BO.pdf (дата звернення07.06.2024)

34. Підручники.com. Електробезпека. URL: https://pidru4niki.com/92796/bzhd/elektrobezpeka (дата звернення 04.06.24)

35. Pro-Op.com.ua. Електробезпека. URL: https://pro-op.com.ua/article/745-elektrobezpeka (дата звернення 04.06.24)

36. Будстандарт Онлайн. НПАОП 40.1-1.32-01. Правила будови електроустановок. Вимоги до електричної безпеки. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=65395 (дата звернення 05.06.24)

37. Navyflex.com.ua. Мікроклімат в будинку: параметри, вимоги і контроль. URL: https://navyflex.com.ua/mikroklimat-v-budynku-parametry-vymogy-i-kontrol/ (дата звернення 05.06.24)

38. kbg.pnu.edu.ua. Мікроклімат та вентиляція. URL: https://kbg.pnu.edu.ua/мікроклімат-та-вентиляція (дата звернення 05.06.24)

39. Klaster.ua. Основні вимоги до освітлення приміщень і робочих місць. URL: https://klaster.ua/ua/stati-i-obzory/osnovnye-trebovaniya-k-osvescheniyu-pomescheniy-i-rabochih-mest (дата звернення 05.06.24)

40. Електронна система здійснення декларування. ДБН В.2.5-56:2014 Системи протипожежного захисту. URL: https://e-construction.gov.ua/laws_detail/3080743763845318619?doc_type=2 (дата звернення 05.06.24)

41. Будстандарт Онлайн. ДБН В.2.5-56:2014 Системи протипожежного захисту. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82138 (дата звернення 05.06.24)

42. Euroservis.com.ua. Правила пожежної безпеки в Україні. URL: https://euroservis.com.ua/ua/pravila-pozharnoy-bezopasnosti-v-ukraine (дата звернення 05.06.24)

43. Pro-Op.com.ua. Інструкція про заходи пожежної безпеки у лабораторії. URL: https://pro-op.com.ua/article/957-nstruktsya-pro-zahodi-pojejno-bezpeki-u-laborator (дата звернення 05.06.24)

44. Підручники.com. Ергономічні вимоги до організації робочих місць. URL:https://pidru4niki.com/14821111/bzhd/ergonomichni_vimogi_organizatsiyi_robochih_mists (дата звернення 05.06.24)

45. Studies.in.ua. Ергономічні вимоги до організації робочих місць. URL: https://studies.in.ua/bjd-lapin/1142-ergonomchn-vimogi-do-organzacyi-robochih-msc.html (дата звернення 05.06.24)